kyndryl

Kyndryl Resiliency Orchestration

Installation 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

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
8.1	June 2020	1.2.4 Kyndryl Resiliency File Replicator	8.1.x
		1.3.2 Software Package	
		3.2.1 Supported versions of MariaDB and Tomcat	
		3.2.4 Supported Browsers	
		5.4 Installation of RO server in GUI mode	
		5.4.1 Migrating DB Component from Local Host to dedicated Server (split installation)	
		5.5.1 Editing the Properties File	
		5.6 Post-installation Steps of RO application	
		5.8 Changing Default Passwords (Recommended)	
		7.17 Configuring Kyndryl Resiliency Orchestration Server and Site Controller for Secured Communication by Using the ActiveMQ Broker	
		7.3 Server Operating System Hardening (Optional)	
		9.6.3 Post-installation Steps after you install the Site Controller in Linux	
		10.8 Post-installation Steps after you install the Site Controller in Windows	
		11.6 Installation of Agents.	
		16 Installing Kyndryl Resiliency Orchestration Server OVA Manually	
		16.5 Creating NICRA OVA for Kyndryl RBR Solution	
		16.5.1 Pre-requisites	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		17 Installing DMC on Windows Server	
8.1.1	September 2020	5.6 Post-installation Steps Kyndryl Resiliency Orchestration application	8.1.x
		29.13.2 Add Exception to Firewall	
		1.3.2 Java versions used in Kyndryl Resiliency Orchestration	
		3.2.1 Supported versions of MariaDB and Tomcat	
		3.2.2 Supported OS for Kyndryl RO and SC	
		3.2.3 Agent Supportability	
		3.2.4 Supported Browsers	
		5.5.1, 9.6.1, 10.7.1 - MODIFY_SYSTEM_FILES property details	
		28.1 Migrating to New Server with Same IP	
		28.2 Migrating to New Server with New IP	
		15.4 Install TDMF on AIX:	
		18.2 Creating Nicra/Sa OVA Using Automation Script	
		9.6.3 and 10.8 Post-installation Steps after you install the Site Controller in Linux/Windows	
		13.3.7Installing TDMF Agent on Linux	
		9.8 and 10.12 Upgrading Site Controller	
8.1.2	December 2020	1.3.2 Software Packages	8.1.x
		3.2.1 Supported versions of MariaDB and Tomcat	
		3.2.2 Supported OS for Kyndryl Resiliency Orchestration	
		4.5.3.1 Vault Integration	
		5.6 Post-installation steps Kyndryl Resiliency Orchestration application	
		7.10.4 Generating Keystore and Trusttore	
		7.10.5 Replacing the default panacesACP keystore and truststore passwords	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		7.10.6.2 Encrypting passwords on Local agents	
		7.13.3 Capturing syslog events	
		7.17.4 Encrypting the custom store passwords for ActiveMQ	
		9.6.3 Post-installation Steps after you install the Site Controller in Linux	
		10.8 Post-installation Steps after you install the Site Controller in Windows	
		17 Installing DMC on Windows Server	
		29.3 Troubleshooting -> Resiliency Orchestration application hangs	
		29.11 Troubleshooting -> Resiliency Orchestration HA Replication Monitoring	
8.1.3	March 2021	1.3.2 Software Packages	8.1.x
		3.2 Supported OS and features	
		4.4 Installation of Apache Tomcat Server (Note about unzip utility)	
		5.6 Post-installation Steps Kyndryl Resiliency Orchestration application	
		6.2 Installation of Resiliency Orchestration Server	
		9.4 Prerequisites and 9.5 Installing Site Controler in GUI mode in Linux	
		10.5 Prerequisites for Installing Site Controller in GUI Mode in Windows	
		11.3 Installation of supported JRE	
		11.6 Installation of Agents on Windows	
		13.1 Installation of Agents on Linux	
		7.10.2 Generating Custom Keystore Certificate	
		22.3 Editing Properties File	
		23 Installing Third-party Software	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		13.1 Installation of Agents	
		23 Installing Third-party Software	
8.1.3.1	April 2021	23.1.1RHEL Supported versions	
8.1.3.2	May 2021	9.4 Co-hosted SC changes the default setting value	
		5.8 Steps to be followed for changing the default password for RO, SC (Linux), SC (Windows) Local agent (Linux)Local Agent (Windows)	
		1.3.1 Software Packages Java versions used in Kyndryl Resiliency Orchestration. Update of JDK to JDK 291	
8.2.0	June 2021	5.6.1 ServiceNow configuration in multitenancy RO setup and single tenancy	
		5.6 under step 15 tomcatuser information update.	
		10.4 and 29.15.2 added Port 135	
		5.6.3.4 ICD section added for multi-tenancy and single tenancy	
8.2.1		3.2 Support matrix update RHEL 8.4 Support matrix update Tomcat 9.0.48	
		5.6.3.2 ICD Integration With RO- two-way communication.	
8.2.3		7.7 note added TLS 1.2 strongly recommended	
		7.21 Added monitor health section to RO server	
		7.8 keystorepass connector update, detail of 2 Jar files to be moved page 141	
		9.9 Added monitor health section to Linux SC	
		10.13Added monitor health section to Windows SC	
8.2.6		7.10 How to generate ACP certificate for RO Custom Keystore certificate updated Page 142	8.2.x
		JDK version updated to 301 for Windows 2019, RHEL 8.4 Page 45	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		RHEL 8.4, Tomcat 9.0.54 supported in Kyndryl RO 8.2.6 Page 57	
		removed the jar file as it is not required due to automation log4j-1.2.17.jar	
		ActiveMQ update with steps 4 to step 8 Page 148	
		4.2 Support matrix updated Page 47	
		18.4 OVA name updated to IBMRO_8.2.6.OVA Page 254	
		Section 1.3.2 Java 311 updates page 24	
		Section 19 DMC sizing Page 266	
		Section 1.3.2 Note with * updated Page 25	
		Section 20.2 Post OVA deployment steps Page 278	
		Section 13.7 Port 577 Image updated Page 198	
		Section 19 ESXi 7.0 updated Page 267	
	Dec 2021	Section 4.3 MariaDB step 3 updated Page 39	
		Section 5.4 Validation key Step 11, Page 56 Table 18: Keywords in the PanacesServerInstaller.properties file, Page 80	
		Section 30.2 Migrating to new Server with New IP Step 15, Page 323	
		5.6 under point 15 added note on mysql user and all other users Page 91	
		3.2 OS versions Tomcat updated to 54 Page 37	
		1.3.2 Table 1 JDK versions updated Page 25	
		1.3.1 Software Packages	
		5.6 under step 15 tomcatuser information update.	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		10.4 and 29.15.2 added Port 135	
		5.6.3,4 ICD section added for multi-tenancy and single tenancy	
		3.2 Support matrix update RHEL 8.4	
		Support matrix update Tomcat 9.0.48	
		7.7 note added TLS 1.2 strongly recommended	
		7.21 Added monitor health section to RO server	
		7.8 keystorepass connector update, given detail of 2 Jar files to be moved page 141	
		9.9 Added monitor health section to Linux SC	
		10.13Added monitor health section to Windows SC	
		7.10 How to generate ACP certificate for RO Custom Keystore certificate updated Page 142	
		JDK version updated to 301 for Windows 2019, RHEL 8.4 Page 45	
		RHEL 8.4, Tomcat 9.0.54 supported in Kyndryl RO 8.2.6 Page 57	
		Removed the jar file as it is not required due to automation log4j-1.2.17.jar	
		ActiveMQ update with steps 4 to step 8 Page 148	
		4.2 Support matrix updated Page 47	
		18.4 OVA name updated to IBMRO_8.2.6.OVA Page 254	
		Section 1.3.2 Java 311 updates page 24	
		Section 19 DMC sizing Page 266	
		Section 1.3.2 Note with * updated Page 25	
		Section 20.2 Post OVA deployment steps Page 278	
		Section 13.7 Port 577 Image updated Page 198	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		Section 19 ESXi 7.0 updated Page 267	
		Section 4.3 MariaDB step 3 updated Page 39	
		Section 5.4 Validation key Step 11, Page 56	
		Section 31.20 Archiving the Resiliency Orchestration Anomaly Detection (ROAD) Raw Data, Page 679	
8.2.7	Jan 2022	Section 3.2 RHEL version 8.5 added in RO, Site Controller, Local Agents row created and Note deleted, Page 37-38	8.2.x
		Section 25.1.1 RHEL version 8.5 added in title, Page 305	
8.2.8	Feb 2022	Removed Upgrade specific Note as it is also required for fresh installation, GA_VERSION_FILENAME_WITHPATH=<validation key>, Page 80	8.2.x
		Added subheadings “Removing old log4J jars” and “Adding new Log4J2 jars” under “Section 4.4 - Installation of Apache Tomcat server”, Page 41,42	
		Added section 31.21 - Removing Older Jars from Backup folder in production Server in Troubleshooting chapter, Page 342	
		19 DMC installation in windows section Added requirement of Windows SC Page 269	
		Added section 30.3 – “Changing Resiliency Orchestration Server IP to New IP” under the section “Migrating the Resiliency Orchestration Server”, Pages 318, 319	8.2.x
		Added section 7.14.2 – “Configuration to receive the AuditInfo and EventLogs on Syslog Server:”, Page 141	
		Section 10.8.1 newly added stating dependence of Windows SC page 183	
		9.6.3.1 Limitation for Linux Site controller Page 169	
8.2.9	March	Added the following section: 31. Migrating remote agents from Agent Node (RO) to Site Controller, Page 322	
		13.6 DMC Agent installation MANAGEMENT_SERVICE in the Generic Agent Object Type text box. BLOCKREPLICATOR-V2 in the Generic Agent Object Class. page 196	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		Section:3.2 Added Note: Character limit depends on OS on page 38	
		Added the following section: 7.22 Standby server configuration, Page 153	
		Added in 2.1.2 point “VI “co-hosted Site Controller not supported page 31	
		13.5.2 User has to set the dmc.exe path in the system environment variable and restart the DMC page 191	
		13.6 Cloud-based RO supports only Private IP for communication with SC and DMC. Page 192	
		5.6 “Post-installation Steps for Kyndryl Resiliency Orchestration application”, Onboarding RO reports to Unified Resiliency Platform, Page 91	
		5.6 “Post Installation Steps for Kyndryl Resiliency Orchestration application”, Added a new step (Step 15) on Page 92.	
		Deleted the sections “14.5 HA Configuration” and “32.10 HA Configuration” to address the JIRA ticket RO-16741.	
		5.6 “Post-installation Steps for Kyndryl Resiliency Orchestration application”, Added a new step (Step 4) on Page 88.	
		18.1 added step13 for FQDN Page 240	
		Added section 33 - Recommendations for Site Controller (SC) High Availability for Linux and Windows, Page 350	
8.2.9.1	April 2022	Section 3.2.1 Agent Supportability, Page 38	8.2.x
		Added Section 35 Known limitation, Page 346	
		Updated section, 7.5 Configuring Resiliency Orchestration for Optimal Performance, Table: Configuring Resiliency Orchestration Server for optimal performance, max_connections, and panaces.mysql.maxconnection values – 1000 and 750.	
8.2.9.2	May 2022	Added a Note in Step 2 under the section “30.1 Migrating to new Server with Same IP” on Page 324. Reference JIRA: RO-41916	8.2.x

`Document Version	Revision Date	Sections Updated	Supported Product Version
		Updated the table in the section “10.4 Ports Used by Windows Based Site Controller” on Page 193. Reference JIRA: RO-42278	8.2.x
		Updated the JAVA_HOME path for both Windows SC and Linux in the section 5.8 Changing Default Passwords (Recommended) on Page 110. Reference JIRA: RO-42278	8.2.x
		Updated Table 4 and Table 5 on Software Sizing Recommendation on Page 33 and Page 35 respectively. Also added a new Note at the end of the table. Reference JIRA: RO-41065	8.2.x
		Updated the heading from “Enabling two-way TLSv1.2 Authentication” to “Authenticating two-way TLS v1.2” on Page 134. Reference JIRA: RO-39785	8.2.x
8.3.0	June 2022	10.4 Port 135 is used for ping operations on windows end points, hence is required to be opened up on the end points for the ping operations to be successful. Page 201	8.3.x
8.3.0	June 2022	10.5 Second bullet point added in prerequisites section on Page 201	8.3.x
		13.6 Step 11 Parameters updated and sequence changed steps added for both Agent RBR and Agentless RBR page 227	
8.3.0	June 2022	Updated Step 1 in the section “5.8 Changing Default Passwords (Recommended)” on Page 115. JIRA: RO-43784	8.3.x
8.3.0	June 2022	Added a new section “9.6.3.1 Post Validation Steps During Server Startup in Linux on Page 198 and “10.8.1 Post Validation Steps During Server Startup in Windows” on Page 214.JIRA: RO-37576	8.3.x
		Updated the section Migrating remote agents from Agent Node (RO) to Site Controller - Page 349	
		Updated the section 3.2.2 Supported Browsers section on Page 44.	8.3.x

`Document Version	Revision Date	Sections Updated	Supported Product Version
		An updated first bullet point in a table under he section 9.3 Ports Used by Linux Based Site Controller on Page 187.	8.3.x
8.3.1	July 2022	Added a new section “3.3 Ports used by RO/SC/Agents” on Page 46. Reference JIRA: RO-44779	8.3.x
		Added a new section “35.2 Backup and Restore of Metadata” on Page 377. Reference JIRA: RO-12614 and RO-43867	8.3.x
8.3.2	August 2022	Added a new section “9.10 Site Controller with Dual IP Support” on Page 205.	8.3.x
		Added a new section “35.3 Socket Read timeout error during synchronizing file set” on Page 381. Reference JIRA: RO-46876	8.3.x
8.3.3	September 2022	Added section “8.1.8 - “Scenarios that Require a RO Restart to Take Effect” on Page 191.	8.3.x
		Updated section: 24.10.2 PanacesAgentsInstaller.properties file, table - Keywords of PanacesAgentsInstaller.properties File, added Note under USER_INPUT_RESULT_JAR_ORA and USER_INPUT_RESULT_JLIB_ORA. (For TS010233040)	
		From section 3.2 Supported OS and features, removed row for 10.3.23 as we are not shipping Bundled with Installer.	
		Added a new section “35.4 MSSQL Local Agent dataset discovery process fails” on Page 402. Reference JIRA: RO-47105	8.3.x
		Updated the “3.2.2 Supported Browsers” section on Page 42. JIRA: RO-47835	8.3.x
		Updated the sections to include RHEL 8.6 version.Supported OS and features25.1.1 RHEL 7.5/7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.4/8.5/8.6 (64-Bit) JIRA: RO-47824	8.3.x

`Document Version	Revision Date	Sections Updated	Supported Product Version
		Deleted the section “Option1 Using “password updater “predecided complex password is set.” on Page 122. Reference JIRA: RO-47875	8.3.x
		Section 30.2 page 353 added Note: Modifying of the IP is not supported and there are unknown risks involved if we do. RO-76	8.3.x
		Section 25.7 Installing LIBLDM Utility Tool created pages 335-336	8.3.x
		Section 35.5 passwordupdater.sh script is non-functional page 383	
8.3.4	October 2022	Updated Step 17 in the section “5.6 Post-installation Steps for IBM Resiliency Orchestration application” on Page 112.RO-49061	8.3.x
		Added a new section 35.6 “HA Configuration Fails” on Page 38RO-49777	8.3.x
8.3.5	Nov 2022	Added note 4.3 “Installation of MariaDB” on Page 53. RO-50422	8.3.x
		Added point 2under note in section 5.4 “Installation of Resiliency Orchestration Server in Graphical Mode” on Page 56.RO-50422	8.3.x
		Updated the section “3.2 Supported OS and Features” with the latest Tomcat version on Page 44 RO-50613	8.3.x
		Updated the section “3.2 Supported OS and Features” with the latest RHEL version on Page 44. RO-50614	8.3.x
		Updated the section “3.2 Supported OS and Features” with the latest MariaDB version on Page 44.RO-50612	8.3.x
		Updated section 3.2.1 “Agent Supportability” page 45 RO-51217	8.3.x
		Section 10.8.1B Post Validation Steps During Server Startup in Windows Page 226 JIRA RO-50606	8.3.x

`Document Version	Revision Date	Sections Updated	Supported Product Version
8.3.6	December 2022	Added a new Note in the section “3.2 Supported OS and Features” on Page 45. RO-48406	8.3.x
8.3.7	January 2023	Updated Supported OS and features (Documented only the tested versions).Added Limitation in the Installing Site Controller in MS- Windows section.	8.3.x
8.3.8	February 2023	Added steps for 18.1 Creating NICR/SA (RHEL 8.4) steps 3.1 to 3.4	
		Changed 18.1 title to updating NICRA/SA (RHEL8.4)	
		Changed 20 Title 18.6 to updating NICRA /SA (RHEL7.6)	
		Moved chapter 20 to 18.6 and pasted after 18.5 and chapter 19 continued older Section 21 is new Section 20.	
		Added to section 18.6 Creating NICR/SA (RHEL 7.6) steps 3.1 to 3.4	
		4.4 installation of Tomcat Server workaround proved to comment out a specified command page53	
		Removed the following text from the Installation of Apache Tomcat Server section:Workaround required: Comment out below command for current RO release: During Postgres Dataset discovery, there is a call made to the TOMCAT Web Server with credentials in the query Parameter. This call is not visible to the user. Since all access requests to TOMCAT are logged in the localhost_access_log file, the credential is visible. Permanent Fix is to change the API to send it in request BODY. However as a workaround we can disable localhost access log	
8.3.9	March 2023	Updated the 3.2 Supported OS and features: RHEL 9.1 , tomcat 9.0.72, Mariadb 10.5.19 Section 3.2 Supported OS and features page 42	
		Updated 1.3.2 Software Packages java version as jdk1.8.0_362	
		Added note in section 7.5 In panaces.property. panaces.acp.server.concurrentRequestProcessCount	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		panaces.acp.server.concurrentRequestProcessCountMax This concurrentRequestProcessCountMax property should be equal or greater than concurrentRequestProcessCount	
		Added note Section 4.5.3.1 Note- Below setting are required to establish a Vault connection. 1.Change $EAMSROOT/installconfig/panaces.properties from 30 to 1000: 2. Set the value of panaces.acp.server.concurrentRequestProcessCountMax = 1000	
		Updated supported browser version.	
8.3.10.0	April 2023	1. Removed Onboarding RO reports to Unified Resiliency Platform from Section 5: Installing the Kyndryl Resiliency Orchestration Application Software Page no :117 2. Updated Supported Supported O/S, D/B Platforms, and Web Server	
8.3.11.0	May 2023	Updated Architecture diagram with port details	
		“jdk” certified version updated to 1.8.0_372	
		Browser updated Google Chrome Version 113.0.5672.127 (Official Build) (64-bit)Microsot Edge Version 113.0.1774.35 (64-bit) FireFox - 112.0.2 (64bit)	
		Updated MariaDB 10.5.20, Tomcat 9.0.73	
		Added section: SSL certificate expiry	
		Updated UpgradeAssist directory command page 286	
8.4.0.0	June 2023	RHEL 9.2 (Plow), Tomcat/9.0.75, Maria DB: 10.5.20, Java : OpenJDK Runtime Environment (Zulu 8.70.0.24-SA-linux64) updated	
		Updated section ‘Configuring Resiliency Orchestration for Optimal Performance’ with reference links, Page 143	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		Under Log4j “if agent logs are not generating “workaround is given	
		Added section: Migrating from one RHEL version to another RHEL version.	
		Updated section – Software Packages. – Added a note. Page - 33	
8.4.1.0	July 23	Deleted step related to validation key passport advantage step 11.	
		Tomcat 9.0.76 Maria DB 10.5.21 updated	
8.4.2.0	August 2023	Removed duplicate information about IBM control desk ICD and Encryption in SNOW. 5.6.1, 5.6.2 removed	
		Updated OpenJDK Runtime Environment (Zulu 8.70.0.24-SA-linux64) (build 1.8.0_382-b05)	
8.4.3.0	September 23	Updated section Kyndryl Resiliency Orchestration Server and Site Controller Sizing Guidelines with AD2C Resource Requirements Added the following sections: • Generating PanacesACP keystore/truststore through Shell Script • Manual steps for creating panacesACP keystore/trustore • Generating sanovi.keystore Deleted multiple sections with old information related to Keystore	
8.4.4.0	October 2023	Updated support matrix Updated Keystore Certification related information	

`Document Version	Revision Date	Sections Updated	Supported Product Version
8.4.5.0	November 2023	Updated support matrix Tomcat 9.0.82 Maria DB: 10.5.22 OpenJDK Runtime Environment (build 1.8.0_392). Section 7.5.1-Swapiness Value Configuration for Linux RO Server added Firefox: 119.0.1 (64-bit) Microsoft Edge: Version 119.0.2151.97 (Official build) (64-bit) Chrome : Version 119.0.6045.160 (Official Build) (64-bit) 7.13.2 added Note: From RO 8.4.5.0 onwards RO GUI logger filename has been changed from "PanacesStrutsGUI.log" to "PanacesGUI.log' from "PanacesStrutsGUI.log.debug" to "PanacesGUI.log.debug" respectively	
8.4.6.0	December 2023	Support matrix RHEL 9.3 (Plow) Tomcat 9.0.83 Supported Browser Information updated 13.2 A single bundle with all agents in one binary to be downloaded from CRO 8.4.0 onwards.	
8.4.7.0	January 2024	Support matrix Tomcat 9.0.84 updated	
8.4.8.0	February 2024	Support matrix Tomcat 9.0.85 ,Maria DB 10.5.24 OpenJDK Runtime Environment (Azul Zulu JDK 8.0.402and bundle with build) updated Chrome: Version 122.0.6261.69 (Official Build) (64-bit) Firefox: 122.0.1 (64-bit) Microsoft Edge: Version 122.0.2365.59 (Official build) (64-bit) Corrected Note 7.13.2added note: From RO 8.4.5.0 onwards RO GUI logger filename has been changed from "PanacesStrutsGUI.log" to "PanacesGUI.log' from "PanacesStrutsGUI.log.debug" to "PanacesGUI.log.debug" respectively.	
8.4.9.0	March 2024	Support matrix Tomcat 9.0.86 updated 7.13.1 for huge DB purge additional functionality added	

`Document Version	Revision Date	Sections Updated	Supported Product Version
		Limit config is added in panaces.properties. panaces.db.NrOfRecordsForBatchDeletion=10000 3.3.4 **Note**: It is not mandatory, from RO 8.4.9.0 onwards to open Port 22 for SSH protocol. Browser updated as Chrome: Version 123.0.6312.59 (Official Build) (64-bit)Version Microsoft Edge: Version 122.0.2365.92 (Official build) (64-bit) Mozilla Firefox: 124.0 (64-bit)Firefox version-124.0 64 bit Section 101.10 added Step 187. Execute the following command on the SC to make .ps1 script to work `Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass` `18.1 RBR OVA` (RHEL 8.4/8.6/8.8) update 9.4 Prerequisite Linux , 10.5 Prerequisite Windows **Note**: One Component IP should be configured to only one SC (Linux/window)	

kyndryl

Contents

kyndryl

List of Figures

kyndryl

List of Tables

Preface

The Kyndryl Resiliency Orchestration Installation Guide provides concepts and procedures to install the Kyndryl Resiliency Orchestration product. This guide is intended for administrators responsible for installing, configuring, and maintaining the product.

> **Note**
>
> The company name Kyndryl and Kyndryl Corporation are used interchangeably. The terminology Kyndryl Resiliency Orchestration used in this document refers to and stands for the Kyndryl Resiliency Orchestration Application. The terminologies Site Controller and Agent Node are used interchangeably.

Purpose

The Installation Guide helps you to install the Kyndryl Resiliency Orchestration Application and its components, by providing you with instructions and detailed procedures.

Audience

This manual is for administrators who are responsible for the installation, configuration, and uninstallation of Kyndryl Resiliency Orchestration software and its services.

kyndryl

1 Installation Overview

1.1 Introduction

The **Kyndryl Resiliency Orchestration** is an industry-leading software product for managing the Enterprise Business Continuity Processes by providing a comprehensive Disaster Recovery (DR) solution. The Kyndryl Resiliency Orchestration automates DR workflows by inter-operating with several industry-leading Databases, Replications, and Cluster Products.

The Kyndryl Resiliency Orchestration Application supports a wide range of operating systems, databases, and their replication schemas. You can choose any of the supported operating systems and databases to customize your disaster recovery solution for your specific business requirements.

1.2 Software Package Components

Find information about the components in the Kyndryl Resiliency Orchestration Software Package that you can choose to install. For downloading instructions, see *Downloading the Software Package*.

1.2.1 Resiliency Orchestration Server

The Kyndryl Resiliency Orchestration Server contains the application binaries that set up the Kyndryl Resiliency Orchestration GUI, the Kyndryl Resiliency Orchestration Remote Agents, the Kyndryl Resiliency Orchestration Web Services, the associated libraries, and other application files. The Server component of the Kyndryl Resiliency Orchestration Product needs to be installed on the server hardware.

Before you install the Kyndryl Resiliency Orchestration Server, you must prepare the server hardware with the supported RHEL operating system and then install the MariaDB database software.

> **Note**
>
> This is mandatory software that you must download and install as part of the Kyndryl Resiliency Orchestration DR Solution.

1.2.2 Kyndryl Resiliency Orchestration Site Controller (Agent Node)

The Agent Node also called the Site Controller, hosts the necessary or applicable Agents to manage the Endpoints remotely. The Site Controller manages the Agents for Kyndryl Resiliency Orchestration by optimizing the communication between an Agent and the Kyndryl Resiliency Orchestration Server.

The Site Controller augments by acting as a gateway for the set of agents for communicating with the Kyndryl Resiliency Orchestration Server.

kyndryl

> **Note**
>
> This is mandatory software that you must download and install as part of the Kyndryl Resiliency Orchestration DR Solution.

1.2.3 Kyndryl Resiliency Orchestration Agents

The Agents play a vital role in monitoring and managing the Endpoints and the applications on the Endpoints. The Kyndryl Resiliency Orchestration Agents are specifically designed to manage applications, components, datasets, and the protection or replication schemas that are hosted on the Production or Primary Endpoints. The same Agents are used to manage the DR Endpoints too. The Agents are collectively managed by the Kyndryl Resiliency Orchestration Site Controller.

If the Agents are installed in the Endpoint hardware, then they are called Local Agents (the agents are Local to the PR or DR Endpoint). If the Agents are installed in the node where the Kyndryl Resiliency Orchestration Server is installed, then they are called Remote Agents (the agents are remote to the PR or DR Endpoint).

> **Note**
>
> This is optional software that you can download and install if you want to install Agents as Local Agents, in the Kyndryl Resiliency Orchestration DR Solution.

1.2.4 Kyndryl Resiliency File Replicator

The Resiliency File Replicator is an enterprise replication software developed by Kyndryl. The Resiliency File Replicator can be used to replicate data (files and directories) across hosts connected within Local or Remote locations. It works with both Local Area Network (LAN) and Wide Area Network (WAN). It can transfer files between any network-shared drives and across heterogeneous platforms. Resiliency File Replicator supports one-to-one, one-to-many, and many-to-one configurations.

> **Note-**
>
> This is optional software provided as free-of-charge software that you can download and install if you want to use this application for File Replication. Refer to the Kyndryl Resiliency File Replicator Installation guide for detailed installation procedures. Refer to the Kyndryl Resiliency File Replicator User guide for usage instructions.

1.3 Downloading the Software Package

1.3.1 Software Versions

1.3.1.1 Licensed Version

You can download the licensed versions of the Kyndryl Resiliency Orchestration software that is available on the *Kyndryl Passport Advantage* (PA) Portal. (https://www-01.ibm.com/software/passportadvantage/)

1.3.1.2 Software Fixes and Updates

You can also download the Kyndryl Resiliency Orchestration software fixes and updates that are available on the Kyndryl Fix Central Portal (https://www-945.ibm.com/support/fixcentral/).

1.3.2 Software Packages

The Kyndryl Resiliency Orchestration Software package contains the following components:

a. Kyndryl Resiliency Orchestration Server (Server)
b. Kyndryl Resiliency Orchestration Site Controller (Agent Node)
c. Kyndryl Resiliency Orchestration Agents (Agents)
d. Kyndryl Resiliency File Replicator (SFR)
e. Kyndryl Resiliency Block Replicator
f. KyndrylRBR VIB
g. Data Mobility Console (DMC)

Note:

The name in parentheses above indicates the name used in the software package. Ensure that you choose the version of the Service or Fix Pack you want to download and then, select all of the components for that version to download.

Java versions used in Kyndryl Resiliency Orchestration

Information about the versions of Java that are used in Kyndryl Resiliency Orchestration Software packages is listed in *Table 1*.

Note: For RO Version 8.3.8 onwards, jdk continues to be bundled and shipped with RO. The local version of the installed jdk is to be used by RO only for AIX agents.

Table 1. Java versions used in Kyndryl Resiliency Orchestration Software package

Java Version	Operating System Version	Remarks

OpenJDK Runtime Environment (Zulu 8.76.0.17-CA-linux64) (build 1.8.0_402-b06)	Windows 2016,2019,2022 Red Hat Enterprise Linux release 9.2 All supported OS and versions except HPUX	Kyndryl Resiliency Orchestration Server / Site Controller/Local Agent

kyndryl

Scope of this Document

The Kyndryl Resiliency Orchestration Installation Guide provides the installation and configuration procedures for the following components that are available in the Software Package:

a. Kyndryl Resiliency Orchestration Server
b. Kyndryl Resiliency Orchestration Site Controller
c. Kyndryl Resiliency Orchestration Agents (Agents)

Note:

The installation procedures for the Kyndryl Resiliency File Replicator are not documented in this document. For the installation procedures for Kyndryl Resiliency File Replicator, refer to the latest *Kyndryl Resiliency File Replicator Installation Guide.*

For the procedures to upgrade to the latest versions of the Kyndryl Resiliency Orchestration Application software and its components, refer to the latest *Kyndryl Resiliency Orchestration Upgrade Guide*.

kyndryl

2 System Requirements

Find information about the minimum system requirements to install the different software components in the Kyndryl Resiliency Orchestration Package.

1. System requirements for Kyndryl Resiliency Orchestration Server. For details, see *System Requirements for Kyndryl Resiliency Orchestration Server*.
2. System requirements for installing the Local Agents. For details, see System requirements for Installing Local Agents.
3. System requirements for installing the SFR. For details, see System requirements for Installing Resiliency File Replicator (SFR).

2.1 System Requirements for Kyndryl Resiliency Orchestration Server and Kyndryl Resiliency Orchestration HA Server

2.1.1 Supported Endpoints for Various Deployment Scenarios

The scalability of the Resiliency Orchestration server depends on the number of production endpoints. The following are the supported number of production endpoints by the Resiliency orchestration Server for various scenarios, as shown in *Table 2*.

Table 2: Supported Number of Production Endpoints by Resiliency Orchestration Server

Resiliency Orchestration Server Deployment Scenarios	Number of Supported Production Endpoints
DR / Cyber Data / DR with Cyber Data	3000
Cyber Platform	2000
DR and Cyber Platform / Cyber Data and Cyber Platform / DR and Cyber Data and Cyber Platform	1000

Note

There is no impact on Resiliency Orchestration server scalability with only the DR scenario.

There is no impact on Resiliency Orchestration server scalability with the introduction of Cyber Data.

The scale for Cyber Data Platform configuration has been verified up to 2000 endpoints. There is a cascading effect on Cyber Platform with DR use case also.

kyndryl

Work is in progress to verify the scale to 3000 endpoints to match the DR/Cyber Data use case.

The following are highlights of the sizing guidelines:

- Every Resiliency Orchestration Server can be co-hosted with the Site Controller. Need additional Site Controllers beyond 250 production agentless endpoints
- Additional Site Controller is always required for managing agentless endpoints as the co-hosted Site Controller cannot manage windows agentless endpoints
- Agent-based endpoints can be handled through co-hosted Resiliency Orchestration for the supported number of endpoints (Linux and windows). Additional Site Controller is needed for Remote agents only as per the guideline
- An additional server component (Staging Server) is required for the Cyber platform. The Staging Server can be co-hosted on the Site Controller
- Site Controller is applicable per site. The user can have any deployment model, and based on that the Site Controller requirement changes. Refer to *Table 3* for details.

Table 3: Deployment Model

Sl No.	Deployment Model
1	2-site for DR only
2	2-site for DR + CR data
3	2-site for DR + CR data + CR platform
4	2-site for DR + CR platform
5	3-site where 2nd site for DR and 3rd site for CR data
6	3-site where 2nd site for DR and 3rd site for CR platform

2.1.2 Kyndryl Resiliency Orchestration Server and Site Controller Sizing Guidelines

The system requirements are defined based on the number of endpoints, which need to be managed. An endpoint is a server used for production irrespective of the physical or logical sites it spans. It can be a VM, a hypervisor, a server running applications or software, and requires to be protected.

The Site Controller is mandatory for production deployments of Kyndryl Resiliency Orchestration. The site Controller is a facilitator between agents and Kyndryl Resiliency Orchestration Server. Therefore, when the Site Controller is down, agents are not available, and hence monitoring and management of DR are compromised for the endpoints managed by that Site Controller. The site controller can manage its agents when the Site Controller is installed within LAN. It helps in reducing bandwidth usage as the communication over WAN to Kyndryl Resiliency Orchestration Server is greatly reduced.

You can install the Site Controller in the following locations:

i. Co-hosted with the Kyndryl Resiliency Orchestration. The Site Controller is installed in the same hardware in which the Kyndryl Resiliency Orchestration Server is installed. Please note that it is mandatory to use the Linux-based Site Controller for installation if you are co-hosting the Site Controller along with the Kyndryl Resiliency Orchestration.

ii. Prerequisites to installing the co-hosted site controller:

iii. The site controller binary has to be installed in the RO server in a different directory other than the server installation directory.
    1. **Example:** If sever binary is installed on /opt/panaces then site controller should be installed /opt/SiteController.

iv. To install the site controller binary on the same server, different IP should be used for the site controller installation.
    1. **Note:** RO server and SC should not be configured with the same IP if installed in the same hardware.

v. Hosted independently of the Kyndryl Resiliency Orchestration. The Site Controller is installed on a separate server and its location is independent of the Kyndryl Resiliency Orchestration Server location. You can use either the Linux-based or Windows-based Site Controller for installation if you are hosting the Site Controller independently of the Kyndryl Resiliency Orchestration.

vi. The AIX-based solution does not support cohosted Sitecontroller with DMC. The user has to install the DMC RO agent and Windows Site Controller on two separate windows boxes.

The following table displays the recommended Kyndryl Resiliency Orchestration software sizing and Site Controller sizing guidelines applicable for the following use cases:

- DR
- Cyber data

kyndryl

- DR and Cyber data

Table 4: Kyndryl Resiliency Orchestration Software Sizing Recommendation Scenario - 1

Production endpoints[1]	**Kyndryl Resiliency Orchestration Server**[2] **(with cohosted Site Controller)**	**Additional Linux Site Controllers**[2]	**Windows Site Controllers**[3]
		Additional Linux Site Controllers and Windows Site Controllers might be needed to manage endpoints agentless	
	CPU = Intel Xeon (2.6 Ghz Dual Core)	Needed in each site for Unix/Linux endpoints	Needed in each site for Windows endpoints
1 to 50	CPU: 6 cores Disk: 150 GB RAM: 16 GB Disk1: 50 GB for binaries/logs Disk2: 50 GB for MariaDB Disk3: 50 GB for site controller	1 X [CPU : 2 Cores, RAM : 16 GB, Disk : 50 GB]	1 X [CPU : 2 Cores, RAM : 16 GB, Disk : 50 GB]
50 to 100	CPU: 6 cores Disk: 250 GB RAM: 24 GB Disk1: 100 GB for binaries/logs Disk2: 50 GB for MariaDB Disk3: 100 GB for site controller	1 X [CPU : 2 Cores, RAM : 16 GB, Disk : 100 GB]	1 X [CPU : 2 Cores, RAM : 16 GB, Disk : 100 GB]
100 to 250	CPU: 8 cores Disk: 350 GB		

kyndryl

Production endpoints[1]	Kyndryl Resiliency Orchestration Server[2] (with cohosted Site Controller)	Additional Linux Site Controllers[2]	Windows Site Controllers[3]
	RAM: 40 GB Disk1: 150 GB for binaries/logs Disk2: 50 GB for MariaDB Disk3: 150 GB for site controller	1 X [CPU : 4 Cores, RAM : 32 GB, Disk : 200 GB]	1 X [CPU : 4 Cores, RAM : 32 GB, Disk : 200 GB]
250 to 500	CPU: 12 cores Disk: 500 GB RAM: 48 GB Disk1: 250 GB for binaries/logs Disk2: 100 GB for MariaDB Disk3: 150 GB for site controller	1 X [CPU : 4 Cores, RAM : 32 GB, Disk : 200 GB]	1 X [CPU : 4 Cores, RAM : 48 GB, Disk : 350 GB]
500 to 1000	CPU: 12 cores Disk: 600 GB RAM: 64 GB Disk1: 350 GB for binaries/logs Disk2: 100 GB for MariaDB Disk3: 150 GB for site controller	1 X [CPU : 4 Cores, RAM : 72 GB, Disk : 500 GB]	1 X [CPU : 6 Cores, RAM : 96 GB, Disk : 700 GB]
1000 to 2000	CPU: 12 cores Disk: 850 GB RAM: 64 GB		

kyndryl

Production endpoints[1]	Kyndryl Resiliency Orchestration Server[2] (with cohosted Site Controller)	Additional Linux Site Controllers[2]	Windows Site Controllers[3]
	Disk1: 500 GB for binaries/logs	2 X [CPU : 6 Cores, RAM : 96 GB, Disk : 700 GB]	2 X [CPU : 6 Cores, RAM : 96 GB, Disk : 700 GB]
	Disk2: 200 GB for MariaDB		
	Disk3: 150 GB for site controller		
2000 to 3000	CPU: 16 cores	3 X [CPU : 6 Cores, RAM : 96 GB, Disk : 700 GB]	3 X [CPU : 6 Cores, RAM : 96 GB, Disk : 700 GB]
	Disk: 1 TB		
	RAM: 96 GB		
	Disk1: 650 GB for binaries/logs		
	Disk2: 200 GB for MariaDB		
	Disk3: 150 GB for site controller		

Note: Either cohosted SC or SC is required and not both of them.

The following table displays the recommended Kyndryl Resiliency Orchestration Software sizing and Site Controller sizing guidelines applicable for the following use cases:

- DR and Cyber platform
- Cyber data and Cyber platform
- DR, Cyber data, and Cyber platform

Table 5: Kyndryl Resiliency Orchestration Software Sizing Recommendation Scenario - 2

kyndryl

Production endpoints[1]	Kyndryl Resiliency Orchestration Server[2] (with cohosted Site Controller)	Additional Linux Site Controllers[2]	Windows Site Controllers[3]
		Additional Linux Site Controllers and Windows Site Controllers might be needed to manage endpoints agentless	
	CPU = Intel Xeon (2.6 Ghz Dual Core)	Needed in each site for Unix/Linux endpoints	Needed in each site for Windows endpoints
1 to 50	CPU: 6 cores Disk: 150 GB RAM: 16 GB Disk1: 50 GB for binaries/logs Disk2: 50 GB for MariaDB Disk3: 50 GB for site controller	1 X [CPU: 2 Cores, RAM : 16 GB, Disk: 50 GB]	1 X [CPU: 2 Cores, RAM : 16 GB, Disk: 50 GB]
50 to 100	CPU: 6 cores Disk: 250 GB RAM: 24 GB Disk1: 100 GB for binaries/logs Disk2: 50 GB for MariaDB Disk3: 100 GB for site controller	1 X [CPU : 2 Cores, RAM : 16 GB, Disk : 100 GB]	1 X [CPU : 2 Cores, RAM : 16 GB, Disk : 100 GB]
100 to 250	CPU: 8 cores Disk: 350 GB RAM: 40 GB Disk1: 150 GB for	1 X [CPU : 4 Cores, RAM : 32 GB, Disk : 200 GB]	1 X [CPU : 4 Cores, RAM : 32 GB, Disk : 200 GB]

kyndryl

Production endpoints[1]	Kyndryl Resiliency Orchestration Server[2] (with cohosted Site Controller)	Additional Linux Site Controllers[2]	Windows Site Controllers[3]
	binaries/logs Disk2: 50 GB for MariaDB Disk3: 150 GB for site controller		
250 to 500	CPU: 12 cores Disk: 500 GB RAM: 48 GB Disk1: 250 GB for binaries/logs Disk2: 100 GB for MariaDB Disk3: 150 GB for site controller	1 X [CPU : 4 Cores, RAM : 32 GB, Disk : 200 GB]	1 X [CPU : 4 Cores, RAM : 48 GB, Disk : 350 GB]
500 to 1000	CPU: 12 cores Disk: 600 GB RAM: 64 GB Disk1: 350 GB for binaries/logs Disk2: 100 GB for MariaDB Disk3: 150 GB for site controller	1 X [CPU : 4 Cores, RAM : 72 GB, Disk : 500 GB]	1 X [CPU : 6 Cores, RAM : 96 GB, Disk : 700 GB]

Note: Either cohosted SC or SC is required and not both of them.

kyndryl

To support the cyber platform use case, an additional server component (staging server) is required which can be hosted on the Site Controller. In the case of cohosted Site Controller, the staging server should be provisioned separately as it cannot be hosted on Kyndryl Resiliency Orchestration Server.

The following table displays details of the recommended size for the staging server:

Table 5b: Recommended size for Staging Server

Production endpoints[1]	**Staging Server[3]**
	Needed for Linux and Window
1 to 1000	1 X CPU: 2 cores Disk: 50 GB RAM: 16 GB

The following table displays the recommended Resiliency Orchestration Software sizing and Site Controller sizing guidelines applicable for the following use case:

- Cyber Platform only

Table 6: Resiliency Orchestration Software Sizing Recommendation Scenario - 3

Production Endpoints[1]	**Kyndryl Resiliency Orchestration Server**	**Staging Server**
	CPU = Intel Xeon 2.6 Ghz Dual Core	For both Windows/Linux

1 to 50	CPU: 6 cores Disk: 150 GB RAM: 16 GB Disk1: 50 GB for binaries/log Disk2: 50 GB for MariaDB Disk3: 50 GB for site controller	1 x CPU: 2 cores Disk: 50 GB RAM: 16 GB
50 to 100	CPU: 6 cores Disk: 250 GB RAM: 24 GB Disk1: 100 GB for binaries/logs Disk2: 50 GB for MariaDB Disk3: 100 GB for site controller	1 x CPU: 2 cores Disk: 50 GB RAM: 16 GB
100 to 250	CPU: 8 cores Disk: 350 GB RAM: 40 GB Disk1: 150 GB for binaries/logs Disk2: 50 GB for MariaDB Disk3: 150 GB for site controller	1 x CPU: 2 cores Disk: 50 GB RAM: 16 GB
250 to 500	CPU: 12 cores Disk: 500 GB RAM: 48 GB Disk1: 250 GB for binaries/logs Disk2: 100 GB for MariaDB Disk3: 150 GB for site controller	1 x CPU: 2 cores Disk: 50 GB RAM: 16 GB
500 to 1000	CPU: 12 cores Disk: 600 GB RAM: 64 GB Disk1: 350 GB for binaries/logs Disk2: 100 GB for MariaDB Disk3: 150 GB for site controller	1 x CPU: 2 cores Disk: 50 GB RAM: 16 GB
1000 to 2000	CPU: 12 cores Disk: 850 GB RAM: 64 GB Disk1: 500 GB for binaries/logs Disk2: 200 GB for MariaDB Disk3: 150 GB for site controller	1 x CPU: 2 cores Disk: 50 GB RAM: 16 GB

[1]Every Kyndryl Resiliency Orchestration Server should always be cohosted with the Site Controller. Need additional Site Controllers beyond 250 production endpoints agentless

[2]Cohosted Site Controller is adequate to manage agent-based Linux/Windows production endpoints as supported in Kyndryl Resiliency Orchestration

[3]The Staging Server can be hosted on the same Kyndryl Site Controller Server

[4]Avgerage Configuration per endpoints is 10

Kyndryl Resiliency Orchestration Server Guidelines: The following are Kyndryl Resiliency Orchestration Server guidelines:

Disk1: For binaries and debug logs
Disk2: For MariaDB with 6 months history of retention
Disk3: For co-hosted site controller
Swap: 2 times the RAM size
OS-specific RHEL standard partitioning structure

Site Controller Sizing/Guidelines: The following are Site Controller sizing/guidelines:

Memory: 3 + 0.09 * N GB (rounded to multiple of 8)
Disk: 0.7 * N GB for binaries and debug logs
Swap: 2 times RAM size
OS-specific RHEL standard partitioning structure

AD2C Resource Requirements and Deployment Recommendation:

AD2C is deployed where the connectivity between source system and AD2C, RO and AD2C can be established. AAD2C can be deployed in RO or RO Site Controller or a separate Linux Server. Based on the connectivity between Source and RO Systems with AD2C, user must take the decision.

Consider the following software and hardware requirements for AD2C:

Software Pre-requisites on the AD2C Server Machine

Software	Supported Versions
RHEL	8.x, 9.x
Podman	4.x.x or higher. Note: For RHEL 8.0 and higher versions, Podman is available by default.
conmon	2.1.x or later Note: conmon should be available on the server before AD2C is installed.

Hardware Requirements

15 GB space must be available in the user home directory (/home/<user>) for installing AD2C. The size of the AD2C installer can be around 1.2 GB.

Note:

- It is recommended to deploy AD2C on Linux SC servers.

2.1.3 System requirements for Installing Local Agents

The Kyndryl Resiliency Orchestration Agents to be installed on the endpoint requires 256 MB memory and 10 GB disk space.

2.1.4 System requirements for Installing Resiliency File Replicator (SFR)

Find the minimum system requirements for installing the optional software, Kyndryl Resiliency File Replicator (SFR) on the Endpoints.

- The SFR application to be installed on the Endpoint requires 1.25 GB of memory and 10 GB of disk space.

2.2 System Requirements for Staging Server

- Staging is similar to an endpoint managed and therefore, the standard configuration settings for an endpoint can be used for Staging Server.

3 Prerequisites

Before you proceed to download and install the Kyndryl Resiliency Orchestration software, ensure that you have read and complied with the prerequisites.

Table 7. Prerequisites

Prerequisite	Mandatory (Yes or No)	Remarks
Installing the GPL Dependencies	Yes	Before you install the Kyndryl Resiliency Orchestration Server, you must install the GPL Licenses.
Installing the MariaDB	Yes	Before you install the Kyndryl Resiliency Orchestration Server, you must install the MariaDB and configure it.
Installing the Apache Tomcat	Yes	Before you install the Kyndryl Resiliency Orchestration Server, you must install the Apache Tomcat and configure it.

3.1 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*.

For more information about the GPL licenses, see *GPL License Information*.

3.2 Supported Operating System, Database Platforms, and Web Server

Table 8. Supported Versions of Different Components and platforms

Server and Components	Operating System Platform	Database Platform	Web Server
	RHEL 9.3 (Plow)	Maria DB: 10.5.22,10.5.24	Apache Tomcat 9.0.83, 9.0.84, 9.0.85,9.0.86
	RHEL 9.2 (Plow)	Maria DB: 10.5.22	Apache Tomcat 9.0.82
Kyndryl Resiliency Orchestration Server	RHEL 9.2 (Plow)	Maria DB: 10.5.21	Apache Tomcat 9.0.80
	RHEL 9.2 (Plow)	Maria DB: 10.5.21	Apache Tomcat 9.0.78
	RHEL 9.1	MariaDB 10.5.20	Tomcat 9.0.73
	RHEL 9.0	MariaDB 10.5.18	Tomcat 9.0.68
	RHEL 7.9, 8.3, 8.4, 8.5, 8.6	MariaDB 10.5.9	Tomcat 9.0.54
	RHEL 7.5, 7.6, 7.7, 7.8, 8.0, 8.1, 8.2, 8.6	MariaDB 10.3.25	Tomcat 9.0.54
Site Controller	RHEL 7.6, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 9.0, 9.1, 9.2 Windows 2016,	Not applicable	Not applicable

Server and Components	Operating System Platform	Database Platform	Web Server
	Windows 2019, Windows 2022		
Local Agents	RHEL 7.6, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 9.0, 9.1 Windows 2016, Windows 2019	Not applicable	Not applicable

Note: **Characters limit for the command/script that can be set for the workflow action. The limit of the characters depends on the OS.**

1. For Linux start with RO version 8.1.2. limit is 4K characters.

2. If the RO version is older than 8.1.2, then the limit is 256 and for Windows, due to OS restrictions, the max length remains 256 characters.

3.2.1 Agent Supportability

Kyndryl Resiliency Orchestration agents can be configured to run either as local agents on the components or as remote agents on the Site Controller server. Kyndryl Resiliency Orchestration solutions come with either local agent support, remote agent support, or both models. The information about the Kyndryl Resiliency Orchestration solutions and their supported agent model is listed below:

- MS Exchange, Sybase, and Kyndryl CSM solutions are supported only with the local agent model.
- MIMIX, SAP HANA, zOS, and Hitachi Replication (Windows) solutions are supported only with the remote agent model.
- The "*DB2 Protection with HADR*" solution signature supports both local and remote agent models.

- All Management Services have remote agent support, except Resiliency Block Replicator which has local agent support.
- For all the other solutions, the remote agent model is the default model however local agents are also available for use.

For the details about the supported versions of OS and databases for the solutions, please refer to the latest Kyndryl Resiliency Orchestration Interop List.

3.2.2 Supported Browsers

The following browser versions are supported for Kyndryl RO.

Supported Browser	Version
Google Chrome	122.0.6261.69 (Official Build) (64-bit)
Microsoft Edge	122.0.2365.59 (Official build) (64-bit)
Mozilla Firefox	122.0.1 (64-bit)

Note

Kyndryl Resiliency Orchestration GUI does not support multiple tabs or multiple windows for pages that require user inputs such as Discovery or configuration for the single logged-on session and Group assignment for a particular user.

It is highly recommended that the autocomplete feature is disabled for all supported browsers. Additionally, in case this feature was not disabled previously, ensure that the autocomplete history is deleted. Please refer to the respective browser's documentation to disable the autocomplete feature and delete the history.

kyndryl

3.3 Ports used by RO/SC/Agents

3.3.1 Ports that are opened on RO Server by RO processes

Port	Protocol	Security	Visibility*	Opened by	Used by	Remarks
8443	HTTPS	TLS 1.2	EXTERNAL	RO Web Application running on TOMCAT	Users of RO GUI	The cipher list is restricted to the recommended white list as per OWASP guidelines, that is **OWASP Cipher String 'B'** (Broad compatibility to browsers). Refer to 'OWASP TLS Cipher String Recommendations
42443	TCP	TLS 1.2	EXTERNAL	RO Message Broker - ActiveMQ	Site Controllers	Agent messages are received via SC.
45443	TCP	TLS 1.2	EXTERNAL	RO Application Server	Agents	Agents connect to RO on this port to exchange messages. Agents connecting to RO directly is NOT recommended. Instead, Agents must connect via SC - however, this port is retained on RO for special cases.
8162	HTTPS	TLS 1.2	EXTERNAL for DEBUG purpose	RO Message Broker - ActiveMQ Admin Web Console on JETTY	Support users for debug Purposes	ActiveMQ comes with an Admin console that is used for debugging purposes only.

kyndryl

Port	Protocol	Security	Visibility*	Opened by	Used by	Remarks
8081	HTTP	-	EXTERNAL for Low-touch Local Agent Upgrade	RO Content Repository - on JACKRABBIT	Local Agents	Is used ONLY if a low-touch upgrade of Local agents is required
1099	RMI	SSL	INTERNAL	RO Application Server	RO GUI and Shell scripts	RO GUI makes Secure RMI calls to serve some web page content
8082	HTTP	-	INTERNAL	RO Application Server REST APIs - on JETTY	RO GUI and Shell scripts	RO GUI invokes REST API to server some web page content
8083	RMI	-	INTERNAL	RO Content Repository - on JACKRABBIT	JACKRABBIT internal usage	-
2099	RMI	-	INTERNAL	RO Message Broker - ActiveMQ RMI port	ActiveMQ internal usage	-
8009	Apache JServ Protocol (AJP)	-	Internal	RO Web Application running on TOMCAT	For internal use	Port used for communication between Tomcat and Apache web server.
8444	HTTPS	TLS1.2	External (if required by REST API clients)	RO Application Server	REST API clients	Optional port.
8005	-	-	Internal	RO Web Application running on	Used by administrators to shut sown	None.

Port	Protocol	Security	Visibility*	Opened by	Used by	Remarks
				Tomcat server.	Tomcat server.	

*Where a port is marked as INTERNAL, network controls must be applied to restrict access within the Server and NOT outside. Where a port is marked as EXTERNAL, review the **Used by** column, and network controls must be applied to restrict only to those entities who need it.

3.3.2 Ports that are opened on SC Server by SC processes

Port	Protocol	Security	Visibility*	Opened by	Used by	Remarks
42443	TCP	TLS 1.2	EXTERNAL	SC Message Broker - ActiveMQ	RO	RO messages intended for the SC and Agents connected via the SC
45443	TCP	TLS 1.2	EXTERNAL	SC Process	Agents	Agents connect to SC on this port to exchange messages.
8162	HTTPS	TLS 1.2	EXTERNAL for DEBUG purpose	SC Message Broker - ActiveMQ Admin Web Console on JETTY	Support users for debug Purposes	ActiveMQ comes with an Admin console that is used for debugging purposes only.
2099	RMI	-	INTERNAL	SC Message Broker - ActiveMQ RMI port	ActiveMQ internal usage	-

*Where a port is marked as INTERNAL, network controls must be applied to restrict access within the Server and NOT outside. Where a port is marked as EXTERNAL, review the **Used by** column, and network controls must be applied to restrict only to those entities who need it.

3.3.3 Ports that are opened by Agent processes

None. Agent processes are Local Agents or Remote Agents that do not open any ports. However, they do need ports to be opened on the end points to monitor and manage. Please see the below section on what ports need to be opened on the endpoints.

3.3.4 Ports that are required to be Open on the Endpoints

Local Agents

None. Since local agents run on the actual endpoint all internally visible ports will be used by the Local Agent process.

Remote Agents a.k.a Agentless Agents:

Remote Agents running on Linux SC or RO

Port	Protocol	Security	Visibility*	Opened by	Used by	Remarks
22*	SSH	-	EXTERNAL	Endpoint	Remote Agent running on Linux SC/RO	Standard SSH port

Note: It is **not mandatory,** from RO 8.4.9.0 onwards to open Port 22 for SSH protocol.

*Where a port is marked as EXTERNAL, review the Used by column and apply network controls to restrict access only to those entities.

In addition to the above port, solution-specific ports need to be open for the Remote Agents. For instance, the Oracle DB port must be open to Oracle Agent. Please refer to the Solution Guide for a complete list of ports that must be open to the Remote Agents.

Remote Agents running on Windows SC

Port	Protocol	Security	Visibility*	Opened by	Used by	Remarks
5986	SSH	-	EXTERNAL	Endpoint	Remote Agent	Standard Windows

					running on Windows SC	secure Powershell port

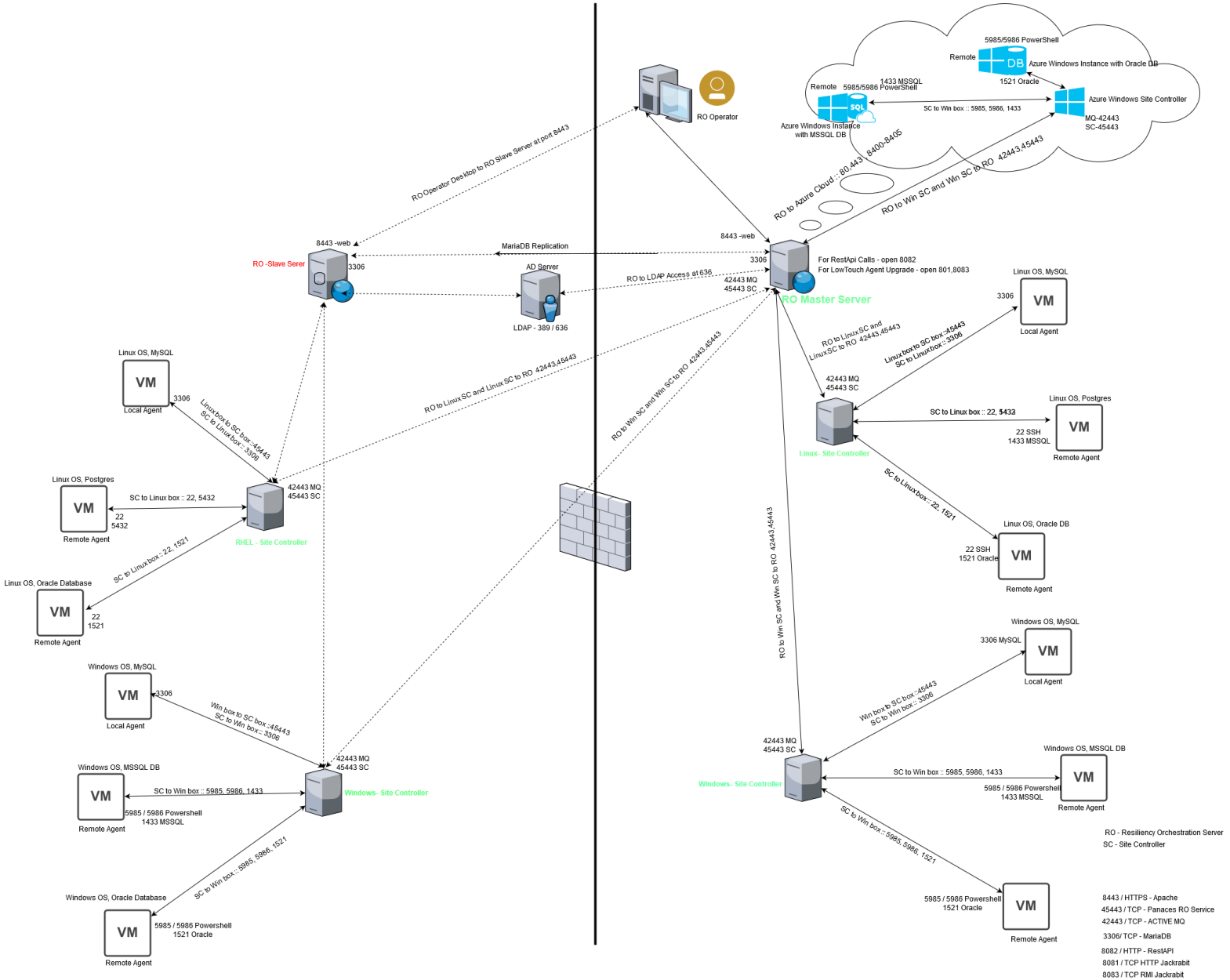
*Where a port is marked as EXTERNAL, review the Used by column and apply network controls to restrict access only to those entities.

In addition to the above port, solution-specific ports need to be open for the Remote Agents. For instance, the MSSQL DB port must be open to MSSQL Agent. Please refer to the Solution Guide for a complete list of ports that must be open to the Remote Agents.

Ports details high level, from RO to SC, SC to Endpoints, etc

<The blank space is appearing so that the image of the next page can be used in a better way>

kyndryl™


RO Operator
RO Operator Desktop to RO Slave Server at port 8443
8443 -web
RO -Slave Serer
3306
MariaDB Replication
AD Server
LDAP - 389 / 636
RO to LDAP Access at 636
8443 -web
3306
For RestApi Calls - open 8082
For LowTouch Agent Upgrade - open 801,8083
RO Master Server
42443 MQ
45443 SC
5985/5986 PowerShell
Remote
Azure Windows Instance with Oracle DB
1521 Oracle
Remote 5985/5986 PowerShell
1433 MSSQL
Azure Windows Instance with MSSQL DB
SC to Win box :: 5985, 5986, 1433
Azure Windows Site Controller
MQ-42443
SC-45443
RO to Azure Cloud :: 80,443, 8400-8405
RO to Win SC and Win SC to RO 42443,45443
Linux OS, MySQL
VM
Local Agent
3306
Linux box to SC box :45443
SC to Linux box :: 3306
RO to Linux SC and Linux SC to RO 42443,45443
RO to Win SC and Win SC to RO 42443,45443
RO to Linux SC and LinuxSC to RO 42443,45443
Linux box to SC box :45443
SC to Linux box :: 3306
Linux OS, Postgres
VM
Remote Agent
22
5432
SC to Linux box :: 22, 5432
42443 MQ
45443 SC
RHEL - Site Controller
Linux- Site Controller
SC to Linux box :: 22, 5432
22 SSH
1433 MSSQL
Linux OS, Oracle Database
VM
Remote Agent
22
1521
SC to Linux box :: 22, 1521
Linux OS, Oracle DB
22 SSH
1521 Oracle
Windows OS, MySQL
VM
Local Agent
3306
Win box to SC box :45443
SC to Win box :: 3306
3306 MySQL
Windows OS, MSSQL DB
VM
Remote Agent
SC to Win box :: 5985, 5986, 1433
5985 / 5986 Powershell
1433 MSSQL
Windows- Site Controller
Windows OS, Oracle Database
VM
Remote Agent
SC to Win box :: 5985, 5986, 1521
5985 / 5986 Powershell
1521 Oracle
RO - Resiliency Orchestration Server
SC - Site Controller
8443 / HTTPS - Apache
45443 / TCP - Panaces RO Service
42443 / TCP - ACTIVE MQ
3306/ TCP - MariaDB
8082 / HTTP - RestAPI
8081 / TCP HTTP Jackrabit
8083 / TCP RMI Jackrabit

4 Preparing the Kyndryl Resiliency Orchestration Server

4.1 Server Hardware

Evaluate the number of Servers you want to set up to host the Kyndryl Resiliency Orchestration Applications, Site Controllers, Kyndryl Resiliency Orchestration Agents, Kyndryl Resiliency Orchestration Database, and Browser.

For determining your system requirements, see the details under *System Requirements*.

Proceed to install the RHEL OS, Kyndryl Resiliency Orchestration Database, and Apache Tomcat on the Server, where you intend to install the Kyndryl Resiliency Orchestration Application Software.

4.2 Installation of RHEL OS

You must install the RHEL Server OS on the Server before installing the Kyndryl Resiliency Orchestration Application Software.

1. Refer to the Linux OS Installation procedures from the official RHEL website, for the instructions for downloading and installing the Linux OS.
2. Install the Linux Enterprise Server OS and ensure to set the following conditions during the installation:
   - Set up the partitions for the different binaries as indicated in the system requirements section. For details, see System Requirements for the Kyndryl Resiliency Orchestration Server.
   - Do not set up the Firewall. Select the **No Firewall** option, during the installation.

4.3 Installation of MariaDB

Refer to the Supported versions of MariaDB for the versions supported.

Download and install the appropriate MariaDB version to be used as the database for Kyndryl Resiliency Orchestration as per the below-listed steps.

Note: The user "sanovireporter" is created by default and does not have any admin privileges. The only grant given to this user is the "select" grant on the VIEWS created in the database.

1. Download the appropriate packages from https://downloads.mariadb.com/MariaDB/
2. Go to the location where MariaDB rpms are downloaded to.
3. Follow the instructions in the README file in the MariaDB rpms folder to install MariaDB. For any additional assistance, please reach out to MariaDB support.
4. Once installed, set the root password of MySQL.

1. #mysqld_safe --skip-grant-tables &
2. #mysql -u root
3. mysql>FLUSH PRIVILEGES;
4. mysql>SET PASSWORD FOR root@'localhost' = PASSWORD('password');

Note: MariaDB service should be owned by mysql user.

```
Last login: Wed Oct 12 13:27:05 2022 from 192.168.255.35
[root@rhel8233 ~]# ps -ef | grep mysql
mysql      1059     1  0 Sep27 ?        00:10:18 /usr/sbin/mysqld
```

4.4 Installation of Apache Tomcat Server

Refer to the Supported versions of Tomcat for the Apache Tomcat version supported. Download the appropriate package of Tomcat to /opt/ from the following link.

https://archive.apache.org/dist/tomcat/

Perform the following steps to install Apache Tomcat:

1. cd /opt/
2. Unzip the apache-tomcat-<version>.tar.gz

   Note - In RHEL 7.9, the unzip utility is not installed by default. You have to install it manually by running the command –

   # yum install zip unzip -y
3. sudo tar -xvzf apache-tomcat-<version>.tar
4. sudo mv apache-tomcat-<version> $TOMCAT_HOME
5. Follow the $TOMCAT_HOME/RUNNING.txt and complete the installation.

When Apache Tomcat is successfully installed, delete the following default files and folders from the $TOMCAT_HOME/webaps path if it exists.

/examples

/docs/

/js-examples

/servlet-example

/webdav

/tomcat-docs

/balancer

/ROOT/admin/nessus-check/default-404-error-page.html

Comment out below line in server.xml of TOMCAT.

<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" prefix="localhost_access_log" suffix=".txt" pattern="%h %l %u %t "%r" %s %b" />.

Removing old log4J jars:

- Remove the older jar file "log4j-1.2.17.jar" from the tomcat folder. Run the following command to find the jar and remove it from the tomcat folder:

```
find $TOMCAT_HOME/lib/ -type f -name "log4j-1.2.17.jar" -exec rm -f {} \;
```

Adding new Log4J2 jars:

Perform the following steps to add new log4j2 jars:

Add the following files in "$TOMCAT_HOME/lib/". Replace the file in case the same file exists.

- log4j-1.2-api-2.17.1.jar
- log4j-api-2.17.1.jar
- log4j-core-2.17.1.jar

Note: The above files are available at EAMSROOT/lib and copy to the TOMCAT library folder.

Note: The default files may vary depending on the Apache Tomcat version.

For more detailed documentation, refer to https://tomcat.apache.org/tomcat-9.0-doc/

If agent logs are not generating

Win SC disconnected from RO and if logs are getting generated

Step 1. Work Around OR Solution for this issue is to copy log4j.xml file from **$EAMSROOT/installconfig** directory to **$EAMSROOT/remote/<IP>/installconfig** directory.

Step 2. restart agent from RO GUI

4.5 Configuring MariaDB

Configure the MariaDB for the following settings:

- Preset Users for MariaDB
- Creating New Users for the MariaDB
- Security Configuration

4.5.1 Preset Users for MariaDB

Kyndryl Resiliency Orchestration uses MariaDB for persistence. During the installation of the Kyndryl Resiliency Orchestration Application Software, the following MariaDB user is created with all privileges:

panaces

The Kyndryl Resiliency Orchestration Application Software is configured to use the panaces User for accessing the MariaDB. You can, however, change the user in the MariaDB. Ensure to change the Preset User to a User of your choice.

4.5.2 Creating New Users in MariaDB

Create new Users and credentials in the MariaDB. Ensure that new Users are set up with all privileges. For instructions about creating a new user in MariaDB, refer to the MariaDB User Guide on the MariaDB website.

Note

Ensure to select the document for the version of the supported MariaDB you installed.

You must use the created User credentials to replace the Kyndryl Resiliency Orchestration Preset user credentials in the Kyndryl Resiliency Orchestration Application files at the time of configuring the installed Kyndryl Resiliency Orchestration Application.

kyndryl

4.5.3 Security Configuration

Kyndryl Resiliency Orchestration Application connects to the MariaDB installed in secure mode (TLS1.2/SSL).

Enable Secure Mode: Maria DB requires server and client key packages to enable this security. The sample CA certificate files available under /opt/panaces/installconfig/mariadbencryption directory.

These key packages (CA certificates) need to be created for each Maria DB Instance for security reasons, refer to the Maria DB Install Guide on the MariaDB website.

If using a custom MariaDB SSL certificate, the custom path should be updated in /etc/my.cnf and $EAMSROOT /installconfig/panaces.properties files,

Example –

If below are the default paths in /etc/my.cnf after installation/upgrade -

[mariadb]

ssl-ca=$EAMSROOT/installconfig/mariadbencryption/ca-cert.pem

ssl-cert=$EAMSROOT/installconfig/mariadbencryption/server-cert.pem

ssl-key=$EAMSROOT/installconfig/mariadbencryption/server-key.pem

and in panaces.properties -

sanovi.server.certificate =

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

Replace these entries with custom paths as mentioned in the example below.

In /etc/my.cnf -

ssl-ca=/var/lib/mysql/mariadbencryption/ca-cert.pem

ssl-cert=/ var/lib/mysql/mariadbencryption/server-cert.pem

ssl-key=/ var/lib/mysql/mariadbencryption/server-key.pem

and in panaces.properties -

sanovi.server.certificate = /var/lib/mysql/mariadbencryption/server-cert.pem

Data at rest encryption: Maria DB requires a "file key management" plugin to support the data at rest encryption.

4.5.3.1 Integration with Vault to store MariaDB keys

Kyndryl Resiliency Orchestration is integrated with Hashicorp Vault Server, which is a secret management tool designed to control access to secrets and passwords. Sensitive information can be secured by storing them in the vault. The information stored can be retrieved from the centralized vault server anytime by authorized users.

The MariaDB secret keys are no longer stored on the local server on which MariaDB is hosted. The vault integration feature hides the sensitive data away in secured vaults and hence provides additional security. These secrets are accessed when the MariaDB services need to be started.

The token method of authentication provided by the Hashicorp vault is used for this integration. It allows users to authenticate using a token.

The vault server setup and upload of the secret keys to the vault server must be done by the security administrator.

To enable centralized vault server integration and retrieve the secret keys from the vault, the following properties should be set in the

$EAMSROOT/installconfig/panaces.properties file.

Note – If the vault server integration is not enabled, the MariaDB secrets required must be on the database server itself.

Note- Below setting are required to establish a Vault connection.

1.Change $EAMSROOT/installconfig/panaces.properties from 30 to 1000:

2. Set the value of panaces.acp.server.concurrentRequestProcessCountMax = 1000

Property Name	Default Value	Description
panaces.security.endpoint.vault.enabled	false	This flag should be set to **true** for enabling the vault integration.

		If this flag is set to **false**, then the vault integration will not be enabled. In that scenario, the other four properties mentioned in this table are not required, and hence can be left blank.
panaces.security.endpoint.vault.serverip	empty	This property value should be set to the vault server's IP address. Example – 127.0.0.1
panaces.security.endpoint.vault.serverport	empty	This property value should be set to the vault port that RO needs to connect to. Example - 8200
panaces.security.endpoint.vault.api	empty	This property should be set to the vault API used to fetch the secret keys. Example - /v1/secret/data/
panaces.security.endpoint.vault.auth_token	empty	This property should be set to the vault authorization token. Example - <Password>

kyndryl

A sample of the panances.properties file is provided below for reference.

#=================Vault Integration for Keys Management ====================

#This property is set to 0 by default, which is a flag for Vault Integration

#This property is used only for using Hashicorp Vault for secrets Management

panaces.security.endpoint.vault.enabled=true

#This property is set to 0 by default, the vault server ip required for Vault Integration

#This property is used only for using Hashicorp Vault for secrets Management

panaces.security.endpoint.vault.serverip=127.0.0.1

#This property is set to 0 by default, the vault service port required for Vault Integration

#This property is used only for using Hashicorp Vault for secrets management

panaces.security.endpoint.vault.serverport=8200

#This property is set to empty by default, the vault service api is required for Vault Integration.

#This property is used only for using Hashicorp Vault for secrets management

panaces.security.endpoint.vault.api=/v1/secret/data/

#This property is set to empty by default, the vault server auth_token is required for Vault Integration.

#This property is used only for using Hashicorp Vault for secrets management

panaces.security.endpoint.vault.auth_token=<Password[1]>

[1]Connect with the Support/Delivery team to get the default passwords.

The following script helps retrieve the MariaDB secret keys from the centralized vault server and start the database. These need to be executed post Resiliency Orchestration server software installation.

One-tier installation -

If Kyndryl Resiliency Orchestration is installed in one-tier mode, execute the below script from the $EMSROOT/installconfig/mariadbencription directory.

```
./startMariaDB_with_Vault.sh
```

The required property values of vault server IP, port number, vault API, and vault auth_token will be picked from the panaces. properties. This script execution requires the public CA key from the vault server to enable the SSL connection.

Two-tier installation -

If Kyndryl Resiliency Orchestration is installed in two-tier mode, then during the execution of the below-mentioned script, the vault server IP, port number, vault API, and vault auth_token will be requested at run-time. Enter the appropriate values at the prompt.

Execute the following script from the $EMSROOT/installconfig/mariadbencription directory.

```
./startMariaDB_with_Vault.sh
```

This script execution requires the public CA key from the vault server to enable the SSL connection.

5 Installing the Kyndryl Resiliency Orchestration Application Software

You can install the Kyndryl Resiliency Orchestration Application Software on a Linux machine and a machine in a Linux Cluster.

5.1 Prerequisites for Installing the Kyndryl Resiliency Orchestration Application Software

1. You should have completed the following installations:
   - Installation of RHEL OS
   - Installation of MariaDB

     Note

     You can either use 1 tier (local host) or 2 tier (dedicated Server) MariaDB setup.

     To migrate existing 1tier DB to 2tier, please refer to the topic Migrating DB Component from Local Host to dedicated Server (GUI mode). For silent mode, click Migrating DB Component from Local Host to dedicated Server in CLI Mode (Split Installation)
   - Installation of the Apache Tomcat Server
2. You must be a root or root equivalent privileged user to install Kyndryl Resiliency Orchestration Application Server.
3. Edit the file **/etc/sysconfig/selinux** to include the option `SELINUX=permissive`.
4. Check **/etc/hosts** file to ascertain if the localhost alias exists or not. If it does not exist, add the `localhost` alias, and the IP address of the Kyndryl Resiliency Orchestration Application Server.

   For Example: `<ip-address><localhost> <hostname>`
5. If you need to use the vault integration feature of the product, confirm that the following required vault integration library files from your vault vendor are available:
   - j2ssh-core-0.2.9.jar
   - javapasswordsdk.jar
   - edmz-par-api.jar

kyndryl

6. You must have downloaded the Kyndryl Resiliency Orchestration Application Software. For details on the software package and downloading procedures, see *Software Package Components* and *Downloading the Software Package*.
7. Ensure `my.conf` file has 644 permission.

Note: For 2-tier/split installation, you will need to follow the below prerequisites.

8. SSH Key gen command to be used on Kyndryl Resiliency Orchestration Server.

```
ssh-keygen -t rsa -m PEM
```

9. A user must be created on a remote DB Server or an existing user account can be used. SSH key-based secure authentication mechanism will be used.
10. Copy the key generated to the DB server using the following command.

```
Ssh-copy-id <db server ip>
```

11. The MYSQL Client should be installed and the mysqladmin file should be present in the Kyndryl Resiliency Orchestration Server.

    Note: Set the mysql and configure the mysqladmin files in the PATH variable.

12. On a remote DB server, the below GRANT command must be run to give remote access (two-tier) to the root user or user with root privileges from the Kyndryl Resiliency Orchestration Server IP/Host Name.

GRANT ALL PRIVILEGES ON *.* TO '<DATABASE_USER_NAME >'@'<RO Server IP>' IDENTIFIED BY '<DATABASE_PASSWORD> ' WITH GRANT OPTION;

GRANT ALL PRIVILEGES ON *.* TO '<DATABASE_USER_NAME >'@'<RO Server hostname>' IDENTIFIED BY '<DATABASE_PASSWORD> ' WITH GRANT OPTION;

13. As an additional authentication mechanism, OS level username and password should also be supported to login and run commands on the DB server.

5.2 Prerequisites for Cyber Resiliency Platform

For prerequisites for Cyber Resiliency Platform, refer to the topic **Prerequisites** in Cyber Incident Recovery for Platform User Guide.

5.3 Mode of installing the Resiliency Orchestration Application Software

You can install the Kyndryl Resiliency Orchestration software by using any of the following methods:

- **Graphical Mode**

Graphical mode installation is an interactive, GUI-based method for installing the Kyndryl Resiliency Orchestration software. You can use the Graphical mode

for installing the Resiliency Orchestration Application Software on Linux, Windows, Solaris, HPUX, and AIX platforms.

- **Silent/Console Mode**

Silent mode installation is a non-interactive method of installing Kyndryl Resiliency Orchestration Software. This method requires the use of a **.properties** file for selecting the installation options. It is supported on Linux, Solaris, HPUX, and AIX platforms.

5.4 Installation of Resiliency Orchestration Server in Graphical Mode

The Kyndryl Resiliency Orchestration Application Software is provided as an image file titled **install.**bin in the Server Package. This package contains all the required binaries and associated software packages to install and run the Kyndryl Resiliency Orchestration Application.

This software installation process includes installing Kyndryl Resiliency Orchestration Server binaries, BCS modules, Kyndryl Resiliency Orchestration Server agents, and other software binaries.

1. Execute either of the following commands, depending on the version of the RHEL OS you are using:

```
sh install.bin
```

or

```
./install.bin
```

Note

1. Java will be installed automatically after the execution of this command.

2. Ensure that free space of approximately 5 GB is available in the server where the Site Controller needs to be installed, before executing the above command. In case the/tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.

Example-

Assuming you want to make /opt/temp as the temporary directory.

#export IATEMPDIR=/opt/temp

After exporting the IATEMPDIR environment variable, proceed with the installation.

2. After extracting the files from the install.bin, the Kyndryl Resiliency Orchestration Server installation starts with the following screen. A progress bar appears at the bottom of the screen indicating that the installer is being loaded.

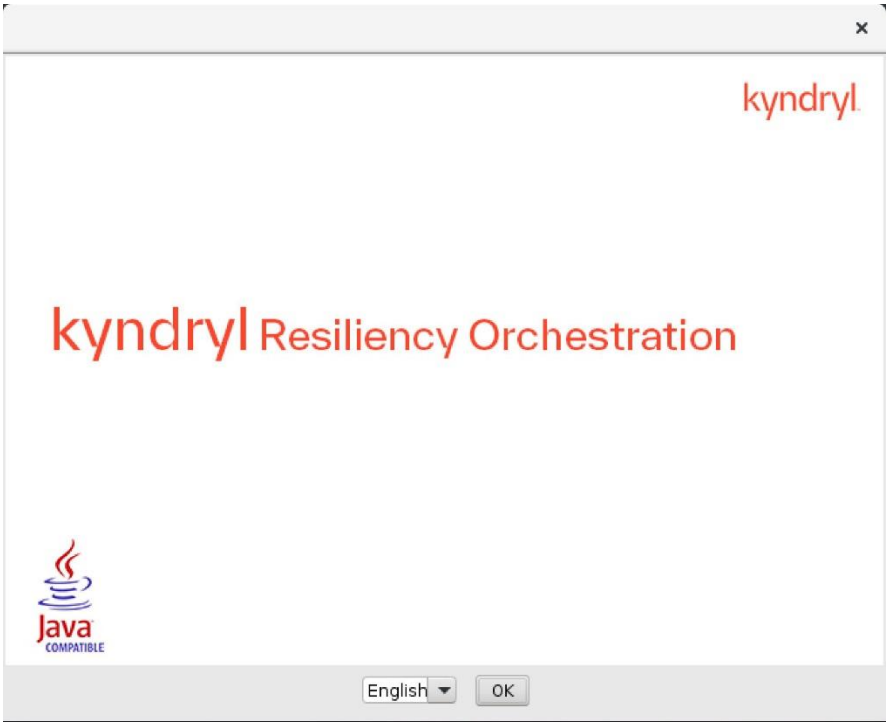


Figure 1: Kyndryl Resiliency Orchestration Installer

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

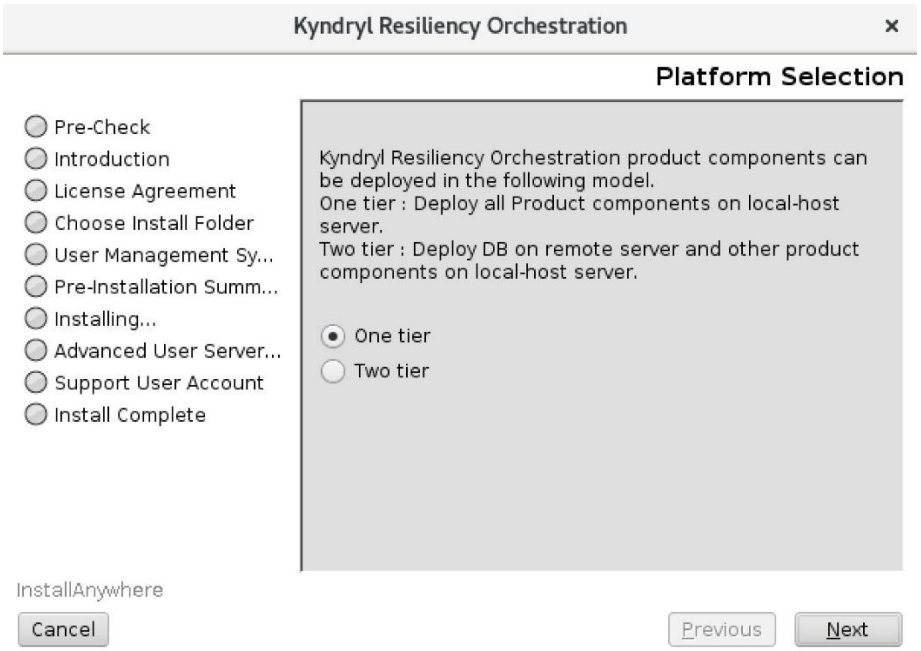


Figure 2: Kyndryl Resiliency Orchestration Server Installation - Platform Selection

4. Refer to the table below and select the appropriate radio button.

Table 8. Platform Selection and Steps to be followed

Radio Button	Description	Steps to Follow
One tier	Select this option to host all components on the local host server.	4.1 through 4.2 below
Two-tier	Select this option and select the MariaDB option to host the DB component on a dedicated server and other components on the local host server.	4.3 through 4.5 below

kyndryl

> **Note**
>
> It is mandatory to select one of the options One Tier or Two Tier. Under Two Tier, the AWS RDS MariaDB option is only applicable when the AWS RDS MariaDB instance is used such as in Cyber Recovery using the AWS Vault solution.

4.1. Select the **One Tier** radio button and then click **Next.** The **Database Access details for single tier** window are displayed for one tier selection.

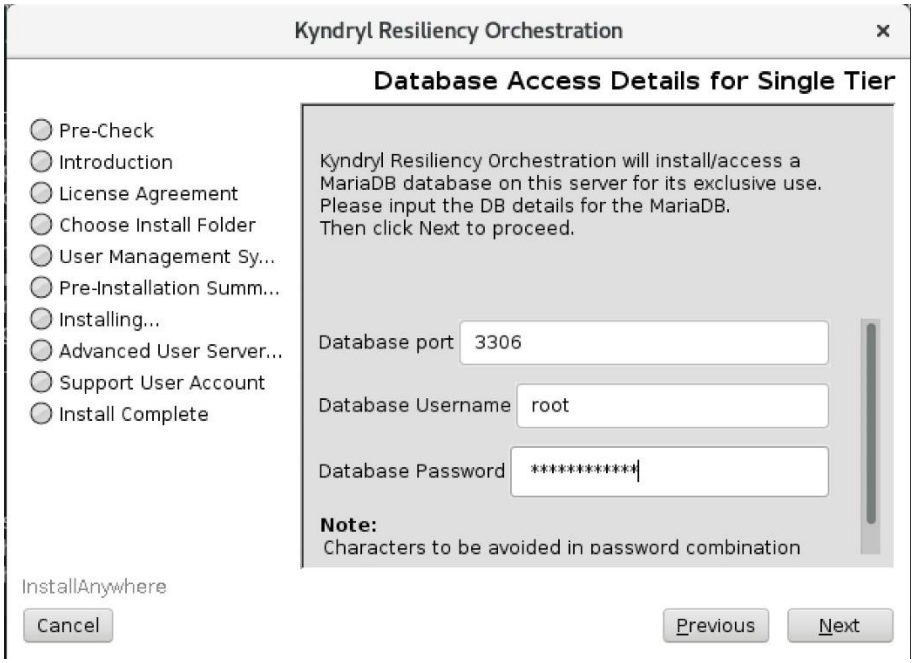


Figure 3: Kyndryl Resiliency Orchestration Server Installation – Database Access Details for Single Tier

4.2. Enter the database port and user details and click **Next**. Skip to step 5 to continue.

4.3. Select the **Two Tier** radio button and select the **MariaDB** radio button as shown in the screenshot below.

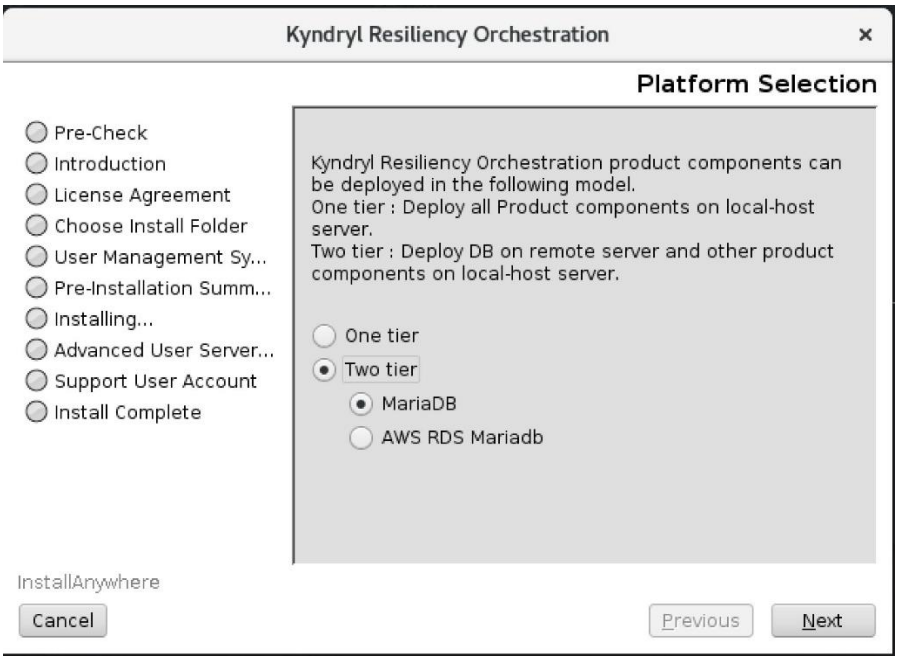


Figure 4 Kyndryl Resiliency Orchestration Platform Selection-Two Tier MariaDB

4.4. Click **Next.** The **Database Access details for the two-tier** window are displayed for two-tier selection.

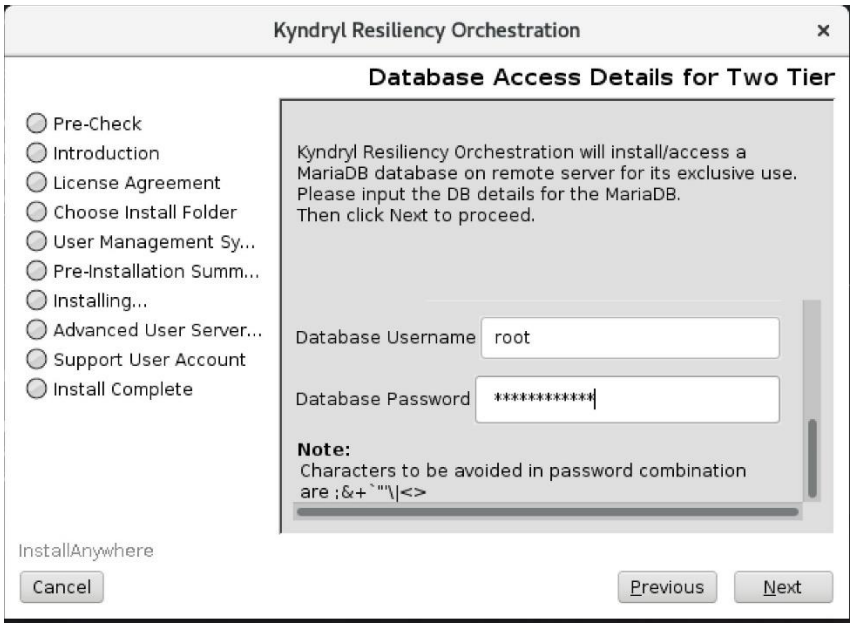


Figure 5: Kyndryl Resiliency Orchestration Server Installation – Database Access Details for Two Tier

4.5. Enter the values for all the fields on the panel.

Table 9. Database Access Details for Two Tier – Field Description

Field	Description
Localhost SSH Private Key	Enter the local host (application server) private key.
Database Host Login User	Enter the DB host server username.
Database host	Enter the database host IP address/host name which could be a fully qualified domain name (FQDN)
Database port	Enter the database port.
Database Username	Enter the database root username.
Database Password	Enter the password for the Database root user.

5. Click **Next**. The **Configure Component Identifier Type (IP/FQDN)** window is displayed.

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

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

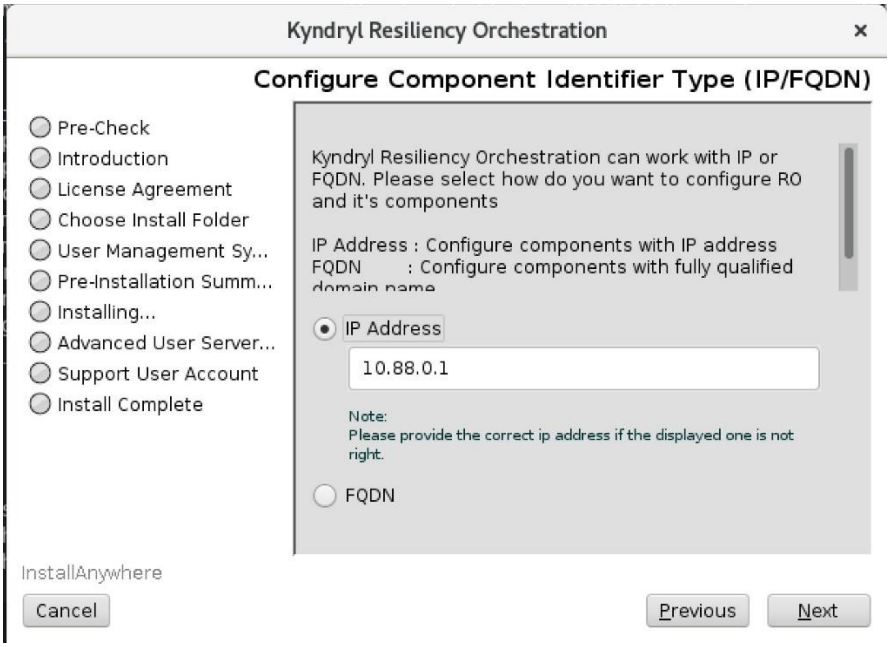


Figure 6: Kyndryl Resiliency Orchestration Server Installation – Configure Component Identifier Type (IP/FQDN) 1

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

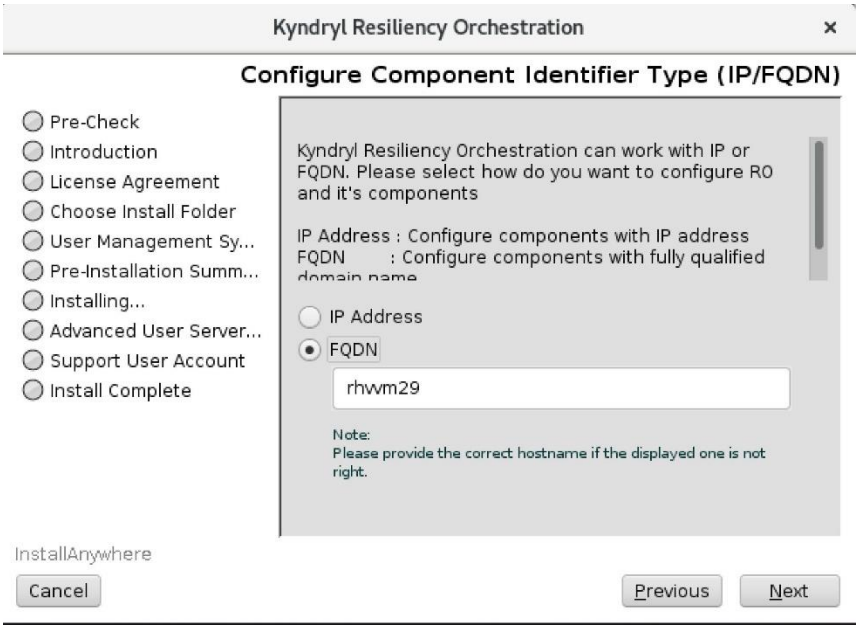


Figure 7: Kyndryl Resiliency Orchestration Server Installation – Configure Component Identifier Type (IP/FQDN)

6. Click **Next**. The **Tomcat Home** window is displayed.

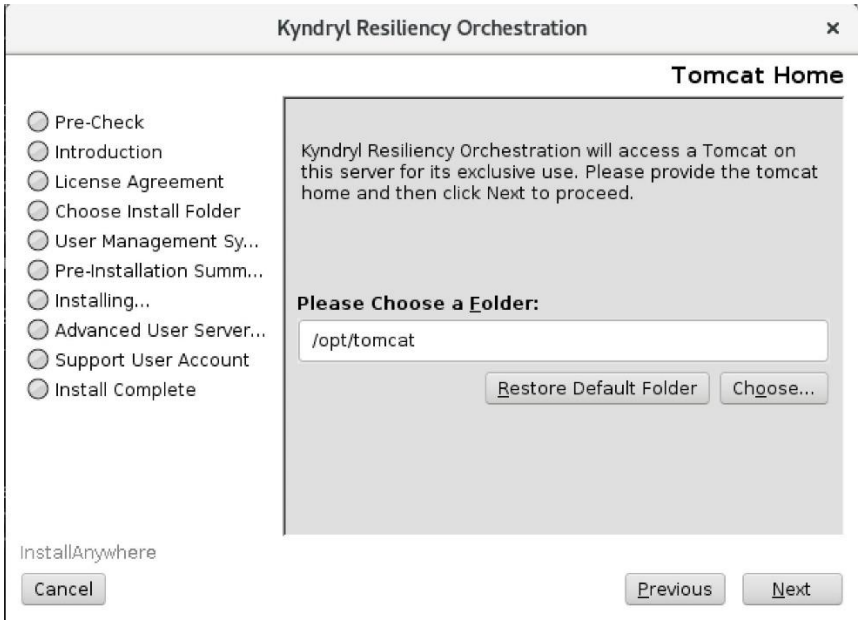


Figure 8: Kyndryl Resiliency Orchestration Server Installation - Tomcat Home

7. 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.

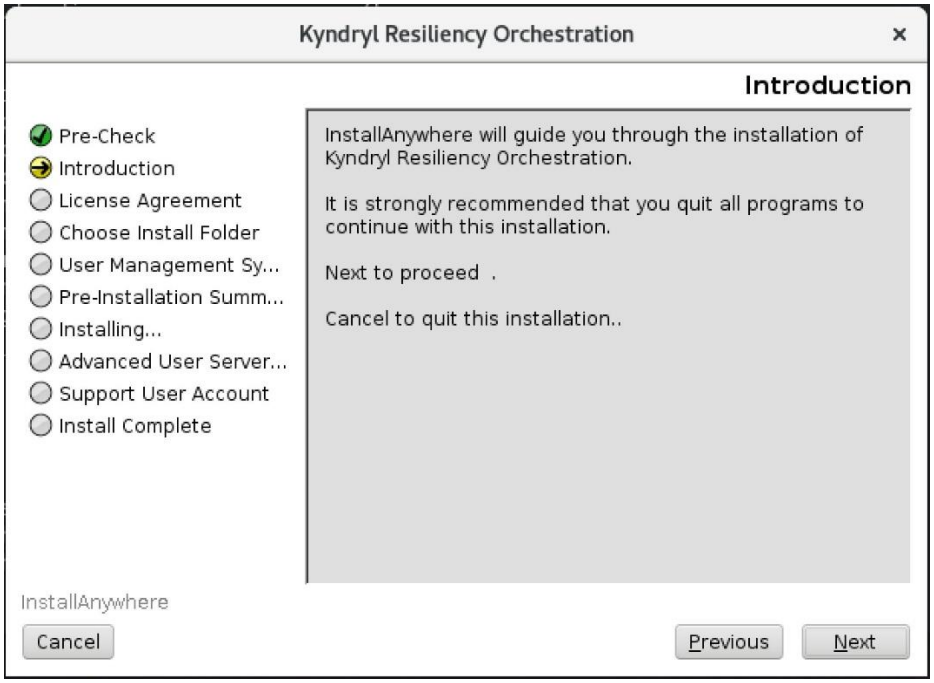


Figure 9: Kyndryl Resiliency Orchestration Server Installation – Introduction Window

8. Click **Next** to continue the installation. The Software License Agreement window is displayed.

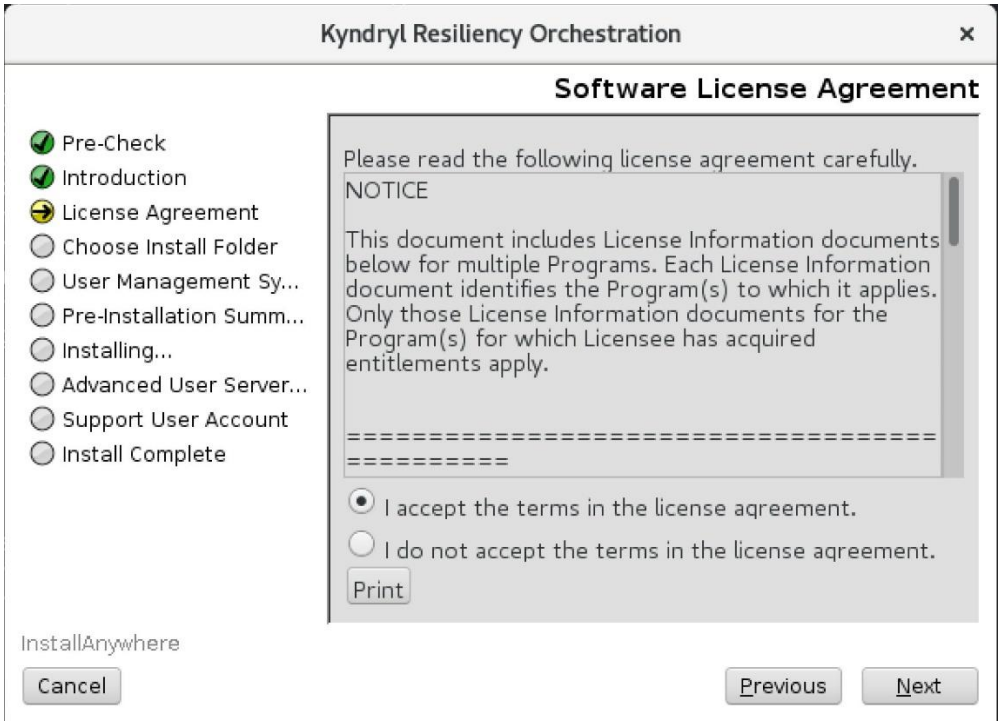


Figure 10: Kyndryl Resiliency Orchestration Server Installation – License Agreement

9. Click the appropriate radio button after you have read through the **License Agreement**.

Table 10: Software License Agreement Options

Radio Button	Description
I accept the terms of the License Agreement	Select this radio button to accept the License Agreement.
I do NOT accept the terms of the License Agreement	Select this radio button to reject the License Agreement and then click **Next**. A pop-up is shown which allows the user to either accept the License Agreement or Quit.

10. Click **Next** after accepting the license agreement to proceed with the installation. The **Choose Install Folder** window is displayed.

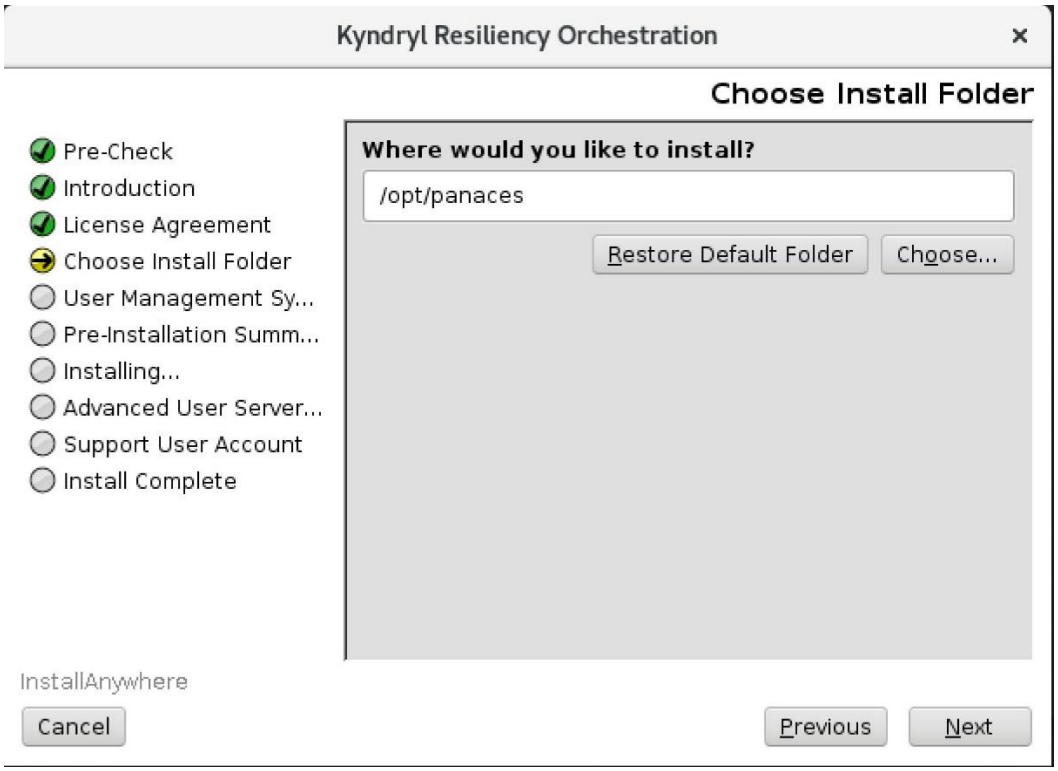


Figure 11: Kyndryl Resiliency Orchestration Server Installation - Choose Install Folder

11. Select a path to install the software by clicking **Choose** and then click **Next**. The **Installation User Account** window is displayed.

> **Note:**
>
> Choose the panaces installation path where the Panaces are to be installed.

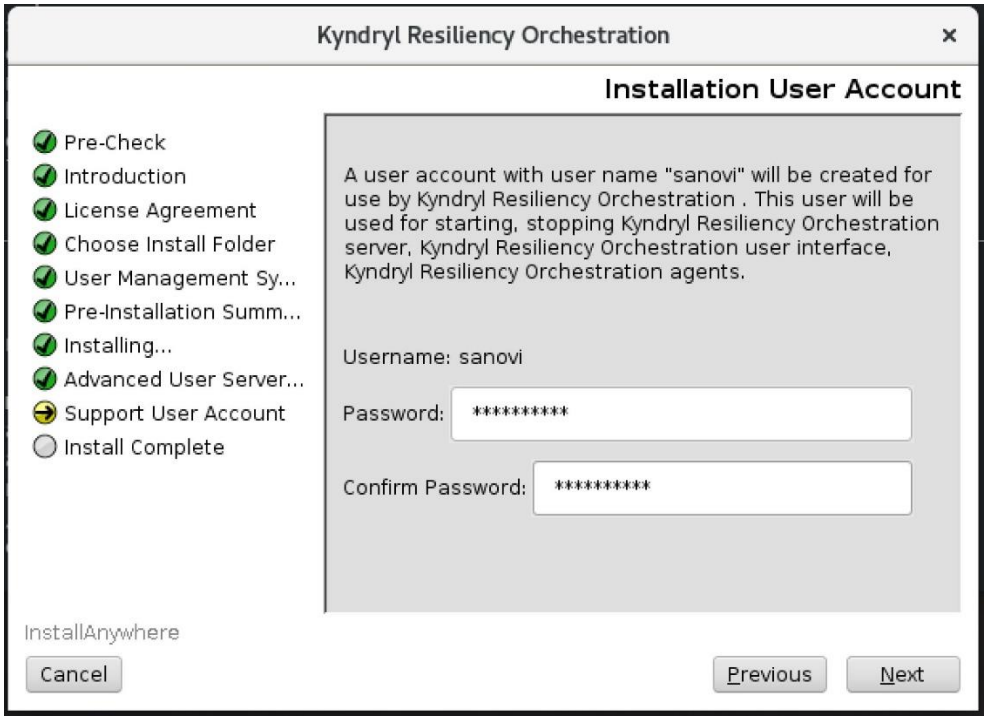


Figure 12: Kyndryl Resiliency Orchestration Server Installation – Installation User Account

12. Click **Next**. The **User Management System** window is displayed.

13. Select the appropriate user management system type.

Table 11: User Management System Selection and steps to be followed

Radio Button	Description	Steps to Follow
Kyndryl Resiliency Orchestration User Management	Select this radio button if you wish to have Kyndryl Resiliency Orchestration manage user details.	12.1 through 12.5 below
Third-Party User Management	Select this radio button if you wish to manage user details via an external application	12.6 through 12.9 below

	such as LDAP or Microsoft Active Directory.	

a. Select the **Kyndryl Resiliency Orchestration User Management** radio button and then click **Next**. The **Pre-Installation Summary** window is displayed.

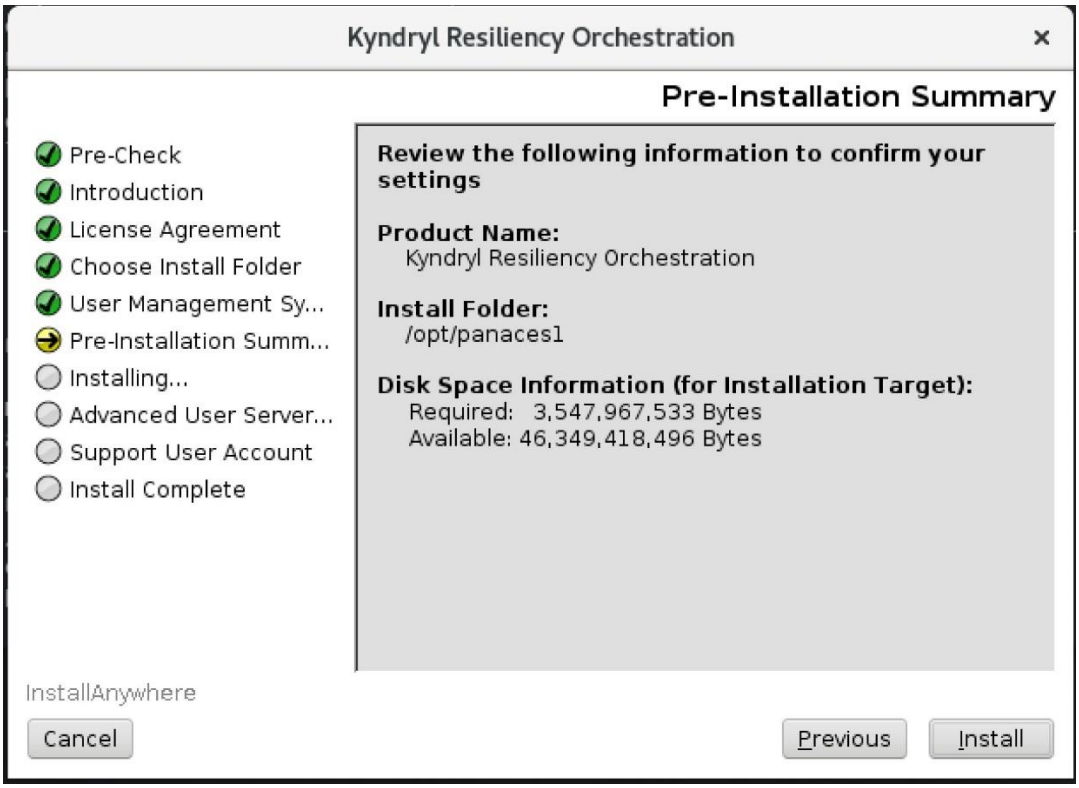


Figure 13: Kyndryl Resiliency Orchestration Server Installation - Pre-Installation Summary

b. Inspect the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify as needed.

c. Click **Install**. The Installing Kyndryl Resiliency Orchestration Server window is displayed.

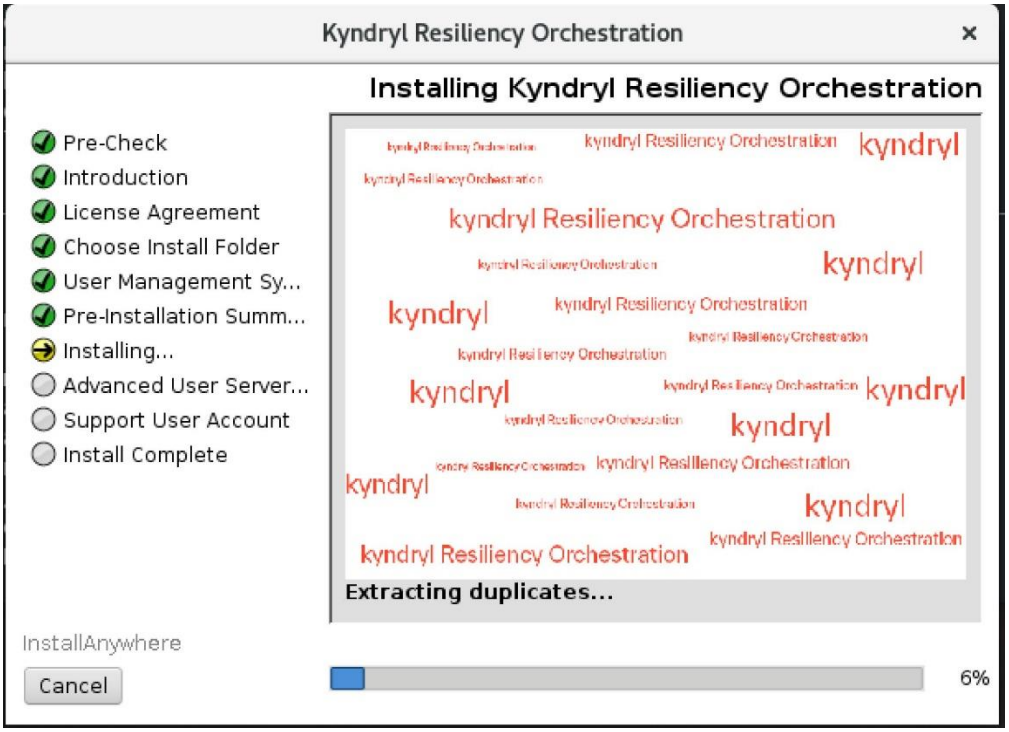


Figure 14: Kyndryl Resiliency Orchestration Server Installation - Installing Kyndryl Resiliency Orchestration Server

d. Click **OK** on SSL enabled on the database dialog box.

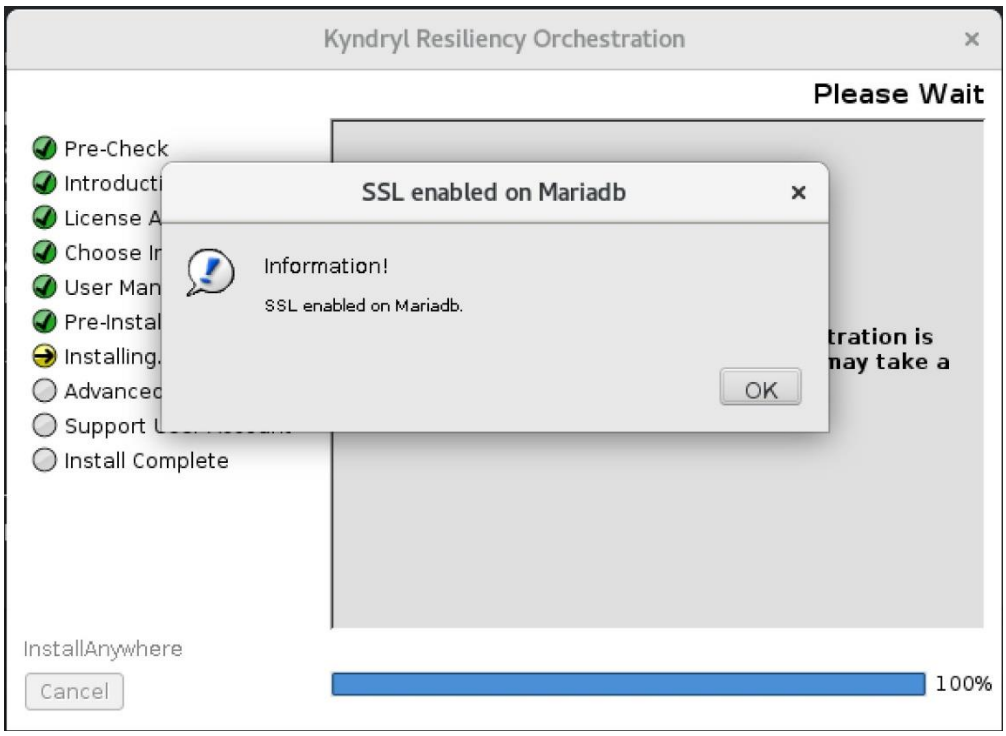


Figure 15: Kyndryl Resiliency Orchestration Server Installation – SSL enabled on Mariadb

Note

BM Resiliency Orchestration Server Installation automatically uploads the Kyndryl Resiliency Orchestration Schema. If it already exists, a confirmation dialog box appears as shown below seeking confirmation to drop the existing Kyndryl Resiliency Orchestration Schema and replace it through the installer.

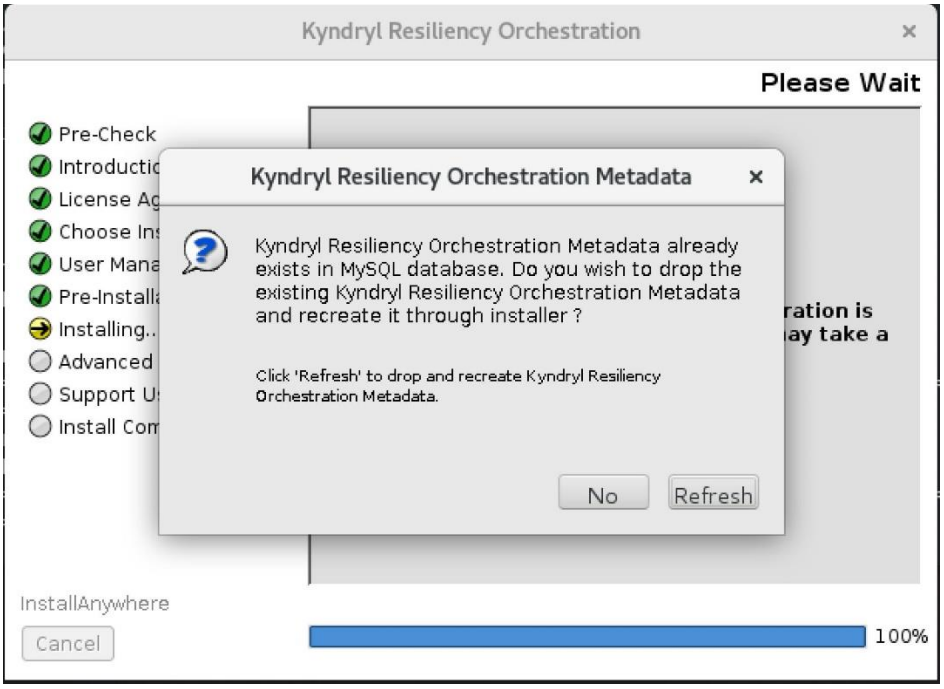


Figure 16: Kyndryl Resiliency Orchestration Server Installation - A confirmation message

e. Click **No** to continue the installation with the existing schema. Else click **Refresh** to drop and recreate Kyndryl Resiliency Orchestration Schema.

Note

To replace the database schema manually, type the following command:

Run the enableEncryptionOnTables.sh script to decrypt data before backup. Refer procedure to enableEncryptionOnTables .

#sudo mysqldump –u root –-databases *panaces pfr* --routines –-triggers -p > backup_file_name.sql

Drop the existing databases if they already exist

sudo mysqladmin –u root drop panaces

sudo mysqladmin –u root drop *pfr*

sudo mysql -u root < $EAMSROOT/lib/mysql_schema_InnoDB.sql

sudo mysql -u root < $EAMSROOT/lib/pfr.sql

```
# sudo $EAMSROOT/installconfig/importTemplateEvents.sh
```

f. The **Advanced User Server Details** screen will be displayed if **Advanced User Management System** is selected. Select the server type and provide the required details for connecting to the external server, as shown in the following two figures.

Note:

By default, the third-party user management tool (LDAP or AD) will perform the authentication and the authorization will be performed by the Kyndryl Resiliency Orchestration application. In case you wish to change the authentication/authorization mode, please refer to the topic changing the Authentication/Authorization Mode in Kyndryl Resiliency Orchestration Admin Guide.

g. Enter the values for all the fields on the panel.

Table 12: Third-Party User Server Details Field Description

Field	Description
LDAP	Select this radio button to enable LDAP as the third-party user management system
Active Directory	Select this radio button to enable Active Directory as the third-party user management system
Server URL	Enter the AD server root domain name with the port as 636.
Server Domain (Applicable for AD only)	Enter the AD server hostname.
Search base for roles	Enter the domain under which the AD users and roles are defined.
User Account for reading directories	
Username	Enter the AD login Username
Password	Enter the AD login password.

AD Default Roles	DEFAULT_USER_AD

h. Click **Next**. The **Support User Account** window is displayed.

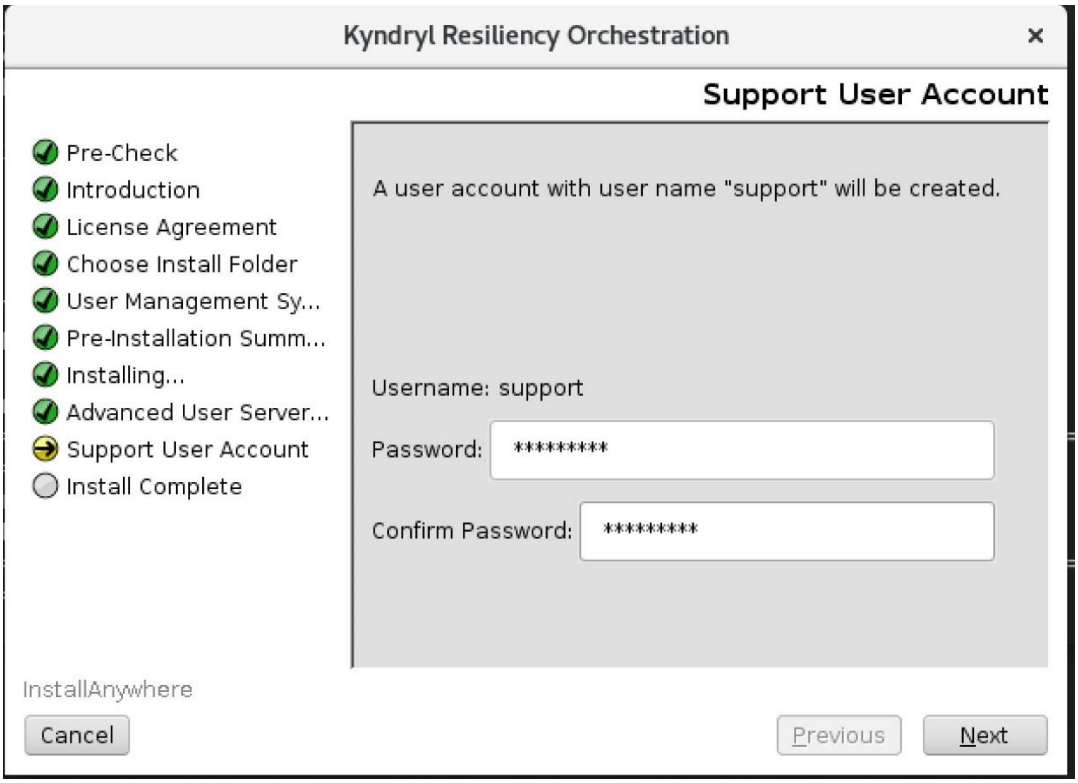


Figure 17: Kyndryl Resiliency Orchestration Server Installation - Support User Account

i. A user account with username **support** is created for use by Kyndryl Resiliency Orchestration Server. Enter the password for this account in the **Password** box. Reenter the password in the **Confirm Password** box.

> **Note**
>
> For invalid passwords, a dialog box appears with an error message.

j. Click **Next**. Once the metadata information is created by the installer, Kyndryl Resiliency Orchestration Server will configure the system with events and events correlation template definitions.

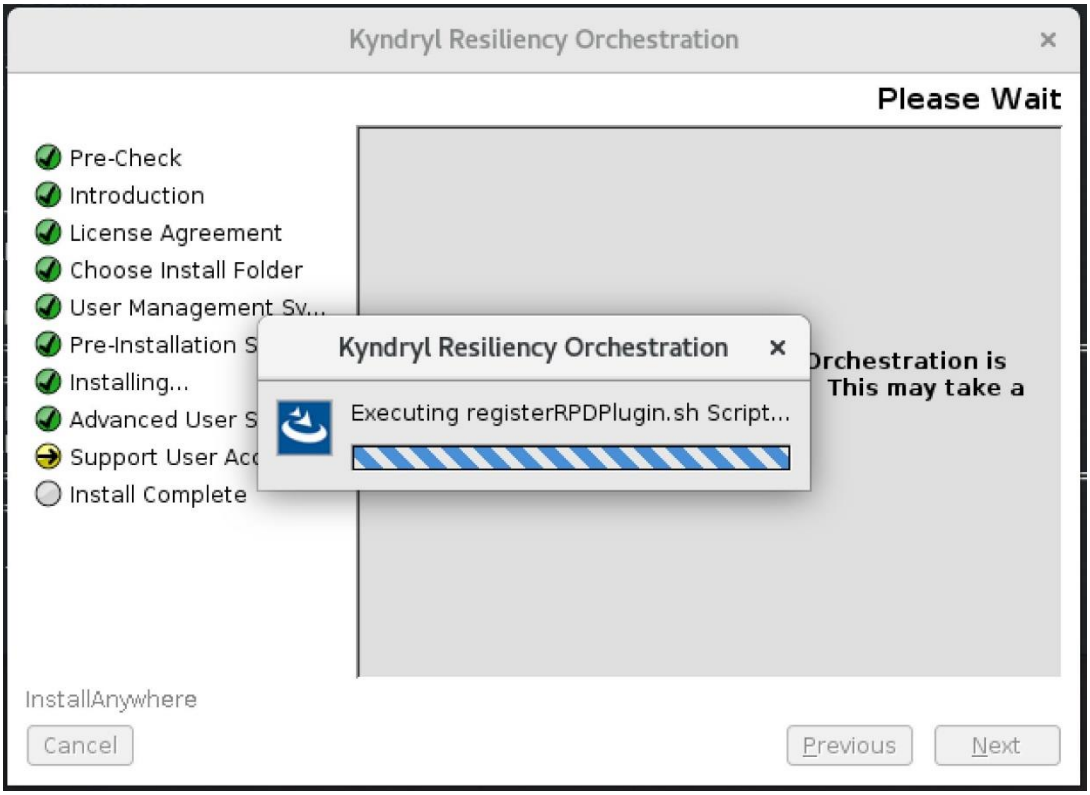


Figure 18: Kyndryl Resiliency Orchestration Server Installation - System Configuration

14. Click **Next**.

> **Note**
>
> In case you get a warning message saying, “Unable to find configuration file (my.cnf)”, please update the max allowed packet to 16MB in my.cnf configuration file and restart the mysql service.

15. Click **Next**. The **Installation Completed** window is displayed, indicating a successful installation.

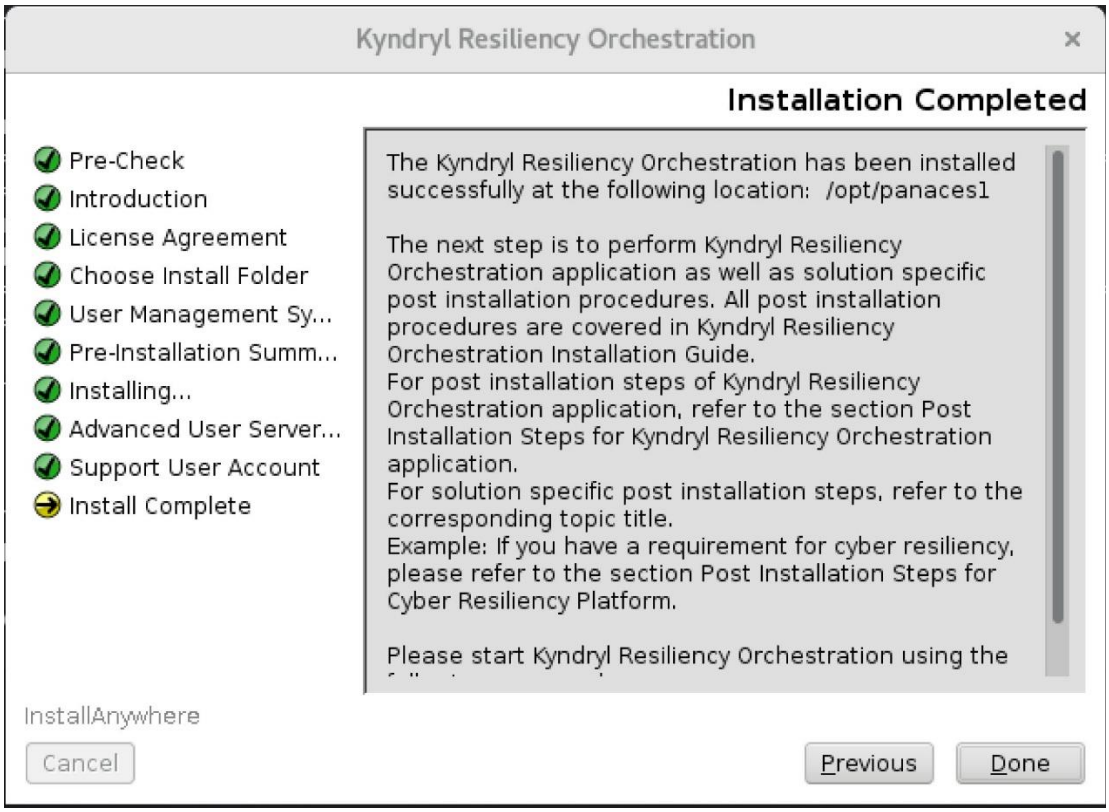


Figure 19: Kyndryl Resiliency Orchestration Server Installation - Installation Completed

16. Click **Done** to complete the installation process.

5.4.1 Migrating DB Component from Local Host to dedicated Server (Split Installation)

Note: Refer prerequisite mentioned in Prerequisites for Installing the Kyndryl Resiliency Orchestration Application Software.

1. Run the enableEncryptionOnTables.sh script under $EAMSROOT/bin in the Kyndryl Resiliency Orchestration server.

```
sudo ./enableEncryptionOnTables.sh "dec" "<DB root user password>"
Check for the below table decryption confirmation message.
Executing the alter ddl statements.
Decrypted
```

2. Execute either of the following commands, depending on the version of the RHEL OS you are using:

```
sh install.bin
```

or

```
./install.bin
```

> **Note**
>
> Java will be installed automatically after the execution of this command.

3. After extracting the files from the install.bin, the Kyndryl Resiliency Orchestration Server installation starts with the following screen. A progress bar appears at the bottom of the screen indicating that the installer is being loaded.

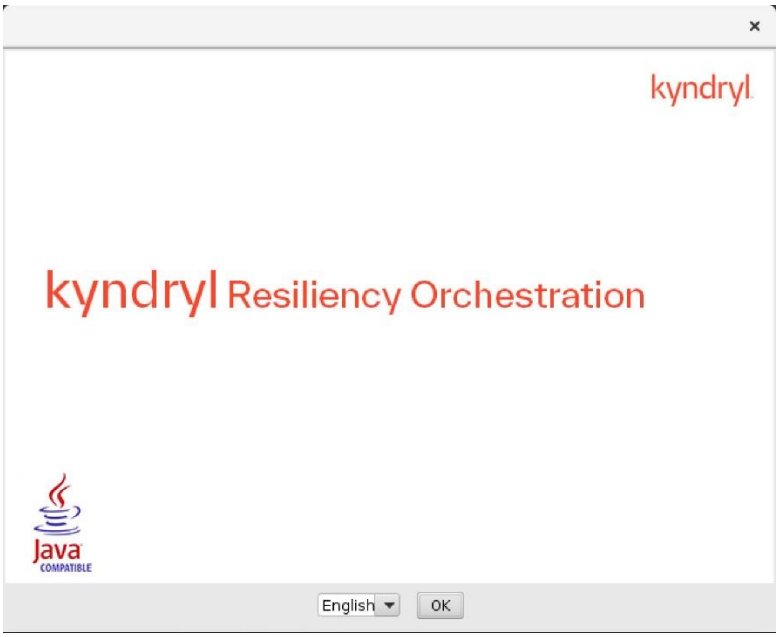


Figure 20: Kyndryl Resiliency Orchestration Installer

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

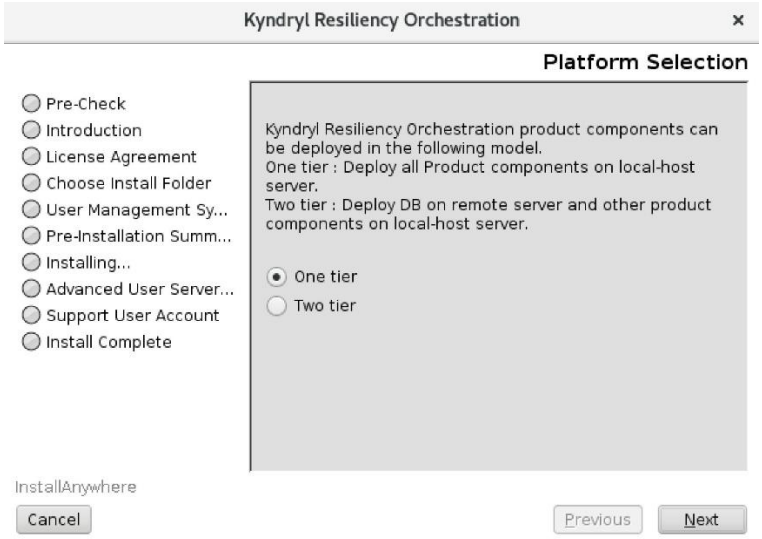


Figure 21 Kyndryl RO Platform Selection One Tier

5. Select the **Two Tier** radio button and select the **MariaDB** radio button. Then click **Next.** The **Database Access details for the two-tier** window are displayed for two-tier selection.

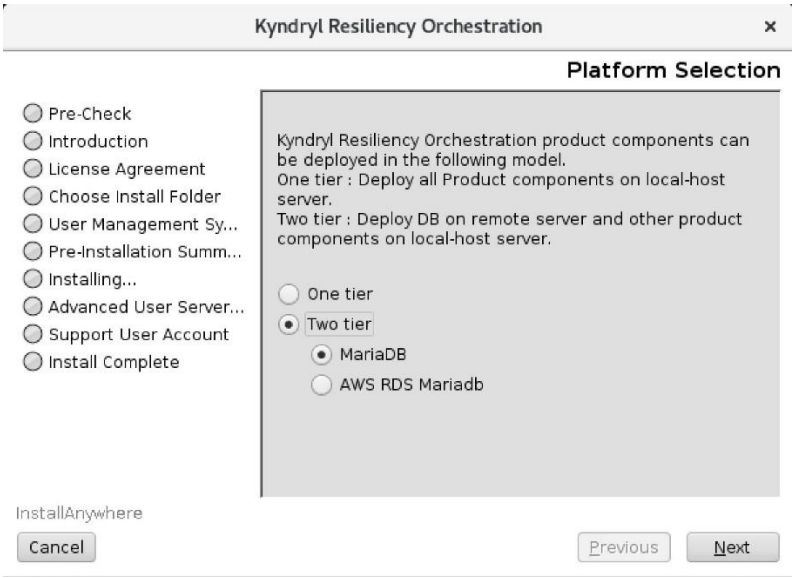


Figure 22: Kyndryl Resiliency Orchestration Server Installation - Platform Selection

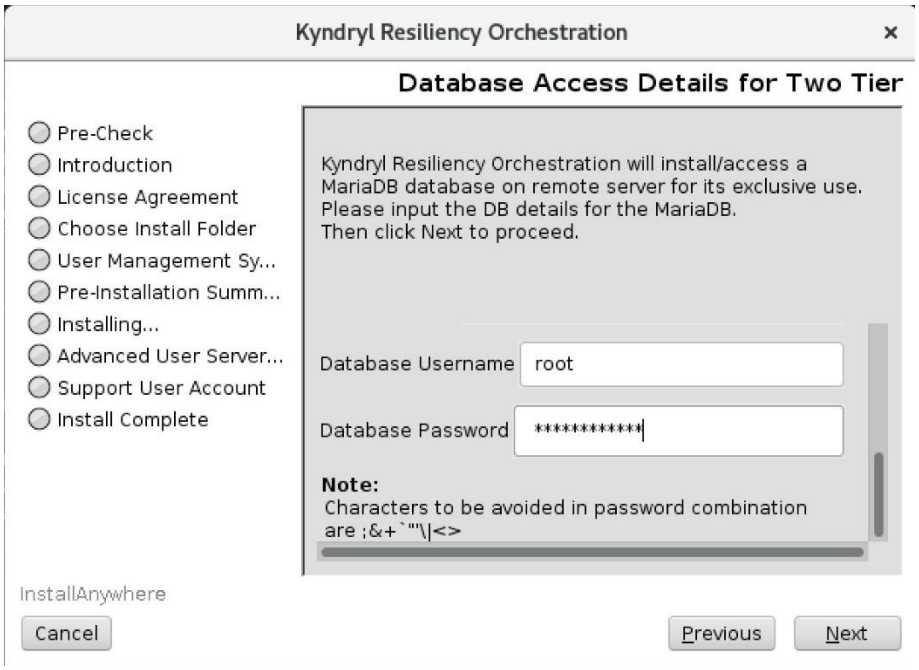


Figure 23: Kyndryl Resiliency Orchestration Server Installation – Database Access Details for Two Tier 2

6. Enter the values for all the fields on the panel.

Table 13. Database Access Details for Two Tier – Field Description

Field	Description
Localhost SSH Private Key	Enter the local host (application server) private key.
Database Host Login User	Enter the DB host server username.
Database host	Enter the database host IP address/name (which could be a fully qualified domain name (fqdn))
Database port	Enter the database port.

Database Username	Enter the database root username.
Database Password	Enter the password for the Database root user.

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

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

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

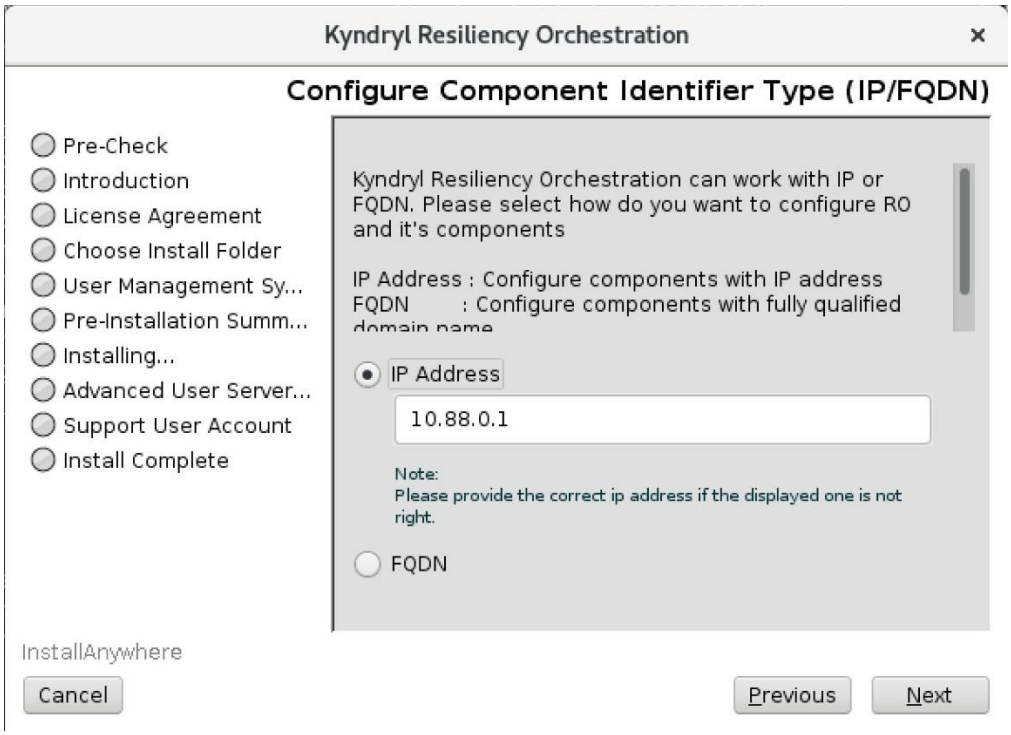


Figure 24: Kyndryl Resiliency Orchestration Server Installation – Configure Component Identifier Type (IP/FQDN) 1

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

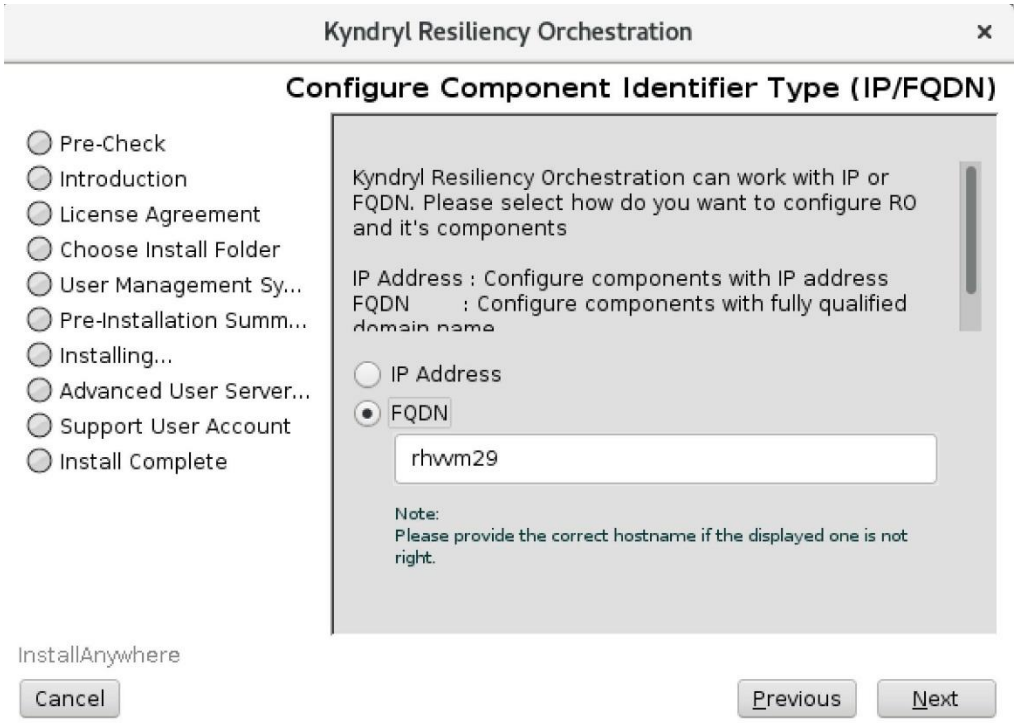


Figure 25: Kyndryl Resiliency Orchestration Server Installation – Configure Component Identifier Type (IP/FQDN) 2

8. Click **Next**. The **Tomcat Home** window is displayed

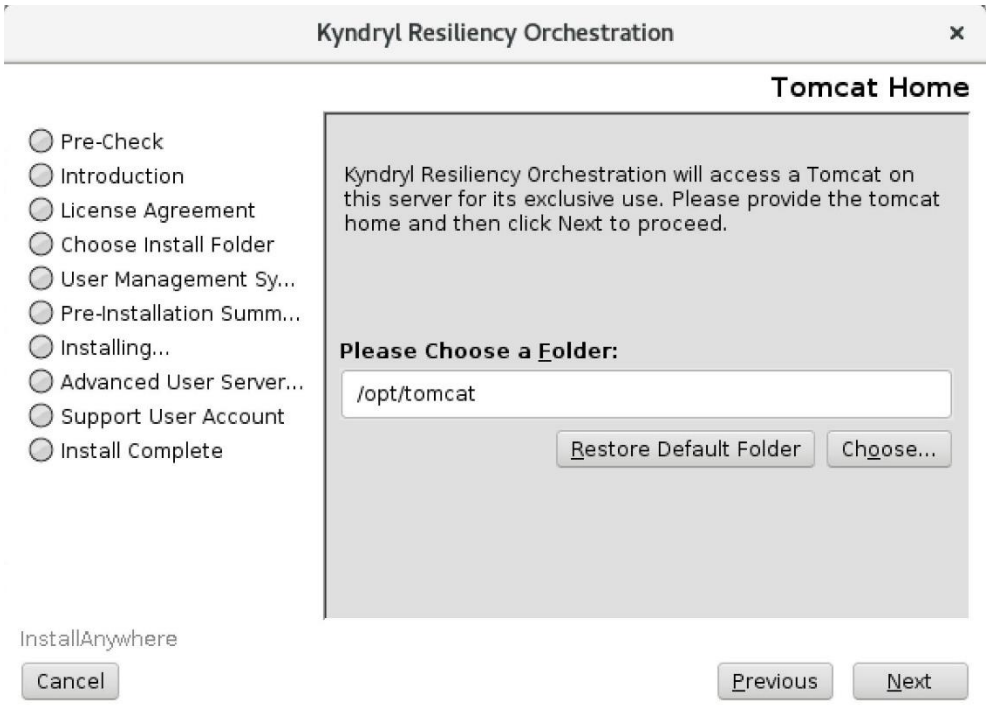


Figure 26: Kyndryl Resiliency Orchestration Server Installation - Tomcat Home

17. 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.

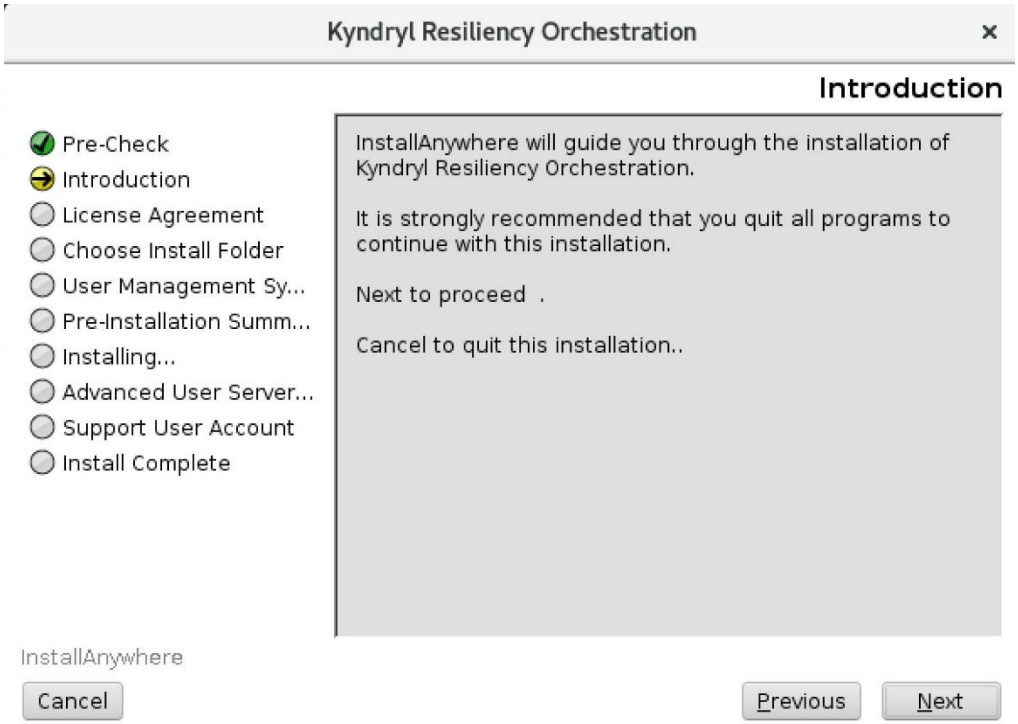


Figure 27: Kyndryl Resiliency Orchestration Server Installation - Introduction

18. Click **Next** to continue the installation. The **License Agreement** window is displayed.

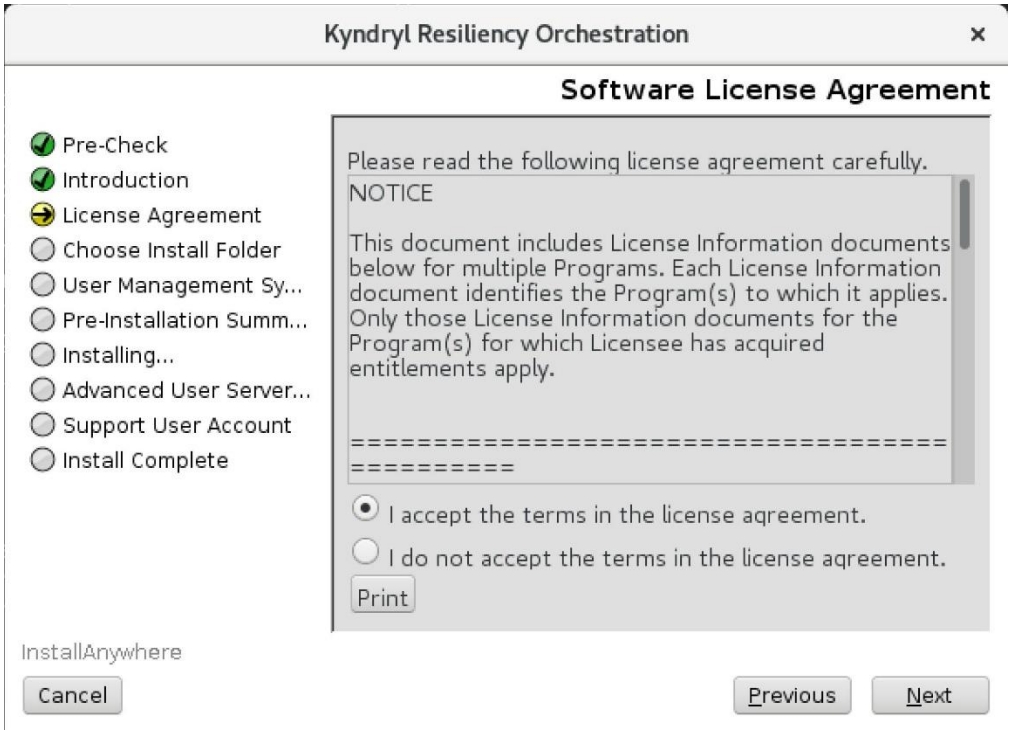


Figure 28: Kyndryl Resiliency Orchestration Server Installation – Software License Agreement

19. Click the appropriate radio button after you have read through the **License Agreement**.

Table 14: Software License Agreement Options

Radio Button	Description
I accept the terms of the License Agreement	Select this radio button to accept the License Agreement.
I do NOT accept the terms of the License Agreement	Select this radio button to reject the License Agreement and then click **Next**. A pop-up is shown which allows the user to either accept the License Agreement or Quit.

20. Click **Next** to proceed with the installation. The **Choose Install Folder** window is displayed.

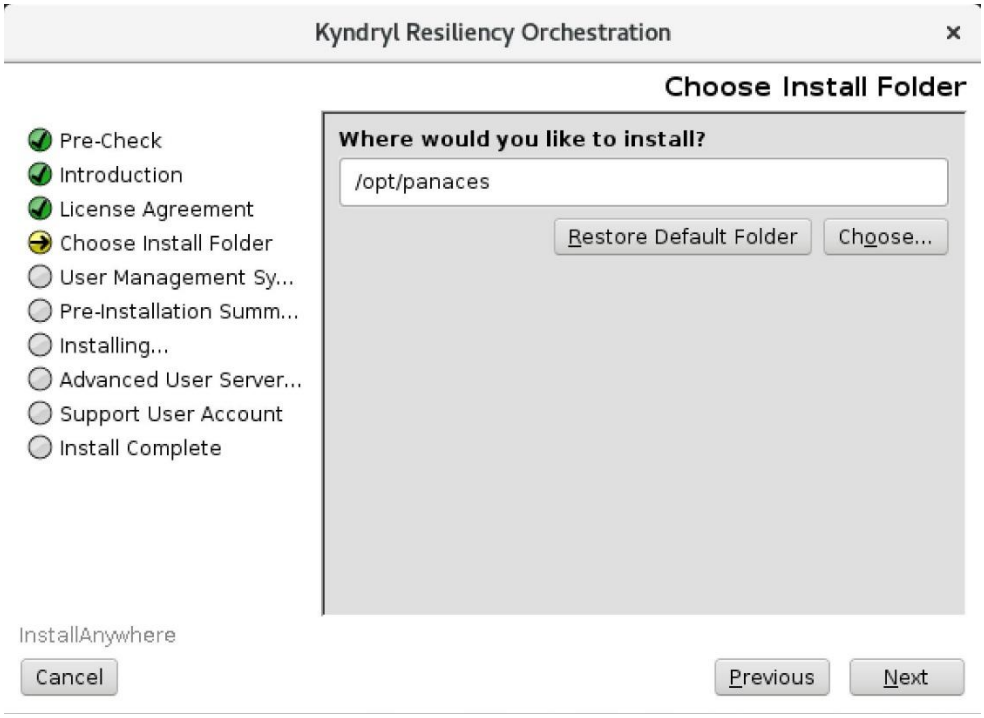


Figure 29: Kyndryl Resiliency Orchestration Server Installation - Choose Install Folder

21. Click **Choose** and select the panaces installation folder where the Panaces is currently installed.
22. Click **Next**. The **Pre-Installation Summary** window is displayed.

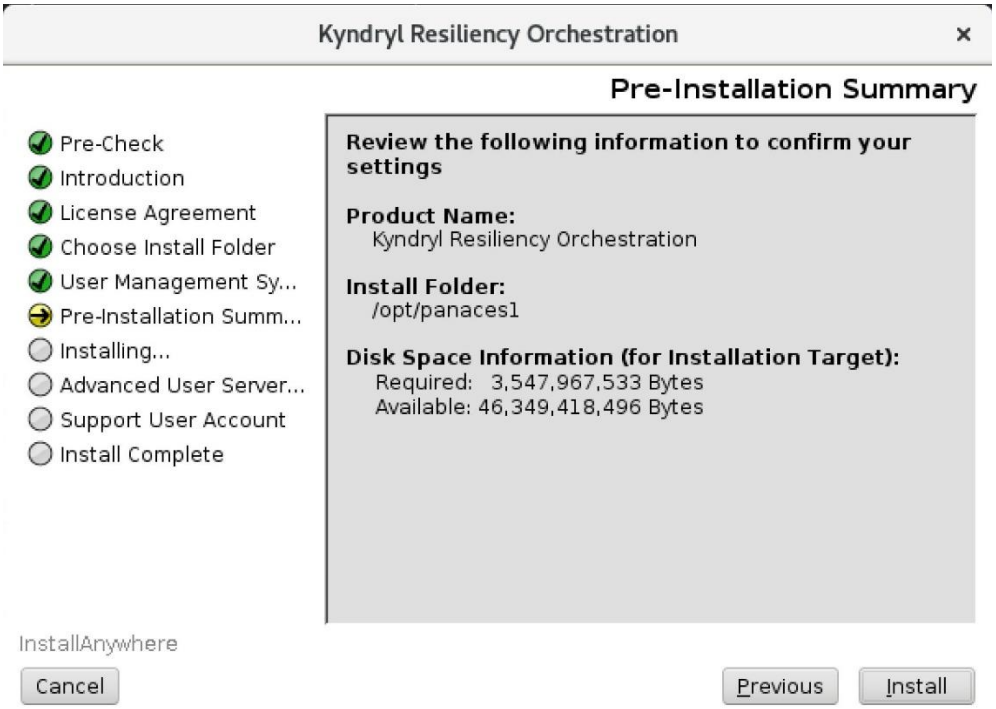


Figure 30: Kyndryl Resiliency Orchestration Server Installation - Pre-Installation Summary

23. Inspect the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify as needed.
24. Click **Install**. The Installing Kyndryl Resiliency Orchestration Server window is displayed.

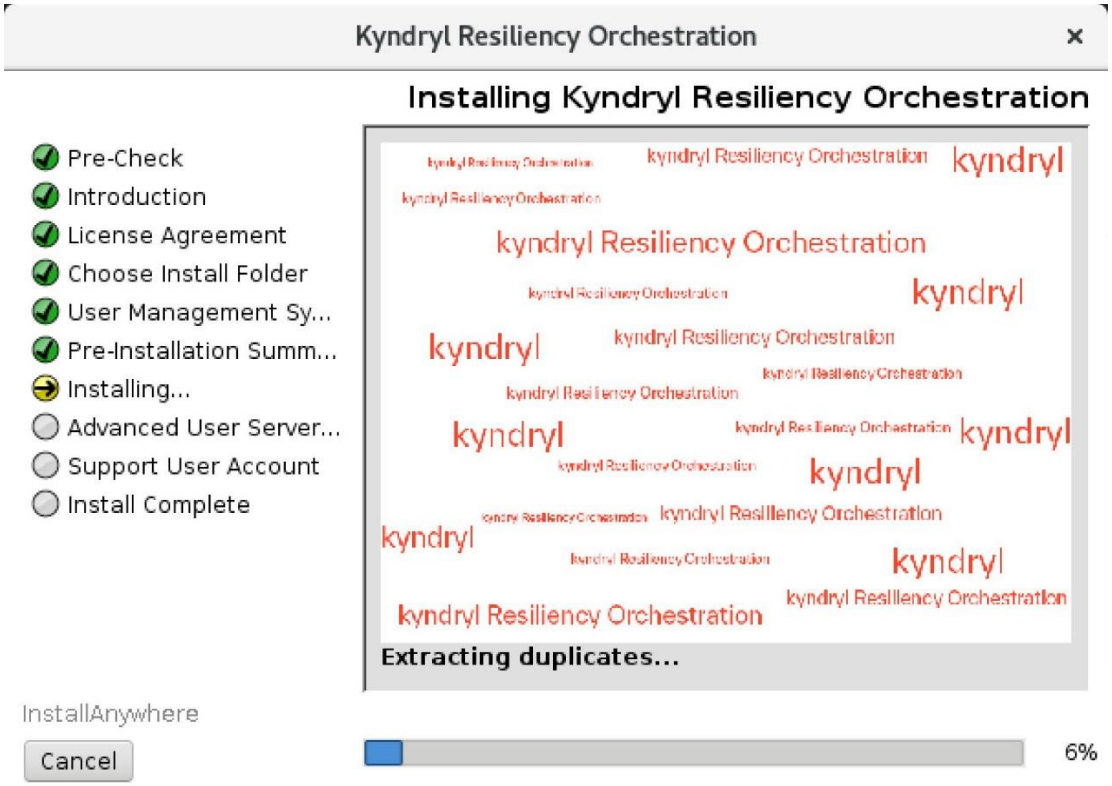


Figure 31: Kyndryl Resiliency Orchestration Server Installation - Installing Kyndryl Resiliency Orchestration Server

25. Click **ok** on SSL enabled on Mariadb dialog box.

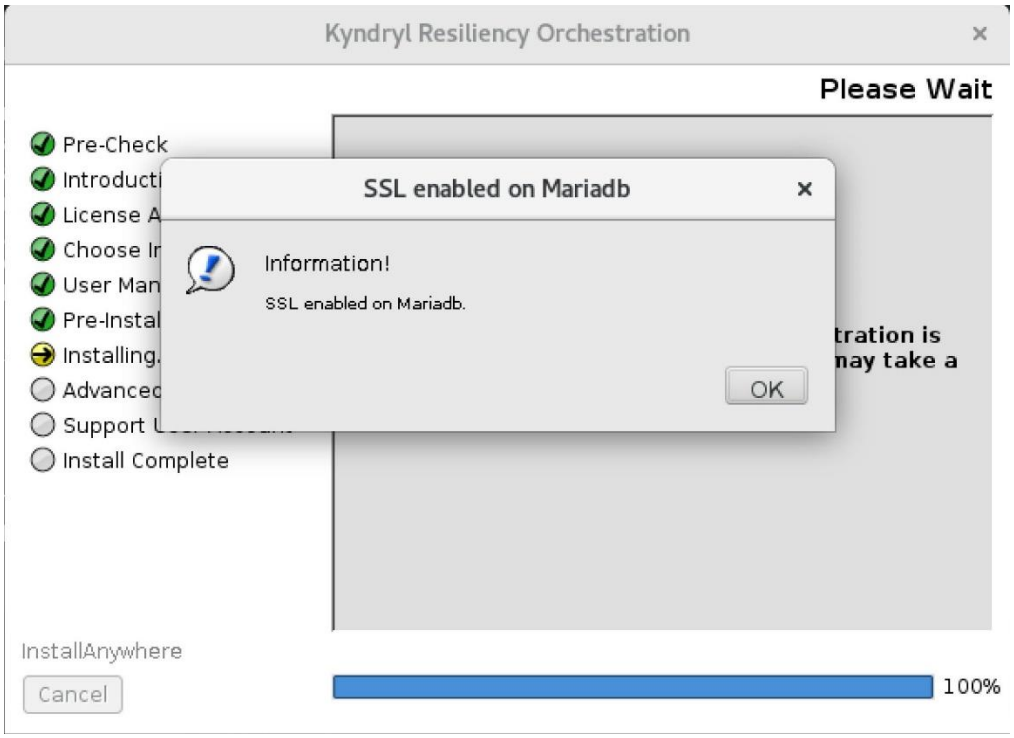


Figure 32: Kyndryl Resiliency Orchestration Server Installation – SSL enabled on Mariadb

26. Click **Ok**. The split process will begin.

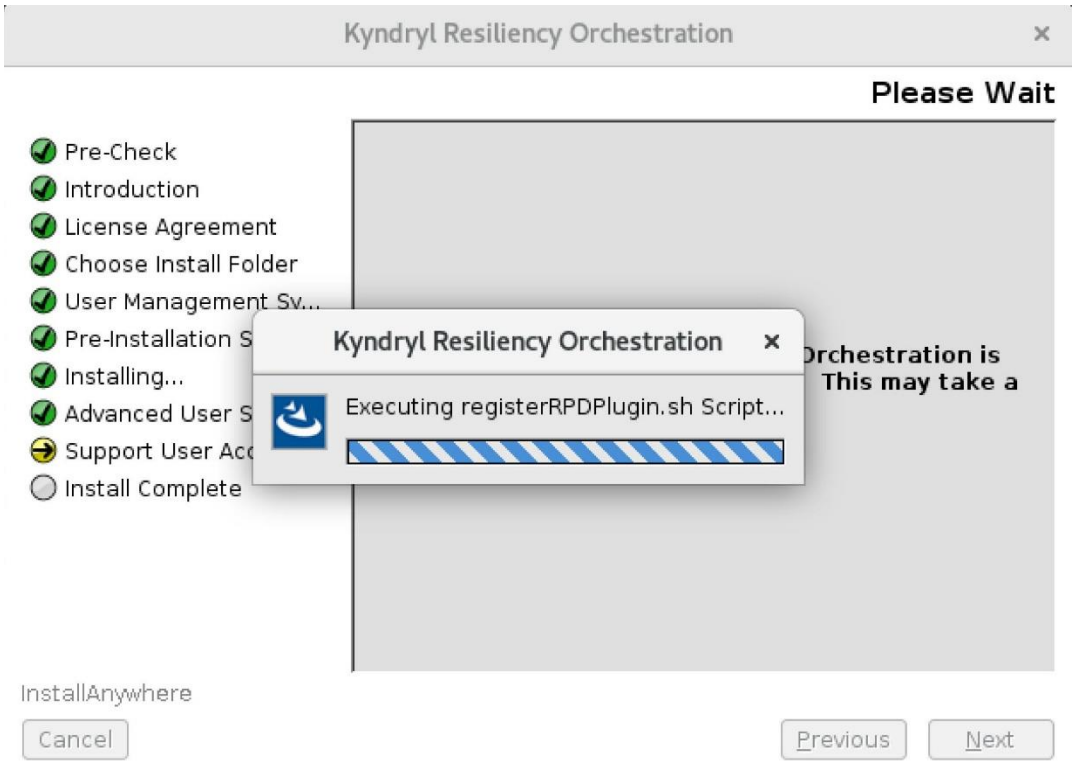


Figure 33: Kyndryl Resiliency Orchestration Server Installation - System Configuration

27. Click **Next**. The **Installation Completed** window is displayed, indicating a successful installation.

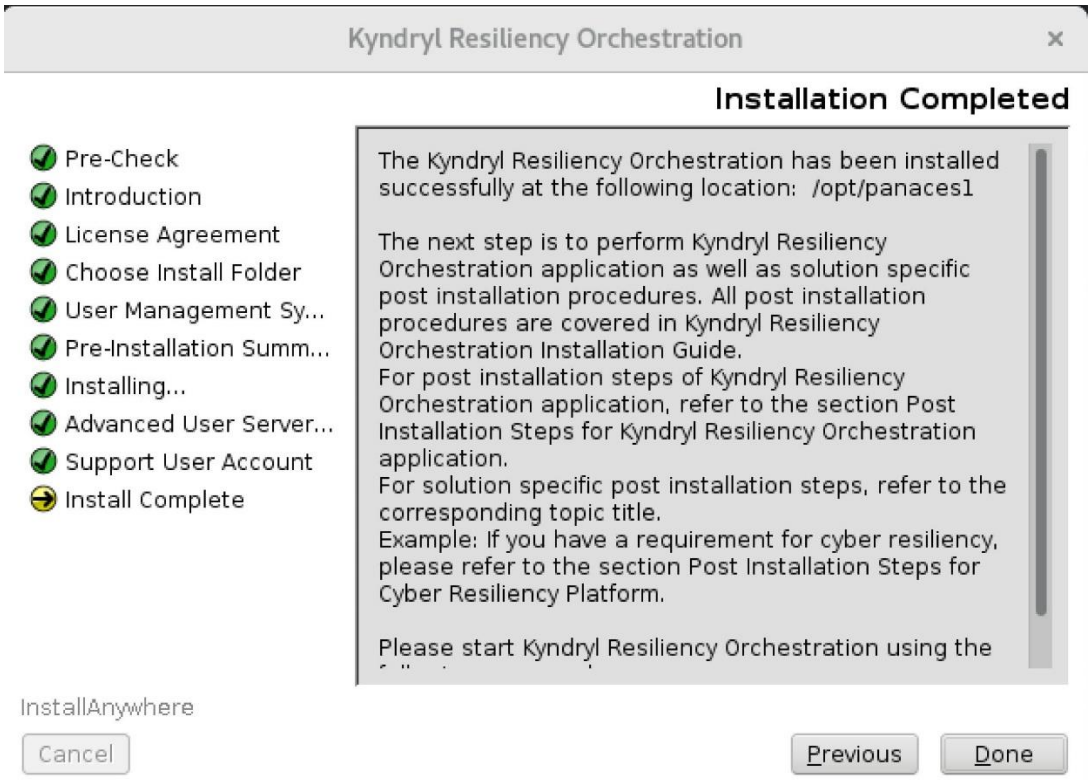


Figure 34: Kyndryl Resiliency Orchestration Server Installation - Installation Completed

28. Click **Done** to complete the installation process.

> **Note:**
>
> Post two-tier installation, it is recommended to remove the ssh connection configuration of the Resiliency Orchestration Server to the MariaDB server.

29. Execute the following command before running the DBTierUpgrade.sh script available in $EAMSROOT/bin/:

```
Check for logs related to DB Backup of source and DB import to
Remote DB:  /opt/panaces/var/log/DBTierUpgrade.log and check for
the "Script executed successfully" message.
```

30. Start the Kyndryl Resiliency Orchestration services.

```
$EAMSROOT/bin/panaces start
```

5.5 Installing the Kyndryl Resiliency Orchestration Server in Silent/console Mode

When you install Kyndryl Resiliency Orchestration in Silent mode, the installation program uses the **.properties** file for the server (PanacesServerInstaller.properties) as well as agents (PanacesAgentsInstaller.properties), to determine which installation options should be implemented. Therefore, before you can run the installation program in Silent mode, you must edit the respective properties file to specify the installation options that you want to invoke, at the time of installation.

Note – Incorrect entries in the properties files can cause installation failure. Also, passwords entered by the user are visible in plain text and therefore not secure. Hence, Silent mode installation is not recommended. Instead, use the GUI mode for Installation as detailed in Installation of Resiliency Orchestration Server in Graphical Mode.

5.5.1 Editing the Properties File

Perform the following steps to edit the properties files.

1. Download the Binaries and properties files from the Kyndryl Passport Advantage site to a location on the intended Resiliency Orchestration Server.

> **Note:**
>
> Ensure that binary file and property files are available in /opt/Server and the logged-in user has sudo permissions equivalent to root.

31. Open the properties file by using the following command:

```
cd /opt/Server

sudo vi PanacesServerInstaller.properties
```

32. Modify the respective properties files for the keywords shown in the following tables.

5.5.1.1 PanacesServerInstaller.properties file

The following table describes the keywords in the `PanacesServerInstaller.properties` file.

There are 2 additional properties added for Fully Qualified Domain Name (FQDN) selection – FQDN_SELECTION and LOCAL_HOST_SERVER.

FQDN_SELECTION Values 0 (default) for IP address or 1 for FQDN /hostname. Local host server values are the Ip address or FQDN /hostname of the local host. Please

make sure to fill this out as per your preference. Do not leave the LOCAL_HOST_SERVER property blank, else installation will fail.

Table 15: Keywords in the PanacesServerInstaller.properties file

Keyword	Description
INSTALLER_UI	Set to "silent" to install without any user interaction. Set to "console" to install with password on demand. **Note:** Silent installation is not recommended as the passwords are stored in the uninstall property file. In case you wish to use the silent mode installation, please ensure to delete the stored passwords as described in Post-installation steps.
MODIFY_SYSTEM_FILES=1	It modifies system files, i.e. /etc/hosts,/etc/sysconfig/selinux, /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
USER_INSTALL_DIR	Enter the path for the directory to install the Kyndryl Resiliency Orchestration Server software.(default path is /opt/panaces/)
ON_DEMAND_PASSWORD	Set to "Yes" if INSTALLER_UI is set to "console." Set to "No" if INSTALLER_UI is set to "silent." **Note:** • Installation is aborted in case an incorrect keyword value is entered. • In case this Keyword is set to "No," then the user will need to input the passwords for the following keywords. DATABASE_PASSWORD, SUPPORT_USER_PASSWORD, and

Keyword	Description
	SANOVI_USER_PASSWORD in the property file. • In case this Keyword is set to "Yes," • Passwords for DATABASE_PASSWORD, SUPPORT_USER_PASSWORD, and SANOVI_USER_PASSWORD will be prompted to be input by the user at the time of installation. **Note:** You will need to select application language and agree to the license.
GA_VERSION_FILENAME_WITHPATH =<validation key>	You need to download the Kyndryl RO Server Upgrade addendum file from the Passport Advantage location, and put the validation key in this property. Example: /opt/Validation_Key
FQDN_SELECTION	Node Identifier Type selection. Values- 0 for IP address or 1 for FQDN/hostname.
LOCAL_HOST_SERVER	Local host server. Values- IP address or FQDN/hostname.
NUMBER_OF_TIERS	Number of Tiers Selection values are 1 or 2 # Value 1: Host all components on the local host server (one tier) # Value 2: Host DB component on a dedicated server and other components on the local host server (two-tier)
SLAVE_MODE_INSTALLATION=No	Slave selection will deploy only the application files on the server. Slave mode values Yes or No (default option is No). **Note** – This property is to be set as Yes only for Standby server installation only when AWS RDS MariaDB instance will be used, such as in Cyber Recovery using AWS Vault solution.
MASTER_HOST	Master_host value is required only on slave mode selection as yes. This property is applicable only for Standby server installation when AWS RDS

Keyword	Description
	MariaDB instance will be used, such as in Cyber Recovery using AWS Vault solution.
DATABASE_TYPE=MARIADB	Database type values are MARIADB or AWS_RDS_MARIADB The Default Database type is MARIADB. Database type to be set as AWS_RDS_MARIADB only when AWS RDS MariaDB instance will be used, such as in Cyber Recovery using AWS Vault solution.
INSTANCE_URL	Instance URL value required only Database type as AWS_RDS_MARIADB. **Example** – panacespoccbx0ty.us-east1.rds.amazonaws.com
DATABASE_PORT	Database port number.
DATABASE_USER_NAME	DB user is root or root equivalent privileged user
DATABASE_PASSWORD	Enter the password to connect to the MariaDB database. Mariadb root password is mandatory.
RDS_CERT_PATH	AWS RDS instance certificate path. This is required only when AWS RDS MariaDB instance will be used, such as in Cyber Recovery using AWS Vault solution
The next three properties are for Two-tier installation (Required only when the Database type value is MARIADB)	
DATABASE_HOST	IP address/Name of remote database host. Required only if platform_selection=2
DATABASE_HOST_LOGIN_USER	Database host OS username. Required only platform_selection=2
SSH_PRIVATE_KEY_ABSOLUTE_PATH	Application server Private key path. Required only platform_selection=2 For example : /root/.ssh/id_rsa
KEYSTORE_FILE_PATH	Add the keystore path. For example: /opt/panaces/installconfig/keystore/sanovi.keystore
REFRESH_EXISTING_SCHEMA	When the Schema Refresh option is chosen, the old schema which is already available in the system will be refreshed. Set the option to 0: If the option is set to 0 the schema will not be refreshed. Set the option to 1: if the option is set to 1, the schema will be refreshed/reset.

kyndryl

Keyword	Description	
	Note: Option 0 is set by default and is the only option for upgrades.	
STOP_KYNDRYL_RESILIENCY_ORCHESTRATION_AND_UNINSTALL	Set the option to 1: If the option is set to 1, the installer will stop the running services and uninstall. Set the option to 0: If set to 0, the services will be running, and the uninstaller will quit. The logs will be available in the \temp directory.	
USER_MANAGEMENT_MODE	**Kyndryl RO**	**THIRD_PARTY**
THIRD_PARTY_SERVER_TYPE	NA	LDAP or AD Default: AD
THIRD_PARTY_SERVER_URL	NA	Enter the third-party Server URL of the AD/ LDAP Server **Note:** Please provide the root domain instead of the Ad server IP.
THIRD_PARTY_SERVER_DOMAIN	NA	The Server Domain applies only to AD. Note: we should not enter the domain for LDAP
DIRECTORY_USERNAME	NA	Enter the Username for reading the external system for the AD/LDAP server.
DIRECTORY_PASSWORD	NA	Enter the Password for reading the external system for the AD/ LDAP server.
SEARCH_BASE_FOR_READING_ROLES	NA	Enter the search base string for the AD/ LDAP server.
AD_DEFAULT_ROLES	NA	The value is default role names. It will accept single and multiple values with comma separation.

Keyword	Description
LICENSE_ACCEPTED	Enter the value as “TRUE” else, an error message is displayed as EULA is not accepted.
SUPPORT_USER_PASSWORD	Enter the password for the support user(default =<Password[1]>). [1]Connect with the Support/Delivery team to get the default passwords.
TOMCAT_HOME	Enter the Tomcat Installation directory path.
CHOSEN_INSTALL_MODE	Keep the field empty for a fresh installation. Set to “Upgrade” for upgrade installation.

kyndryl

5.5.1.2 PanacesAgentsInstaller.properties file

The following table describes the keywords in the `PanacesAgentsInstaller.properties` file.

Table 16: Keywords in the PanacesAgentsInstaller.properties file

Keyword	Description
INSTALLER_UI	Displays the mode of installation as "silent".
MSSQL_AGENT_WINDOWS_CHK Sanovi File replicator _AGENT_CHK SYBASE_AGENT_SOL_CHK SRS_AGENT_CHK ORACLE_AGENT_CHK ORACLE_DATA_GUARD_AGENT_CHK TRUE_COPY_AGENT_CHK SRDF_AGENT_CHK HPXP_AGENT_CHK DB2_AGENT_CHK POSTGRES_AGENT_CHK	Enter 1 to install the agent. Enter 0 to not install the agent.
USER_INPUT_RESULT_JAR_MSSQL	Enter the full path of the directory where the MSSQL Jar files have been installed. For example: On Windows, the location of the Jar files would be C:\Program Files\Microsoft SQL Server 2000 or 2005 Driver for JDBC\lib
USER_INPUT_ORACLE_HOME	Enter the full path of the directory where the Oracle is installed.
USER_INPUT_RESULT_JAR_ORA	Enter the full path of the directory where the Oracle Jar files have been installed. Usually, it is $ORACLE_HOME/jdbc/lib
USER_INPUT_RESULT_JLIB_ORA	Enter the full path of the directory where jar library files are located. Usually, it is $ORACLE_HOME/jlib
USER_INPUT_RESULT_JAR_SYBASE	Enter the full path of the directory where the Sybase Jar files have been installed. For Example: <sybase installation path>/jConnect-5_5/classes.
USER_INPUT_RESULT_SYBASE_LOG IN	Enter the Sybase Admin login ID.

Keyword	Description
USER_INPUT_RESULT_PRIMARY_PANACES_SERVER	Enter the IP address/Name of the primary server.
USER_INPUT_RESULT_SECONDARY_PANACES_SERVER	Enter the IP address/Name of the secondary server.
PANACES_AGENT_NODE_ADDRESS	Enter the IP address/Name of the Kyndryl Resiliency Orchestration Agent.
PANACES_AGENT_NODE_BIND_ADDRESS	Resiliency Orchestration IP, the private IP of the Production/DR server
REG_PANACES_CLASSPATH	Displays the Kyndryl Resiliency Orchestration classpath. By default, the following classpath is displayed: lax.nl.env.PANACES_CLASSPATH
USER_INPUT_RESULT_DB2DIR	Enter DB2 installation path
USER_INPUT_RESULT_DB2_INSTANCEUSER	Enter DB2 instance username
USER_INSTALL_DIR	The full pathname for the directory in which you want to install the agent software.
AGENTS_START_YES	Enter 1 if you want to start the agents automatically after the Kyndryl Resiliency Orchestration installation. Enter 0 if you want to start the agents manually. Refer to the Starting and Stopping of Agents in the respective *Installation of Agents* chapter in this guide for more information.
USER_INPUT_RESULT_POSTGRES_LOGIN	By default, "postgres" will be prefilled as the login ID.
USER_INPUT_RESULT_NAT_SERVER	NAT IP Address/Name
USER_INPUT_RESULT_SITE_CONTROLLER_SERVER	Enter Site Controller IP address/Name
CHOSEN_INSTALL_MODE	Enter Upgrade Note: This is used only during Upgrade

1. Execute the following command to start the installation.

```
sudo ./install.bin -f
PanacesServerInstaller.properties
```

33. Follow the *Post-installation Steps*.

> **Note:**
>
> Restart the Resiliency Orchestration Server after updating the parameters in the above table.

5.5.2 Migrating DB Component from Local Host to dedicated Server in CLI Mode (Split Installation)

For migrating DB Component from local host to dedicated server in CLI mode, refer to Installing the Resiliency Orchestration Agent Server in Silent Mode and perform the following.

Note: Refer to prerequisites mentioned in Prerequisites for Installing the Kyndryl Resiliency Orchestration Application Software.

1. Ensure two tier prerequisites mentioned under Prerequisites for Installing the Kyndryl Resiliency Orchestration Application Software are in place.
2. Make sure the Kyndryl Resiliency Orchestration server and DB servers are server Hardened.
3. Log in to the Kyndryl Resiliency Orchestration server and execute the below commands:
   a) ssh-keygen -t rsa -m PEM
   b) ssh-copy-id os_user@DBserverIP

   Verify is the ssh connection is established by using the below command in the Kyndryl Resiliency Orchestration server.

   ssh os_user@DBserverIP

   Note: Password will not be prompted.
4. Log in to the DB server and execute the below query.

```
sudo mysql -uroot -p<DB root password>
```

```
GRANT ALL PRIVILEGES ON *.* TO '<DATABASE_USER_NAME >'@'<RO Server
IP>' IDENTIFIED BY '<DATABASE_PASSWORD> ' WITH GRANT OPTION;

GRANT ALL PRIVILEGES ON *.* TO '<DATABASE_USER_NAME >'@'<RO Server
hostname>' IDENTIFIED BY '<DATABASE_PASSWORD> ' WITH GRANT OPTION;
```

Note: In the above query by default the root user password for db is "password". Don't change it unless the root user password for DB is changed.

Check connectivity to the DB server by using the below command from the Resiliency Orchestration application server:

```
sudo mysql -h 1< DB server IP> -u< DATABASE_USER_NAME>  -p<DB user password>
```

5. Run the enableEncryptionOnTables.sh script under $EAMSROOT/bin.

```
sudo ./enableEncryptionOnTables.sh "dec" "<DB root user password>"
```

Check for the below table decryption confirmation message.

```
Executing the alter ddl statements.
Decrypted
```

6. Run the same Kyndryl Resiliency Orchestration Server installer again used while performing 1 tier fresh installation.

   Perform the split installation by updating the below key value in the panaces properties file.

   NUMBER_OF_TIERS=2

   DATABASE_HOST = <DB server IP>

   DATABASE_HOST_LOGIN_USER = <DB server OS username>

   SSH_PRIVATE_KEY_ABSOLUTE_PATH = <SSH key private key absolute path>

   REFRESH_EXISTING_SCHEMA = 0

7. Execute the following command before running the DBTierUpgrade.sh script available in $EAMSROOT/bin/:

Check for logs related to DB Backup of source and DB import to Remote DB: /opt/panaces/var/log/DBTierUpgrade.log and check for the "Script executed successfully" message.

8. Start the Kyndryl Resiliency Orchestration services.

```
$EAMSROOT/bin/panaces start
```

5.6 Post-installation Steps for Kyndryl Resiliency Orchestration application

1. After successful installation of the Kyndryl Resiliency Orchestration application,

1.1. Delete the PanacesServerInstaller.properties and install.bin files from the downloaded locations.

1.2. Delete Installation_log folder from /tmp location.

Steps 2 – 5 are required to apply third-party dependencies

2. Download the ThirdPartyJSLib.zip file from the link GPL-dependent binaries (https://sourceforge.net/projects/gnu-utils/files/binaries/) to /tmp

   For more information about the GPL licenses, see *GPL License Information*

3. Extract the ThirdPartyJSLib.zip file to /tmp.
4. Copy the .js files to the following location:

   /opt/apache-tomcat/webapps/PanacesGUI/scripts

5. Copy /tmp/ThirdPartyJSLib/*.* to $TOMCAT_HOME/webapps/PanacesGUI/scripts.

   Example: sudo cp -r /tmp/ThirdPartyJSLib/*.* /opt/tomcat9/webapps/PanacesGUI/scripts/

6. Remove /tmp/ThirdPartyJSLib*.*

34. Add all the vault integration library files to the following locations:

- {TOMCAT_HOME}/webapps/PanacesGUI/WEB-INF/lib
- {TOMCAT_HOME}//webapps/PanacesGUI/pages/classes/lib
- {TOMCAT_HOME}//webapps/userPortal/WEB-INF/lib
- {TOMCAT_HOME}//webapps/userPortal/pages/classes/lib
- {EAMSROOT}/agents/vault/{yourVaultName}/lib
- {EAMSROOT}/lib

> **Note:**
>
> - You will need to set the execute (770) and the Tomcat user group permissions for the vault integration library files in the TOMCAT_HOME locations.
> - You will need to set the execute (770) and Panaces user group permissions for the vault integration library files in the EAMSROOT locations.

35. If you would like to use the Cisco UCS Director (Unified Computing System Director) integration feature of the product, procure the following library files and replace them at the respective locations:

- {EAMSROOT}/lib/ucsd-oa-annotations.jar
- {EAMSROOT}/lib/ucsd-oa-api.jar
- {EAMSROOT}/lib/ucsd-rest-api-sdk-v2.ja
- {EAMSROOT}/lib/cuic-sdk-v2-0.jar
- {EAMSROOT}/lib/inframgr.jar

36. To import Certificate Authority (CA) certificate for authentication via Active Directory, perform the steps listed below.

    a. Run the following command to import the CA certificate

    ```
    a. keytool -import -keystore $EAMSROOT/<jdk-
    version>/jre/lib/security/cacerts -alias 'ad-server-cert' -
    file /ad server certificate path>
    ```

    Example:

    keytool -import -keystore /opt/panaces_RO_abc/jdk1.8.0_181/jre/lib/security/cacerts -alias 'ad-server-cert' -file /tmp/ad-server-cert.cer.

    b. Enter the following keystore password when prompted.

    Password: <Password>

    Note:

    The default password is “<Password>”. Please use the updated password.

    c. Confirm the import command by entering "Yes" on the console.

    Note:

    - To know how to export Active Directory CA certificate to be used in the Kyndryl Resiliency Orchestration application, please refer to the topic Exporting Certificate from the Active Directory server in Kyndryl Resiliency Orchestration Admin Guide.
    - CA certificate should be imported every time the Kyndryl Resiliency Orchestration application is reinstalled, upgraded, or in case the CA certificate expires.

37. Enter the IP and root domain of the AD server in the /etc/hosts file.

    192.x.x.x lnplatform01

    127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

    ::1 localhost.localdomain localhost6 localhost6.localdomain6

    #localhost lnplatform01

    localhost lnplatform01

<ip address of AD server and root domain>

> **Note:**
>
> In the case of Hybrid mode (Active Directory-Kyndryl Resiliency Orchestration Server), you can change the default object class name as per the object class created in the AD server. By default, the object class is “sanovirole”

Example:

ad.roles.object.class=<object class created in AD server>

in EAMSROOT/installconfig/panaces.properties

Example- ad.roles.object.class=myrole

38. Back up $TOMCAT_HOME/webaps/PanacesGUI/WEB-INF/lib/PanacesGUI.jar
39. Add the following files in ” $TOMCAT/webapps/ROOT/”. Replace the file in case the same file exists.

> **Note:**
>
> The files are available at $EAMSROOT/installconfig/ Update_Default_Tomcat_Files.

File alert_48.gif

File asf-logo-wide.svg

File favicon.ico

File hdr-bgr.gif

File ico_footer.gif

File index.jsp

File root.css

File sanovi_cloud_drm_logo.png

File subtab_bg.gif

And add the below content in the web.xml file at the end but before "</web-app>”

Path is "$TOMCAT/conf/web.xml”

```
<error-page>
<error-code>404</error-code>
```

```
<location>/index.jsp</location>
</error-page>

<error-page>
<error-code>400</error-code>
<location>/index.jsp</location>
</error-page>

<error-page>
<error-code>500</error-code>
<location>/index.jsp</location>
    </error-page>
```

40. Perform the following steps to avoid an abnormal shutdown and crashing of Tomcat services.

    Edit the file CATALINA_HOME/conf/server.xml and set the shutdown passphrase:

    ```
    <Server port="8005"
    shutdown=""<Password> "">
    If this functionality is not needed, it must be deactivated
    with the following option
    <Server port=""-1"" shutdown=""SHUTDOWN"">
    The local management scripts allow a shutdown of the server
    even if the shutdown port is disabled."
    ```

    > Note:
    >
    > Ensure that you replace "<Password>" with your encrypted password.

41. To encrypt plain text passwords in tomcat-users.xml, add the below line in the server.xml file just before the </Realm> tag.

    digest="md5".

    a. Go to $TOMCAT_HOME/conf/ tomcat-users.xml and replace the same encrypted password used in the server.xml file in the below-mentioned lines.

    ```
    <user username="tomcat" password="<encrypted password>"
    roles="tomcat"/>
    <user username="both" password="<encrypted password>"
    roles="tomcat,role1"/>
    ```

”

42. Add the below line in the $TOMCAT_HOME/conf/server.xml file.

```
<Valve
className="org.apache.catalina.valves.ErrorReportValve"

showReport="false"

showServerInfo="false"/>
```

Example of $TOMCAT_HOME/conf/server.xml file -

```
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">

<!-- SingleSignOn valve, share authentication between web
applications
Documentation at: /docs/config/valve.html -->
<!--
<Valve className="org.apache.catalina.authenticator.SingleSignOn"
/>
-->

<!-- Access log processes all examples.
Documentation at: /docs/config/valve.html
Note: The pattern used is equivalent to using pattern="common" -->
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%h %l %u %t "%r" %s %b" />
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showReport="false"
showServerInfo="false" />

</Host>
</Engine>
```

43. Add `secretRequired="false"` in server.xml's connector tag and restart the services for the UI to come up.
44. If you would like to use some of the advanced reporting features, download and configure BIRT as detailed in the steps below.

    1. Download the BIRT runtime (version 4.8.0/4.9.0) from the BIRT website https://download.eclipse.org/birt/downloads/drops/R-R1-4.8.0-201806261756/ birt-runtime-4.8.0-20180626.zip

    2. Unzip birt-runtime-4_8_0.zip.

    Refer to the note about unzip at Unzip Note

    3. Copy birt-runtime-4_8_0/WebViewerExample to $TOMCAT_HOME/webapps/

4. Rename 'WebViewerExample’ directory to the 'birt’ directory

5. Copy the file 'connection_profile_dashboard’ from $TOMCAT_HOME/webapps/PanacesGUI/report/ to $TOMCAT_HOME/webapps/birt/ directory

6. Copy all .rptdesign files from $TOMCAT_HOME/webapps/PanacesGUI/report/ to $TOMCAT_HOME/webapps/birt/report/ directory

7. Copy 'mariadb-java-client-2.3.0.jar’ from $TOMCAT_HOME/webapps/PanacesGUI/WEB-INF/lib/ to $TOMCAT_HOME/webapps/birt/WEB-INF/lib/

8. Run the command 'chown -R tomcatuser:tomcatusergroup $TOMCAT_HOME/webapps/birt/'

Note: tomcatuser: This user is created at the Linux level under the group “tomcatusergroup”. This user owns the directories and files related to the tomcat server sub-system which is responsible for Resiliency Orchestration User Interface. This user is also responsible to change any file system permissions and replacements.

Note: Of all the OS users created by RO, only mysql users can be created with the login setting.

45. Add the following property to the $TOMCAT_HOME/bin/catalina.sh script –

```
JAVA_OPTS="$JAVA_OPTS -
Djavax.xml.transform.TransformerFactory=com.sun.org.apache.
xalan.internal.xsltc.trax.TransformerFactoryImpl"
```

Note: Add the above property snippet in the Catalina.sh script file at a particular location as shown in the example screenshot below. This is performed to avoid any XmlUtil UI issues.

Example:

46. Run the following scripts:

```
Go to $EAMSROOT/bin
sudo ./SecurityUserInjection.sh
```

47. Post the installation, it is recommended to change the default passwords for Panaces and PFR MariaDB user, Panaces MariaDB Truststore, Jackrabbit admin, ActiveMQ Broker Resiliency Orchestration, and Site Controller producer and consumer as detailed in the section *Changing Default Passwords (Recommended)*.

48. Start the Kyndryl Resiliency Orchestration Services. See *Starting and Stopping Resiliency Orchestration Server*.

Users are recommended to generate panaces ACP keystore/truststore certs with their own complex password to ensure more security. Users can generate these certs using scripts under EAMSROOT/bin/GenerateCerts folder. For more information, refer to the **Generating Custom Keystore (Optional)** section in this document.

5.6.1 ServiceNow configuration and Control Desk information

Refer to the **Workflow APIs and Incidents Integration** document.

5.7 Post-installation Steps for Cyber Resiliency Platform

For post-installation steps for Cyber Resiliency Platform, refer to the topic **Post-installation Steps for Cyber Resiliency Platform** in Cyber Incident Recovery for Platform User Guide.

5.8 Changing Default Passwords (Recommended)

Starting from 8.1.3.1, a user has the option of making the following password changes.

5.8.1 Using “Custom password” the User decided a complex password can be implemented.

1. Change the Panaces and PFR MariaDB user default password using the below commands.

   In the Resiliency Orchestration Server, execute these commands –

   ```
   cd $EAMSROOT/bin

   sudo ./changeDBPassword.sh panaces.mysql.password

   sudo ./changeDBPassword.sh pfr.db.password
   ```

   Provide the new strong password when you are prompted to.

kyndryl

Note:

It is recommended to choose a strong password that has a mix of alpha-numeric characters and special characters, with a minimum length of 25. Special characters other than space character is allowed. Special characters supported are - ‘ ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] / < > , . ; ? ' : |

You must escape the following special characters while entering a password in the command line - ' ~ ! $ & / < >,. ; ? ': |

Example – P3t3r\:Pant323\~lkj0@19^jf83 - *In this example, and ~ are escaped using* \|

Synchronize the MariaDB using the same new strong changed passwords for panaces.mysql.password and pfr.db.password in the database

```
MariaDB [mysql]> set password for 'panaces'@'localhost'=password('New-Strong-panaces-Password');

MariaDB [mysql]> set password for 'pfradmin'@'localhost'=password('New-Strong-pfr-Password');
```

2. To change the default panaces MariaDB truststore password for panaces.mysql.truststore.password, use the following command.

    1. Change the default password to a new strong password on the existing truststore (truststore.jks) which is present in $EAMSROOT/installconfig/mariadbencryption directory using the below command.

        ```
        $EAMSROOT/jdk1.8.0_221/bin/keytool -storepasswd -keystore $EAMSROOT/installconfig/mariadbencryption/truststore.jks
        ```
        Enter keystore password: Enter as <Password>
        New keystore password: <Enter the new strong password>
        Re-enter new keystore password: <Enter the new strong password again>

    2. Encrypt the truststore password and store it on the Resiliency Orchestration Server using the following procedure.

        1. Go to $EAMSROOT/tools/bin/
        2. Run the script Encryptor.sh with the new strong plain text password as a command-line argument as shown in the example here.

            Example –

```
$EAMSROOT/tools/bin/>sh Encryptor.sh <Password>
```

3. The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password**.

   Example –

   Password to encrypt: `<Password>`
   Encrypted password:
   `<Password>`

   Decrypted password: `<Password>`

   The encrypted password should be updated in the panaces.properties which are located in $EAMSROOT/installconfig, and the property name is panaces.mysql.truststore.password.

3. To change the Jackrabbit default repository admin user password, use the below procedure -

```
$EAMSROOT/bin/changeRepositoryAdminUserPassword.sh <default
password> <new strong password>
```

Example -

./changeRepositoryAdminUserPassword.sh <Password[1]>

[1]Connect with the Support/Delivery team to get the default passwords.

To encrypt and update the truststore password on the Resiliency Orchestration server, use the below procedure.

1. Go to $EAMSROOT/tools/bin/
2. Run the script Encryptor.sh with the new strong plain text password as a command-line argument.
3. The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password**.
4. The encrypted password should be updated in the panaces. properties which are located in $EAMSROOT/installconfig, and the property name is a repository.admin.user.password.

4. To change the default Passwords for the ActiveMQ Broker, refer to the section *Configuring Kyndryl Resiliency Orchestration Server and Site Controller for Secured Communication by Using the ActiveMQ Broker*.

Note – After updating all the encrypted passwords, delete the log file $EAMSROOT/var/log/Encryptor.log for security reasons.

6 Installing Kyndryl Resiliency Orchestration Server on Linux Cluster in the Graphical Mode

This chapter outlines the procedures for installing the Kyndryl Resiliency Orchestration Server on Linux Cluster.

6.1 System Requirements

For the system requirements for installing Kyndryl Resiliency Orchestration Server on Linux Cluster.

> **Note**
>
> Ensure that the Kyndryl Resiliency Orchestration Server installation location is on the shared volume. This is the location of the installed software as explained in the sections below.

6.2 Installation of Resiliency Orchestration Server

Kyndryl Resiliency Orchestration Server Software is installed on a dedicated Linux Server as the Kyndryl Resiliency Orchestration Primary server. The server software requires the Kyndryl Resiliency Orchestration Server Platform package and MariaDB software to be installed on the same server.

The cluster management system features data integrity and application availability, using redundant hardware, shared disk storage, power management, robust cluster communication, and application failover mechanisms.

Perform the following steps on the dedicated Linux Server to install and setup the Kyndryl Resiliency Orchestration Primary Server:

1. Install the Red Hat Enterprise Linux Server OS (Refer to Supported OS for Kyndryl Resiliency Orchestration and Site Controller for the version to install).

49. Install Linux Cluster with these configurations: DLM mode, GFS Shared file system with a minimum of 30 GB, IP service and script service for MariaDB, and Kyndryl Resiliency Orchestration.
50. Install MariaDB. Refer to the Supported versions of MariaDB for the version to install.
51. Install the Kyndryl Resiliency Orchestration Server Software.
52. Set up the environment.

> **Note**
>
> Refer to Step 5 under Installation of Kyndryl Resiliency Orchestration Server Platform on Linux Cluster Nodes to set up the environment.

Follow the sections given below to complete the Kyndryl Resiliency Orchestration Server installation.

6.2.1 Installation of Linux Enterprise Server OS

1. Install the Linux Enterprise Server OS without firewall settings and MariaDB database package.

Kyndryl Resiliency Orchestration uses the following ports:

- For accessing the Resiliency Orchestration GUI - ports 8443
- For communication among the Resiliency Orchestration and Site Controller, and Agents – ports 42443 and 45443

> **Note:**
>
> Ensure to allow the required ports when configuring the Firewall at the Operating System level.

53. Allow the software to install the packages selected by default and choose all packages available under the 'Development' list, and make sure that "Postgre SQL Database and MariaDB Database" are not selected under the 'Server' list. Do not click the "**Details**" hyperlink to make further selections.
54. Edit the file `/etc/sysconfig/selinux` to include the option `"SELINUX=permissive"`.
55. Check `/etc/hosts` file to ascertain if the localhost alias exists. If it doesn't exist, add the localhost alias, and the IP address of the Kyndryl Resiliency Orchestration Server system.

For Example:

<ip-address> <hostname>

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

6.2.2 Installation of Linux Cluster

Install Linux Cluster version for Kyndryl Resiliency Orchestration OS version with DLM Mode for GFS shared volume and IP service. To install and configure the Linux cluster refer to the following documents:

RED HAT Cluster suite rh-cs-en-4 and rh-gfs-en-6_1 from RED HAT

kyndryl

6.2.3 Additional Settings for Linux Installation

1. Open a terminal, log in as root and issue the following command, whenever the system is rebooted.

```
# /sbin/sysctl -w net.ipv4.tcp_retries2=4
```

56. To avoid this, perform the following steps:

    - Open the 'conf' file by issuing the following command:

```
vi /etc/sysctl.conf
```

    - Add the following statement and save it:

```
edit /etc/sysctl.conf with "net.ipv4.tcp_retries2=4" at the
end of the file.
```

57. Reboot the system.

6.2.4 Installation of Kyndryl Resiliency Orchestration Server Platform on Linux Cluster Nodes

Use the "clusvcadm" utility to relocate user services between cluster nodes for installation, and perform the following steps to install the Kyndryl Resiliency Orchestration Server platform on two cluster nodes, for example, can be Cluster Node A and Cluster Node B.

1. Create a directory titled 'mysql' in <shared cluster volume> by issuing the following command, only if it does not exist:

```
cd /<shared volume>

mkdir mysql
```

58. Create a Soft link for the 'Mysql' Database folder by issuing the following command:

```
cd /var/lib

ln –s <shared Cluster Volume>/mysql /mysql
```

59. Create a 'panaces' folder under the shared volume. To create it, run the following command at the shared volume:

```
mkdir <shared volume> /panaces
```

60. Once the "panaces" link is created, check for its existence with the following command:

```
ls panaces (or) ls
```

61. Set up environment variable EAMSROOT to /opt/panaces at the command line:

```
export EAMSROOT=/opt/panaces
```

6.2.5 Post-Installations of Kyndryl Resiliency Orchestration Server Platform on Linux Cluster

Use the "clusvcadm" utility to relocate a cluster to a cluster node, for example, Cluster Node A, and perform the following steps:

1. Start MariaDB services whenever the system is rebooted by issuing the following command:

```
# /etc/init/mysql start &
```

62. Check whether you can log in to MariaDB as a root or root privileged username using the following command:

```
# mysql -u <username>
```

6.2.6 Installation of Resiliency Orchestration Server Software

For the procedure to install Kyndryl Resiliency Orchestration Server software, refer to the section *Installation of Resiliency Orchestration Server*.

6.3 Starting and Stopping Resiliency Orchestration Server

For the procedures to start and stop Kyndryl Resiliency Orchestration Server, see *Starting and Stopping Resiliency Orchestration Server*.

6.4 Configuring Linux Cluster

The following information applies to the Red Hat Enterprise Linux 7 Server edition.

In the Linux Cluster, configure MariaDB and Kyndryl Resiliency Orchestration application startup files as script files for application failover. Linux Cluster will start and stop the application from these script files.

To configure MariaDB and Kyndryl Resiliency Orchestration applications on the cluster, create the following scripts files on /opt/panaces/bin folder.

Create Mysqlbat. The sh file for MariaDB Server and type the following code:

```
start()

{

sh /etc/init.d/mysql start

}

stop()

{
```

```
sh /etc/init.d/mysql stop
}
status()
{
mysqladmin status
}
if [ "#1" = "start" ] ; then
    start
elif [ "#1" = "stop" ] ; then
    stop
elif [ "#1" = "status" ] ; then
   status
fi
```

6.4.1 Checking the Application Status by Exit Code (Linux Cluster)

For Kyndryl Resiliency Orchestration Linux cluster integration, add the following exit code value in the installation folder/panaces/bin/panaces.sh file.

Find the **status()** function in the panaces file. Add exit 9 as given in the code below:

```
status()
{ add the following case in Panaces Binary
  panaces_running
  if [ #? = 0 ] ; then
        echo "Panaces server is not running"
exit 9
  else
        echo "Panaces server is running"
```

```
    fi


    tomcat_running
    if [ #? = 0 ] ; then
          echo "Tomcat server is not running"
          exit 9
    else
          echo "Tomcat server is running"
    fi
}
```

A sample Cluster Configuration is given below:

```
<resources>
<clusterfs device="/dev/sdb1" force_unmount="1" fstype="gfs"
mountpoint="/panacs" name="mygfs" options=""/>
  <ip address="<IP>" monitor_link="1"/>
  <script file="/opt/panaces/bin/panaces.sh" name="Panaces"/>
  <script file="/opt/panaces/bin/mysqlbat.sh" name="mysql"/
</resources>
```

> **Note**
>
> After the installation is complete, relocate the cluster and test the application's function from both servers.

6.4.2 Linux Cluster Administration

For Linux cluster administration, refer to Red Hat Linux Documentation.

kyndryl

7 Configuring Resiliency Orchestration Server

You can configure the Resiliency Orchestration application Server for the following mandatory and optional features:

Mandatory Features

- Configuring the Resiliency Orchestration application to use the MariaDB
- Server (OS) Hardening
- Running the SecurityUserInjection script

Optional Features

- Configuring Resiliency Orchestration for Optimal Performance
- Configuring Resiliency Orchestration to use the Resiliency File Replicator

7.1 Configuring the Resiliency Orchestration application to use the MariaDB

The Resiliency Orchestration application software is installed with preset User credentials for accessing the MariaDB. You can configure Kyndryl Resiliency Orchestration application software to use different MariaDB user credentials.

You must first set up new user credentials after installing MariaDB. For instructions, see *Creating New Users in MariaDB*. Ensure that the new user you create in the MariaDB is set up with all privileges.

To configure the Resiliency Orchestration application software for the new MariaDB user, complete the following steps:

1. Navigate to the directory where the Resiliency Orchestration application software is installed, by entering the following command at the command prompt:

```
# cd installconfig
```

63. In this directory, enter the following command at the command prompt to display the properties file for the Resiliency Orchestration application:

```
# vi panaces.properties file
```

64. In the **panaces.properties** file, change the preset value for the parameter `panaces.mysql.username` to the new username that you created in MariaDB. The preset parameter for the MariaDB user is set as `panaces`.

```
panaces.mysql.username = <new mariadb user>
```

65. Save and close the **panaces.properties** file.

7.2 Configuring Resiliency Orchestration with different MariaDB user passwords

When password(s) for the MariaDB users are changed, perform the following steps to configure Kyndryl Resiliency Orchestration with the new password.

1. Navigate to the user installation directory (where Kyndryl Resiliency Orchestration Server is installed). To navigate to the *bin* directory, enter the following command at the command prompt:

```
# cd bin
```

66. To provide the MariaDB user password for Resiliency Orchestration Server, run the following command:

```
# sudo ./changeDBPassword.sh panaces.mysql.password
```

67. Upon running the above command, you will be prompted to provide the password. Provide the password and press 'enter'. Password(s) provided will be encrypted and saved into the **panaces.properties** file.

7.3 Server Operating System Hardening (Optional)

Complete the following steps to harden the Resiliency Orchestration Server.

Note

- You can follow your company's IT policy for hardening the Resiliency Orchestration Server, as this hardening section is optional
- You will need to create a root equivalent sudo user as these steps will disable the root user. –
- The user 'sanovi' will have specific application-specific commands as configured in the steps below.
- $EAMSROOT will point to the Resiliency Orchestration installation directory. For In the following steps /opt/panaces are used as $EAMSROOT. Please replace /opt/panaces with an absolute path of $EAMSROOT.

1. Log in with root or root equivalent user
2. Set the password for the Kyndryl user

```
passwd sanovi
```

3. Change to the bin directory

```
cd /opt/panaces/bin
```

4. Execute the script to secure the server –

kyndryl

For RHEL 7.x execute:

```
./serverHardening.sh
```

For RHEL 8 execute:

```
./serverHardening_rhel8.sh
```

5. Delete the following entry from /etc/sudoers

```
sanovi  ALL=(ALL)       NOPASSWD: ALL, !/bin/su
```

6. Update the /etc/sudoers file with the below content

Note: Ensure to replace /opt/panaces with an absolute path of $EAMSROOT.

User_Alias USERS = sanovi

Cmnd_Alias NCMDS =/usr/bin/ls,/usr/bin/cd,/opt/panaces/bin/AIXOSAgent.sh,/opt/panaces/bin/AS400Agent.sh,/opt/panaces/bin/AS400OSAgentGeneric.sh,/opt/panaces/bin/AddDefaultUserRoles.sh,/opt/panaces/bin/AddPolarEventsMapping.sh,/opt/panaces/bin/AddRepeatableRAL.sh,/opt/panaces/bin/AddSignature.sh,/opt/panaces/bin/AgBulkUploadCLI.sh,/opt/panaces/bin/AgentNodeToSiteControllerUpgrade.sh,/opt/panaces/bin/AppToFGMapProcessor.sh,/opt/panaces/bin/AutomatePortTunnel.sh,/opt/panaces/bin/AwsAgent.sh,/opt/panaces/bin/AwsAgentStartup.sh,/opt/panaces/bin/BCSApplicationGroupUpgradeUtility.sh,/opt/panaces/bin/BCSVMReplicationUpgradeUtility.sh,/opt/panaces/bin/BlockreplicatorAgent.sh,/opt/panaces/bin/BulkUploadCLI.sh,/opt/panaces/bin/CISCO5000RAgent.sh,/opt/panaces/bin/CISCO5000RAgentGeneric.sh,/opt/panaces/bin/CRPlatformGCVersioningUpgrade.sh,/opt/panaces/bin/CheckinInstallerBinaries.sh,/opt/panaces/bin/ComponentCredUpdate.sh,/opt/panaces/bin/DB2UpgradeUtility.sh,/opt/panaces/bin/DBTierUpgrade.sh,/opt/panaces/bin/DRMAgentsStart.sh,/opt/panaces/bin/DRMAgentsStatus.sh,/opt/panaces/bin/DRMAgentsStop.sh,/opt/panaces/bin/DRMChangeUserMgmtMode.sh,/opt/panaces/bin/DRMSupportUserPasswordChange.sh,/opt/panaces/bin/DataGuardAgent.sh,/opt/panaces/bin/DefaultWorkflowCreatorForAllGroup.sh,/opt/panaces/bin/EnableRPORTOForGroup.sh,/opt/panaces/bin/EncryptDirectoryServerPassword.sh,/opt/panaces/bin/EventUpgradeUtility.sh,/opt/panaces/bin/EventUpgradeUtilityForDB2.sh,/opt/panaces/bin/ExchangeRS-TypeDef.sh,/opt/panaces/bin/FOTEUpgrade.sh,/opt/panaces/bin/GroupBulkUploadCLI.sh,/opt/panaces/bin/GroupContinuityStatusUpgradeUtility.sh,/opt/panaces/bin/GroupProtectionUpgrade.sh,/opt/panaces/bin/HMCAgent.sh,/opt/panaces/bin/HPUXOSAgent.sh,/opt/panaces/bin/HPXPAgent.sh,/opt/panaces/bin/IBMBRAppStackDiscovery.sh,/opt/panaces/bin/IBMCSMProtectionBulkUploadCLI.sh,/opt/panaces/bin/IBMCloudAgent.sh,/opt/panaces/bin/IBMCloudAgentStartup.sh,/opt/panaces/bin/IBMDS8000Agent.sh,/opt/panaces/bin/IBMDS8000AgentGeneric.sh,/opt/panaces/bin/IBMGM-TypeDef.sh,/opt/panaces/bin/LinuxOSAgent.sh,/opt/panaces/bin/LinuxOSAgentGeneric.sh,/

opt/panaces/bin/MIMIXAgent.sh,/opt/panaces/bin/MIMIXAgentGeneric.sh,/opt/panaces/bin/MSExchAgent.sh,/opt/panaces/bin/MSSQLAgent.sh,/opt/panaces/bin/MSSQLSecurityUpgradeUtility.sh,/opt/panaces/bin/ManageComponent.sh,/opt/panaces/bin/ManagerDashboardUpgrade.sh,/opt/panaces/bin/MySQL-SR-peDef.sh,/opt/panaces/bin/MySQLAgent.sh,/opt/panaces/bin/NetAppAgent.sh,/opt/panaces/bin/OpenVMSAgent.sh,/opt/panaces/bin/OracleAgent.sh,/opt/panaces/bin/PFRAgent.sh,/opt/panaces/bin/PFRChangeUserMgmtMode.sh,/opt/panaces/bin/PFRSupportUserPasswordChange.sh,/opt/panaces/bin/PanacesBlobUpgrade.sh,/opt/panaces/bin/PanacesUpgrade.sh,/opt/panaces/bin/PanacesUpgradeRemoteAgents.sh,/opt/panaces/bin/PostgreSQL-SR-TypeDef.sh,/opt/panaces/bin/PostgresAgent.sh,/opt/panaces/bin/PurgeMysqlLogs.sh,/opt/panaces/bin/RegisterPolicies.sh,/opt/panaces/bin/Remote_host_permission.sh,/opt/panaces/bin/ReportsMigration.sh,/opt/panaces/bin/ResourceMapping.sh,/opt/panaces/bin/SAPHANAAgent.sh,/opt/panaces/bin/SRDFAgent.sh,/opt/panaces/bin/SRMCLI.sh,/opt/panaces/bin/SecurityPassphraseUpgradeUtility.sh,/opt/panaces/bin/SecurityUpgradeUtility.sh,/opt/panaces/bin/SecurityUserInjection.sh,/opt/panaces/bin/SiteController.sh,/opt/panaces/bin/SnapMirrorTypeDef.sh,/opt/panaces/bin/SolarisOSAgent.sh,/opt/panaces/bin/SpectrumBulkUploadCLI.sh,/opt/panaces/bin/SybaseAgent.sh,/opt/panaces/bin/SybaseSecurityUpgradeUtility.sh,/opt/panaces/bin/SystemCreatedGroupsUpdate.sh,/opt/panaces/bin/TrueCopyAgent.sh,/opt/panaces/bin/UCSDAgent.sh,/opt/panaces/bin/UniAgentComponentInfo.sh,/opt/panaces/bin/UniAgentConsolidation.sh,/opt/panaces/bin/Uninstaller.sh,/opt/panaces/bin/UnlockUserAccount.sh,/opt/panaces/bin/UpdateComponentKeyPair.sh,/opt/panaces/bin/UpdateDBAfterInilization.sh,/opt/panaces/bin/UpgradePasswordToAES.sh,/opt/panaces/bin/UpgradePasswordToSHA256.sh,/opt/panaces/bin/UpgradeSignature.sh,/opt/panaces/bin/VMClient.sh,/opt/panaces/bin/VMSSERVERAgent.sh,/opt/panaces/bin/VaultAgent.sh,/opt/panaces/bin/VaultMetadataUpgrade.sh,/opt/panaces/bin/VcenterAgent.sh,/opt/panaces/bin/VcenterUpgradeUtility.sh,/opt/panaces/bin/VmwareAgent.sh,/opt/panaces/bin/VmwareAgentStartup.sh,/opt/panaces/bin/VmwareVmotionDetection.sh,/opt/panaces/bin/WMIToPowerShellUpgrade.sh,/opt/panaces/bin/WindowsOSAgent.sh,/opt/panaces/bin/WorkFlowImportFromCLI.sh,/opt/panaces/bin/ZOSAgent.sh,/opt/panaces/bin/ZOSBulkUploadCLI.sh,/opt/panaces/bin/ZertoAgent.sh,/opt/panaces/bin/ZertoAgentStartup.sh,/opt/panaces/bin/apptemplate.sh,/opt/panaces/bin/changeDBPassword.sh,/opt/panaces/bin/changeRepositoryAdminUserPassword.sh,/opt/panaces/bin/common-localization.sh,/opt/panaces/bin/common-unix.sh,/opt/panaces/bin/common-win.sh,/opt/panaces/bin/common.sh,/opt/panaces/bin/commonNetwork.sh,/opt/panaces/bin/commonStorage.sh,/opt/panaces/bin/drmagents_env,/opt/panaces/bin/drmlogadmin,/opt/panaces/bin/drmlogs.sh,/opt/panaces/bin/drmtype.sh,/opt/panaces/bin/enableEncryptionOnTables.sh,/opt/panaces/bin/encryptPassword.sh,/opt/panaces/bin/etl.sh,/opt/panaces/bin/events_info.sh,/opt/panaces/bin/export-event.sh,/opt/panaces/bin/import-event.sh,/opt/panaces/bin/importDefinitionForTemplate.sh,/opt/panaces/bin/initializeJackRa

bbitRepositry.sh,/opt/panaces/bin/invokeAgentCommand.sh,/opt/panaces/bin/licenseUpgrade.sh,/opt/panaces/bin/panaces,/opt/panaces/bin/panaces_env,/opt/panaces/bin/raiseEvent.sh,/opt/panaces/bin/sas_env,/opt/panaces/bin/serverHardening.sh,/opt/panaces/bin/startDRMAnalyticsEngine.sh,/opt/panaces/bin/startVMProtection.sh,/opt/panaces/bin/startWorkflowExporter.sh,/opt/panaces/bin/updateEventDisplayName.sh

```
USERS ALL = NCMDS
```

68. Reboot the server to take effect of changes for server hardening with the following command

    ```
    reboot
    ```

69. Since the root user is disabled, log in using the `sanovi` user
70. Change the directory by entering the following command:

    ```
    cd $EAMSROOT
    ```

    As the server is hardened now, you must prefix sudo for all commands you run subsequently. For example, to start Resiliency Orchestration services, you can run the following command:

    ```
    sudo ./panaces start
    ```

71. Run the SecurityUserInjection script. For instructions, see *Running the SecurityUserInjection script*.

> **Important:**
>
> In case the optional Server Hardening script has been executed and if any files or folders have been added or any permission changes are done under EAMSROOT/ or $TOMCAT_HOME/, then execute the following command.
>
> cd $EAMSROOT/bin
>
> sudo ./SecurityUserInjection.sh.

7.4 Running the SecurityUserInjection script

Post the Server OS hardening for the first time, and ensure that you run the SecurityUserInjection script before you edit or add files or folders in the Resiliency Orchestration application software.

Complete the following steps to run the SecurityUserInjection script:

1. Go to $EAMSROOT/bin/

72. Run the following command:

```
sudo SecurityUserInjection.sh
```

7.5 Configuring Resiliency Orchestration for Optimal Performance

Depending on the expected number of groups that will be supported by Kyndryl Resiliency Orchestration Software, the Java maximum heap memory limit parameter needs to be specified. This is defined in the variable named DRM_SERVER_JVM_MEM, which is located at starting lines of the Resiliency Orchestration startup script *panaces* located at $EAMSROOT/bin/. The default value of this variable is set to -Xmx2048m.

Update the following parameters as shown in Table 17 for optimal performance depending on the expected number of recovery groups for your installation:

Table 17. Configuring Resiliency Orchestration Server for optimal performance

No. of Recovery Groups	File Name and Path	Parameters	Value
250	/etc/my.cnf	max_connections	1000
	$EAMSROOT/installconfig/panaces.properties	panaces.mysql.maxconnection	750
	$EAMSROOT/installconfig/panaces.properties	panaces.acp.server.concurrentRequestProcessCount	500
500	/etc/my.cnf	max_connections	1500
	$EAMSROOT/installconfig/panaces.properties	panaces.mysql.maxconnection	1000
	$EAMSROOT/installconfig/panaces.properties	panaces.acp.server.concurrentRequestProcessCount	1000

- The **panaces.acp.server.concurrentRequestProcessCount** parameter is used to set the number of threads that process the messages from agents.

- The **panaces.mysql.maxconnection** parameter is used to set the number of open mysql connections to DB.

  Note: It is recommended to set the **panaces.mysql.maxconnection** property value to ~65% of **max_connections** (/etc/my.cnf).

- **Note**: In panaces.property check values of

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

  This concurrentRequestProcessCountMax property should be equal or greater than concurrentRequestProcessCount.

For optimal performance, you can set the number of processes for Resiliency Orchestration and Linux Site Controller at a value approximate to 10000. You can set this limit in **/etc/security/limits.conf** file. Edit this file by altering or appending the following to set the limit:

```
root            soft    nproc           10240
root            hard    nproc           10240
root            soft    nofile          20480
root            hard    nofile          20480
panacesuser       soft     nproc        10240
panacesuser         hard   nproc        10240
panacesuser         soft   nofile       20480
panacesuser         hard   nofile       20480
```

In linux site controller if the agent count is more than 150 agents, set the below recommend limits:

```
panacesuser       soft     nproc                16384
panacesuser         hard   nproc                16384
panacesuser         soft   nofile               20480
panacesuser         hard   nofile               20480
```

kyndryl

For recommended guidelines, see Guidelines for setting ulimits (WebSphere Application Server) (ibm.com) and Operating system user limit requirements (Linux and UNIX) - IBM Documentation.

After making these changes, restart the Resiliency Orchestration Application Server and Linux Site Controller. For instructions to start the Resiliency Orchestration Server, see *Starting and Stopping Resiliency Orchestration Server*.

7.5.1 Swapiness Value Configuration for Linux RO Server

Use 60 as a value for swappiness for both RO and Site controller including HAs.

7.6 Configuring Resiliency Orchestration for Security

TLS protocol is used for communication between the Kyndryl Resiliency Orchestration server and the Agents.

By default, Kyndryl Resiliency Orchestration Server and Agents communication are secure with TLS using TLSv1.2 protocol with a strong cipher.

Resiliency Orchestration also provides support for lower communication protocols: SSL and NONSECURE for communication between Resiliency Orchestration Server and Agents.

The property `panaces.acp.communicationType` in `<EAMS ROOT>/installconfig/panaces.properties` are used to set the communication protocol between the Resiliency Orchestration Server and Agents.

You need to configure the Resiliency Orchestration Server and Agents to use the same communication type.

Table 18: Resiliency Orchestration Server and Agents

Resiliency Orchestration Server	Local Agents (N)*	Local Agents (N-1)**
SECURE	SECURE	SECURE
NONSECURE	NONSECURE	NONSECURE
SECUREWITHTLS	SECUREWITHTLS	SECUREWITHTLS

* (N) is the current local agent.
** (N-1) is the previous local agent over which the current local agent is installed.

Following properties in the panaces.properties file enables the user to choose a specific communication protocol and cipher. The communication protocol used is TLS 1.2 by default and is configurable.

```
panaces.acp.communicationTLSProtocolVersion = TLSv1.2
```

By default, the following ciphers are present in panaces.properties file

```
panaces.acp.communicationTLSCipher=TLS_DHE_RSA_WITH_AES_256_GCM_SHA38
4,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_
SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256
_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AE
S_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
```

If you wish to customize your cipher, please refer to https://www.owasp.org/index.php/TLS_Cipher_String_Cheat_Sheet

Note:

It is recommended to have the same ciphers for the Kyndryl Resiliency Orchestration server and the Agents.

7.6.1 Authenticating two-way TLSv1.2

The communication between the Kyndryl Resiliency Orchestration server and the Site Controller is by default two-way TLS. From Kyndryl Resiliency Orchestration version 8.0.2.0 onwards the product has been enhanced to support two-way TLS authentication between Agents and Kyndryl Resiliency Orchestration server/Site Controller. This section describes how to leverage this enhanced security feature.

A server can be configured to allow connections from any client (like in one-way TLS) or it can be configured to ask any clients that attempt to connect to it to get authenticated. Therefore, for a client to get authenticated, it requires a client certificate. In two-way TLS authentication, aka TLS with client certificate authentication, the client certificate is also involved in addition to the server certificate for hardening the authentication process. Just like a server certificate, a client certificate contains basic information about the client's identity, its public key and the digital signature of a CA on this certificate verifies that this information is authentic. The client certificate should be signed by a CA that the server trusts and it is obvious that both X.509 certificates should exist before the connection.

Prerequisite -

Two-way TLSv1.2 authentication between Agents and Kyndryl Resiliency Orchestration server/Site Controller should be enabled only after Kyndryl Resiliency Orchestration server, Site Controller, and all Agents are installed/upgraded to the 8.0.2.0 or above version.

7.6.1.1 Configurations in Kyndryl Resiliency Orchestration Server and Site Controller

In the Kyndryl Resiliency Orchestration server, the properties present in the panaces.properties file should be set as shown in ***Properties 1 - Kyndryl RO Server properties*** to enable two-way TLSv1.2 authentication between Agents and Kyndryl Resiliency Orchestration server.

```
panaces.acp.communicationTLSProtocolVersion = TLSv1.2
panaces.acp.security.tls.two-way.authentication.enable=true
```

Properties 1 - Kyndryl RO Server properties

In Site Controller, the properties present in files SiteController.cfg and panaces. properties should be set as shown in ***Properties 2 - Site Controller properties*** to enable two-way TLSv1.2 authentication between Agents and Site Controller.

```
SC_TLS_PROTOCOL_VERSION=TLSv1.2
panaces.acp.security.tls.twoway.authentication.enable=true
```

Properties 2 - Site Controller properties

In both the Kyndryl Resiliency Orchestration server and Site Controller, the `panaces.acp.security.tls.two-way.authentication.enable` property will be false by default. It should be set to true for two-way to be enabled.

Important - Failing to enable the properties mentioned in ***Properties 1 - Kyndryl RO Server properties*** and ***Properties 2 - Site Controller properties*** will result in a connection failure.

Whenever there is any update of two-way TLS related properties in the Site Controller or Kyndryl Resiliency Orchestration server, the corresponding panaces services should be restarted for the change to take effect.

Note:

a. Both Kyndryl Resiliency Orchestration server and Site Controller should be updated with the ***Properties 1 - Kyndryl RO Server properties*** and ***Properties 2 - Site Controller properties*** to use two-way TLS.

b. If the ***Properties 1 - Kyndryl RO Server properties*** and ***Properties 2 - Site Controller properties*** are not set in both Kyndryl Resiliency Orchestration server and Site Controller, the communication mode will be the default, which is one-way TLS.

The communication between the Kyndryl Resiliency Orchestration server and Site Controller is via ActiveMQ and two-way TLS authentication is enabled by default. Keystore and truststore entries are present with default privateKeyEntry and publicKeyEntry. However, we recommend using self-signed certificates. To configure your panacesACP.keystore and panacesACP.truststore entries, the files under $EAMSROOT/tools/apache-activemq-5.13.2/conf directory have to be updated in both the Kyndryl Resiliency Orchestration server and the Site Controller***.*** Failing to update at either end will cause a connection failure.

Whenever there is a key update on either the client or the server, panaces services restart is required for both parties involved in the connection.

7.6.1.2 Configuring Local Agent for two-way TLS

By default, one-way TLS is enabled for Local Agent connection to Kyndryl Resiliency Orchestration server/Site Controller.

After installing/upgrading the agent to the 8.0.2.0 or above version, you will be provided with panacesACP.truststore and panacesACP.keystore files under $EAMSROOT/DRMAgents/installconfig/keystore directory.

The panacesACP.truststore will be pre-loaded with the default configuration. The panacesACP.keystore will be empty.

While enabling two-way TLS, make sure to update the panacesACP.keystore with private key entry, and also update the public key in the counterpart's (Kyndryl Resiliency Orchestration server/Site Controller) truststore. Failing to update the keystore of Agent and truststore (public key) in Kyndryl Resiliency Orchestration server/Site Controller will cause a communication failure.

Note - Adding to the trust store on Kyndryl Resiliency Orchestration server/Site Controller is required only if Agent's certificate is not issued by a well-known CA.

To generate self-signed certificates, please refer to *Generating Keystore and Truststore for Agent and Site Controller*.

7.6.1.3 Configuring Remote Agent for two-way TLS

By default, one-way TLS authentication is enabled for Remote Agent connection to Kyndryl Resiliency Orchestration server/Site Controller.

Once the Kyndryl Resiliency Orchestration server/Site Controller is set to two-way TLS by enabling properties mentioned in *Properties **1** - Kyndryl RO Server properties* and ***Properties 2 - Site Controller properties***, there is no further change required at the remote agent level.

7.7 Enabling Backward Compatibility for Communication between Kyndryl Resiliency Orchestration and the Agents

Important! For better security, it is recommended that you upgrade your local agents to the latest version.

The Kyndryl Resiliency Orchestration is preconfigured with TLS1.2. However, in case your installed Agents do not support TLS1.2, you can still use TLS1.0 or TLS1.1. Please make the following changes if you require a lower version of the protocol to be supported.

```
panaces.acp.communicationTLSProtocolVersion = TLSv1.2, TLSv1.1, TLSv1.0
```

Note: All the SSL & TLS versions older than 1.2 are having lots of known vulnerabilities. Hence we recommend using only TLS1.2.

7.8 Configuration Changes in Tomcat (Secure Access)

You must use the secure mode of GUI access. The following are the steps to enable a secure mode of GUI access:

1. Get the KEYSTORE file with the password.
   - The default Sanovi KEYSTORE file/Password(Certificate) is shipped with the product.
   - To use a Customer certificate, get the KEYSTORE file and password from the customer.

73. Open server.xml using, sudo vi **`$TOMCAT_HOME/conf/server.xml`**
74. Delete the following default connector.

    <Connector port="8080" redirectPort="8443" connectionTimeout="20000" protocol="HTTP/1.1"/>

75. Add/edit the below connectors with the following details to update the file: (Assuming EAMSROOT as /opt/panaces)

```
<Connector port="8443"
protocol="panaces.server.common.TomcatStoreKeyDecryption"
SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
keystoreFile="/opt/panaces/installconfig/keystore/sanovi.keystore"
```

```
keystorePass="<Password> " compression="on"
compressionMinSize="2048"
nocompressionUserAgents="gozilla,traviata"
compressableMimeType="text/html,text/xml,text/plain,text/cs
s,text/javascri
pt,text/json,application/x-
javascript,application/javascript,application/json"/>
```

7.9 Configuration Changes in Tomcat (Nonsecure to Secure Redirection)

You must use the secure mode of GUI access. The following are the steps to enable a secure mode of GUI access (redirects non-secure access to secure access):

1. Get the KEYSTORE file with the password.
    - The default Sanovi KEYSTORE file/Password(Certificate) is shipped with the product.
    - To use a Customer certificate, get the KEYSTORE file and password from the customer.

76. Open server.xml using, sudo vi **$TOMCAT_HOME/conf/server.xml**
77. Delete the following default connector.

    <Connector port="8080" redirectPort="8443" connectionTimeout="20000" protocol="HTTP/1.1"/>

78. Add/edit the below connectors with the following details to update the file: (Assuming EAMSROOT as /opt/panaces)
    - Use the following details for nonsecure to secure redirection configuration:

```
<Connector executor="tomcatThreadPool"
port="8080" protocol="HTTP/1.1"
connectionTimeout="60000"
redirectPort="8443"  compression="on"
compressionMinSize="2048"
 nocompressionUserAgents="gozilla,                traviata"
compressableMimeType="text/html,text/xml,text/plain,text/cs
s,text/javascri
pt,text/json,application/x-
javascript,application/javascript,application/json"/>
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
```

```
SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
keystoreFile="/opt/panaces/installconfig/keystore/sanovi.keystore"
keystorePass="<Password[1]>" compression="on"
compressionMinSize="2048"
nocompressionUserAgents="gozilla,traviata"
compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascri
pt,text/json,application/x-
javascript,application/javascript,application/json"/>
```

79. Open $TOMCAT_HOME/webapps/PanacesGUI/WEB-INF/web.xml

- Search for **servlet-mapping** --- at **/app/*.** The searched content displays the following snippet:

```
<servlet-mapping>
<servlet-name>spring</servlet-name>
<url-pattern>/app/*</url-pattern>
</servlet-mapping>
```

- Add the following content after **</servlet-mapping>**

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Entire Application</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

- Open web.xml using, sudo vi $TOMCAT_HOME/conf/**web.xml** and set the session config value to 20 as shown below for additional security.
- <session-config>
  <session-timeout>20</session-timeout>

</session-config>”Restart the Resiliency Orchestration services, with the following command:

```
sudo $EAMSROOT/bin/panaces restart
```

A Port number is not required in the URL for accessing Resiliency Orchestration and Kyndryl Resiliency File Replicator GUI through the browser.

For Example: If the user enters the web URL as http:// <Resiliency Orchestration IP>/PanacesGUI, it is auto-redirected to https:// =<Resiliency Orchestration IP>/PanacesGUI

7.10 Generating Custom Certificates (Keystore) (Optional)

Resiliency Orchestration agent communication certificates are used by RO to communicate securely with Sitecontrollers and Agents. To enable secure mode of GUI access RO GUI secure certificate is used.

These certificates are available by default to the user on installing the RO.

But users are recommended to create certificates with their own passwords to ensure more security.

There are two ways of generating certificates: Automated and Manual.

7.10.1 Prerequisites

JDK needs to be installed.

7.10.2 Automated way of Generating RO GUI certificates , RO agent communication certificates (panacesACP.keystore, panacesACP.truststore, and sanovi.keystore) for RO and Agent/Site Controller:

Generating PanacesACP keystore/truststore through Shell Script

Notes:

- Keystore/Truststore password supports Alphabets, Numbers and following special characters ~ ! @ # % ^ & * ( ) _ - + = { } [ ] / , . ; ? : | only. $ < > " ' ` \ and Space are NOT supported in the password.

- When new panacesACP keystore and truststore are generated in RO , the new panacesACP.trustore has to be copied from RO to the below locations of all the local agents. Only then local agent gets connected to RO/SC

    - EAMSROOT/DRMAgents/installconfig/keystore
    - EAMSROOT/UpgradeAssist/installconfig/keystore.

Also, copy the panaces.acp.truststorePassword from EAMSROOT/installconfig/panaces.properties of RO to panaces.acp.truststorePassword in EAMSROOT/DRMAgents/installconfig/panaces.properties of local agent . Then restart the services in agent.

Steps:

1. User can generate new panacesACP certs using "Generate_panacesACP.keystore-panacesACP.truststore.sh" script under EAMSROOT/bin/GenerateCerts folder.

2. Input required for cert generation has to be filled in params.txt file available in the same folder.

3. User can run the script after filling the params.txt file.

4. On running this script, user will be asked few confirmations. Once user proceeds , user has to enter the password to be used for generating keystore/trustore files when prompted.

5. On completion of script execution, new panacesACP.keystore and panacesACP.trustore will be created and copied to EAMSROOT/installconfig/keystore , EAMSROOT/tools/activemq/conf

6. Before copying the new keystore files, existing keystore/trustore backup will be taken by the script and placed in the same folder.

7. Script also updates the password used to create cert in panaces.properties , SiteController.cfg (these files are available in EAMSROOT/installconfig), credentials-enc.properties, jetty.xml(these two files are located in EAMSROOT/tools/activemq/conf)

8. Before updating these files with the new password, back up of them will be taken by the script and placed in the same folder.

kyndryl

9. Copy the panaceACP.keystore, panacesACP.truststore , Replace_Keystores_LinSC.sh, temp.txt files from EAMSROOT/bin/GenerateCerts to /tmp directory of all the Linux SC s mapped to RO.

10. Execute the Replace_Keystores_LinuxSC.sh as ROOT user from all the Linux SC s mapped to the RO so that the new certs gets copied to the Linux SC also.

11. Copy the panaceACP.keystore,panacesACP.truststore,Replace_Keystores_WinSC.bat,temp.txt files from eamsroot/bin/GenerateCerts to C:\ (C drive)of all the Win SC s mapped to the RO.

12. Execute the Replace_Keystores_WinSC.bat as administrator from cmd prompt of all the Win SC s mapped to the RO so that the new certs gets copied to the Win SC also.

13. Running the above script in Lin SC, new certs gets copied in EAMSROOT/installconfig/keystore , EAMSROOT/tools/activemq/conf ,passwords are updated in panaces.properties , SiteController.cfg (these files are available in EAMSROOT/installconfig), credentials-enc.properties, jetty.xml(these two files are located in EAMSROOT/tools/activemq/conf).

14. Running the script in WinSC, new certs gets copied in EAMSROOT/installconfig/keystore , EAMSROOT/tools/windows/activemq/conf ,passwords are updated in panaces.properties , SiteController.cfg (these files are available in EAMSROOT/installconfig), credentials-enc.properties, jettysc.xml(these two files are located in EAMSROOT/tools/windows/activemq/conf).

15. After the execution of all these three scripts, RO/Lin SC/Win SC should be up and running and the SC status should be connected in RO.

16. Once RO, SC are connected to each other, user should delete the temp.txt file in eamsroot/bin/GenerateCerts location from RO.

Generating sanovi.keystore through Shell script

1. User can generate sanovi.keystore by executing Generate_sanovi.keystore.sh under EAMSROOT/bin/GenerateCerts folder.

kyndryl

2. Before executing this script, user has to fill the sanovikeystore_params.txt file available in the same folder.

3. On running the script, user will be asked to enter the password to be used for generating sanovi.keystore. Keystore password supports Alphabets, Numbers and following special characters ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] /, . ; ? : | only. < > " ' ` \ and Space are NOT supported in the password.

4. Once script execution gets completed, new sanovi.keystore gets created and placed in EAMSROOT/installconfig/keystore.

5. Password used for generating the keystore, is updated in the TomcatHome/conf/server.xml and EAMSROOT/installconfig/resources/jetty.xml by the script.

6. Once script execution completed, RO should be up and running and user should be able to access through RO UI also.

7.10.3 Manual steps for creating RO GUI certificates , RO agent communication certificates (panacesACP, keystore/truststore and sanovi.keystore)

Note: When new panacesACP keystore and trustore are generated in RO , the new panacesACP.trustore has to be copied from RO to the below locations of all the local agents. Only then local agent gets connected to RO/SC

- EAMSROOT/DRMAgents/installconfig/keystore
- EAMSROOT/UpgradeAssist/installconfig/keystore

Also, copy the panaces.acp.truststorePassword from EAMSROOT/installconfig/panaces.properties of RO to panaces.acp.truststorePassword in EAMSROOT/DRMAgents/installconfig/panaces.properties of local agent.Then restart the services in agent.

Execute the following commands in any RO where new certs are to be created :

You can go to a tmp folder for key generation, say (/tmp/certs). Under that, you can do below.

```
1. openssl genrsa -out serverCA.key 2048
```

kyndryl

2. `openssl req -x509 -new -nodes -key serverCA.key -sha256 -days <enter no.of days for cert to be valid> -out serverCA.pem`

3. `openssl pkcs12 -export -name server-cert -in serverCA.pem -inkey serverCA.key -out serverkeystore.p12`

4. `keytool -importkeystore -destkeystore panacesACP.keystore -srckeystore serverkeystore.p12 -srcstoretype pkcs12 -alias server-cert`

5. `keytool -import -alias server-cert -file serverCA.pem -keystore panacesACP.truststore`

Notes:

- After executing the 3rd command, user will be asked to enter export password(plain text password). It is recommended to choose a strong password that has a mix of alpha-numeric characters and special characters, with a minimum length of 25. Special characters other than space character is allowed. Special characters supported are ~ ! @ # % ^ & * ( ) _ - + = { } [ ] / , . ; ? ' : |

- After executing 4rth command, user will be asked to enter source and destination password where both are same as the export password used in 3rd command. Also this password will be considered as keystore password.

- After executing 5th command, user has to enter another plaintext password which will be considered as truststore password.

After executing these commands,user can find panacesACP.keystore , panacesACP.truststore files under /tmp/certs folder.Now copy these keystore/truststore files to the below paths.

1) eamsroot/installconfig/keystore --- in RO /Lin SC/Win SC

2) eamsroot/tools/activemq/conf ---- in RO and Lin SC

3) eamsroot/tools/windows/activemq/conf ------ in Win SC

4) after moving run securityinjection in RO/SC

kyndryl

5) Encrypt keystore plain text password(used in command 4 above) and truststore plain text password (used in command 5 above).using encryptPassword.sh under EAMSROOT/bin and Update below parameters with encrypted password in panaces.properties and SiteController.cfg files:

- panaces.acp.keystorePassword
- panaces.acp.truststorePassword

5)encrypt using activemq encrypt and update it in credentails-enc.properties (Encrypt ActiveMQ passwords and update configuration files. The script to encrypt the password for ActiveMQ is in $EAMSROOT/tools/apache-activemq-5.13.2/bin.

Example :

./activemq encrypt --password <Password> --input "<Password>"

!&|',. ; ? : /~() ---- these special characters should be escaped with \ before them while encryption

where --password is the secretkey and --input is the storepassword of the keystores.

The secretkey can be seen in the file $EAMSROOT/tools/apache-activemq-5.13.2/bin/env

ACTIVEMQ_ENCRYPTION_PASSWORD=<Password[1]>

[1]Connect with the Support/Delivery team to get the default passwords.

The output of the encrypted text should be placed in credentials-enc.properties, which is in

$EAMSROOT/tools/apache-activemq-5.13.2/conf/credentials-enc.properties. - for RO/Lin SC

$EAMSROOT/tools/windows/apache-activemq-5.13.2/conf/credentials-enc.properties - for Win SC

Update values corresponding to keystore password and truststore. password as shown in the example here.

Example -

keystore.password=<Password>(Encrypted keystore Password)

truststore.password=<Password> (Encrypted truststore Password)

6) Update the below parameter in jetty.xml file under $EAMSROOT/tools/apache-activemq-5.13.2/conf with the keystore plain password in RO/Linux SC like the below

Note : if the password contains & , it should be updated as & in jetty.xml

```
<property name="keyStorePassword" value="keystore plain text password"
/>
```

7) In Win SC, update $EAMSROOT/tools/windows/activemq/conf/jettysc.xml with keystore plain text password.

Note : if the password contains & , it should be updated as & in jettysc.xml

8)Restart panaces services in RO and SC services in the respective SC s so that the new certs becomes effective

Steps to generate sanovi.keystore

```
keytool -genkey -alias sanovi_keystore keyalg RSA -keysize 2048  -
validity <enter no.of days for cert to be vaid> -keystore
eamsroot/installconfig/keystore/sanovi.keystore
```

Note :

1) On executing the above command, user will be asked to enter password which will be considered as sanovi.keystore plain password.

2) Once the keystore is created, update the password in <TomcatHome>/conf/server.xml in below keystorePass parameters (there will be two keystorepass parameters and both has to be updated)

```
keystorePass="KEYSTORE PLAIN PASSWORD" compression="on"
compressionMinSize="2048" nocompressionUserAgents="gozilla,traviata"
```

3)Encrypt this password using eamsroot/tools/bin/Encryptor.sh and place the encrypted password in eamsroot/installconfig/resources/jetty.xml

```
<Set name="KeyStorePassword">ENCRYPTED KEYSTORE PASSWORD</Set>
```

```
<Set name="TrustStorePassword">ENCRYPTED TRUSTSTORE PASSWORD</Set>
```

4)Run securityuserinjection from RO and restart RO services.

7.10.4 Validating Key Store

You need to use the following snippet to validate the created key store files :

```
keytool -v -list -keystore panacesACP.keystore

keytool -v -list -keystore panacesACP.truststore

keytool -v -list -keystore sanovi.keystore
```

7.11 Port Forwarding

Kyndryl Resiliency Orchestration uses the following ports:

- **8443:** Port 8443 needs to be opened for secure GUI access
- **22**: Port 22 needs to be opened for communicating with Low touch agent
- **8081,8083:** Ports 8081 and 8083, need to be opened only during upgrading Local Agents from Resiliency Orchestration Agent Upgrade UI
- **42443 and 45443:** The ports 42443 and 45443, need to be opened for secured communication amongst Resiliency Orchestration Server, Site Controller, and Agents.

You can reduce the number of open ports by using the following Port forwarding procedures.

7.11.1 Prerequisites for Port Forwarding

The following are prerequisites for port forwarding:

- Httpd service. Apache service should be installed
- Server Certificate
- SSL Certificate Key File
- http modules: Mod_ssl, mod_proxy, mod_proxy_http

7.11.2 Configuring ActiveMQ Broker to support Port Forwarding

To configure the ActiveMQ Broker to support the Port Forwarding, complete the following tasks:

- Enabling HTTPS Transport Connector
- Importing HTTPD Certificate
- Configuring Site Controller for Port Forwarding
- **Till now we have generated & copied the certs for the RO server. The below steps now deal with active mq.**
  Handling certs for Active MqLets call this password as - truststore password. Make a note of this as well.
  After these steps, you should have -1. panacesAcp.KeyStore
  2. panacesACP.truststor
  3. KeyStore password
  4. truststore passwordNow, we need to copy create the encrypted passwords for active mq for keystore & truststoreAt <EMASROOT>/tools/apache-activemq-5.13.2/conf, you have - panacesACP.keystore, panacesACP.truststore & credentials-enc.properties
  4. Generate encrypted password for keystore
  <EMASROOT>/tools/apache-activemq-5.13.2/bin/activemq encrypt --password <Password> –input <keystorepassword>
  Make a note of this & call this **encryptedkeystorepassword**
  5. Generate an encrypted password for truststore
  <EMASROOT>/tools/apache-activemq-5.13.2/bin/activemq encrypt --password <Password> –input <truststorepassword>
  Make a note of this & call this **encryptedtruststorepassword**
  6. Open credentials-enc.properties (at<EMASROOT>/tools/apache-activemq-5.13.2/conf) & update the passwords like below
  keystore.password=<Password> (**encryptedkeystorepassword**)
  truststore.password=<Password> (**encryptedtruststorepassword**)7. Now from /tmp/certs copy the panacesACP.keystore & panacesACP.trustsore to <EMASROOT>/ tools/apache-activemq-5.13.2/conf
  8. Finally, restart panaces services - <EAMSROOT>/bin/panaces restart

7.11.2.1 Enabling HTTPS Transport Connector

1. Go to the <Resiliency Orchestration installation path>/tools/apache-activemq-5.13.2/conf/ folder and open the files activemq-security.xml and activemq.xml

80. Uncomment the line starting with the string <transportConnector name="https"

> **Note**
>
> For https port forwarding, the hostname of the server in which the Site Controller is installed should not have special characters.

7.11.2.2 Importing HTTPD Certificate

You need to perform the following steps for importing the httpd certificate:

1. Copy the SSL Server certificate, which is used in the httpd configuration section, to a folder.

81. Run the following command to import httpd certificate to /opt/panaces/installconfig/keystore/panacesACP.truststore:

```
keytool -import -alias "panacesacp_keystore" -file <httpd
certificate, which is copied in the folder> -keystore
$EAMSROOT\installconfig\keystore\panacesACP.trustStore
```

82. Enter the default password: uyts637KHDS337$%

> **Note**
>
> It is recommended that the users should create their truststore and keystore and use them as corresponding values for the truststore and keystore. The users should also create their passwords.

7.11.2.3 Configuring Site Controller for Port Forwarding

You need to perform the following steps for setting up the Site Controller to communicate with the Resiliency Orchestration on the HTTPS port:

Replacing the Port and Protocol attributes in the `Sitecontroller.cfg` file

- Go to `${EAMSROOT}/installconfig/`
- Open the `Sitecontroller.cfg` file
- Update the Port and Protocol attributes as shown in the following example:
- `MQ_RO_CONNECTION_PROTOCOL=https`
- `MQ_RO_CONNECTION_PORT=43443`
- Save the `Sitecontroller.cfg` file.

7.11.3 Configuration

This section describes port forwarding from secure https (443) to the following ports:

- Resiliency Orchestration Server secure tomcat secure port 8443
- Resiliency Orchestration Server nonsecure tomcat port 8080
- Resiliency Orchestration features using other ports 8082
- ActiveMQ Broker feature that uses port 43443
- ActiveMQ Admin Console that uses port 8162 (optional)

You must perform the following steps for enabling port forwarding:

kyndryl

7.11.4 HTTP configuration (/etc/httpd/conf/httpd.conf)

The user needs to perform the following http configuration at /etc/httpd/conf/httpd.conf:

1. Enable proxy_module, mod_ssl module, and proxy_http_module in httpd.conf of Apache web server.

```
LoadModule proxy_module modules/mod_proxy.so

LoadModule proxy_http_module modules/mod_proxy_http.so

LoadModule ssl_module modules/mod_ssl.so
```

83. Provide the ssl.conf file path.

```
Include conf.d/ssl.conf
```

84. Port 443 should be listening in ssl mode as specified below in httpd.conf file.

```
Listen 443 ssl

Listen 80
```

85. Provide the following proxy configuration and forward the configuration.

```
ProxyRequests Off

# Control Client Access

<Proxy https://<IP:8443/>Order Deny,Allow

Allow from all

</Proxy>

# Set TCP/IP network buffer size for better throughput (bytes)

ProxyReceiveBufferSize 4096

ServerName localhost

ProxyPass /PanacesGUI https://<IP>:8443/PanacesGUI

ProxyPassReverse /PanacesGUI https://<IP>:8443/PanacesGUI

ProxyPass /rmi http://<IP>:8081/rmi

ProxyPassReverse /rmi http://<IP>:8081/rmi

ProxyPass /rmi http://<IP>:80/rmi
```

```
ProxyPassReverse /rmi http://<IP>:80/rmi

ProxyPass /IBMRODashboard https://<IP>:8443/IBMRODashboard

ProxyPassReverse /IBMRODashboard https://<IP>:8443/IBMRODashboard

ProxyPass /cdrm-ws http://<IP>:8080/cdrm-ws

ProxyPassReverse /cdrm-ws http://<IP>:8080/cdrm-ws

ProxyPass /rest http://<IP>:8082/rest

ProxyPassReverse /rest http://<IP>:8082/rest

ProxyPass /admin  https://<IP>/admin

ProxyPassReverse /admin https://<IP>/admin

ProxyPass /MQB  https://<IP>:43443/MQB

ProxyPassReverse /MQB https://<IP>:43443/MQB

Timeout 2400

ProxyTimeout 2400

ProxyBadHeader Ignore

ServerRoot "/etc/httpd"
```

Note: The user needs to add the above configuration parameters as per their requirements.

For Example: If the requirement is Site Dashboard, the user needs to add KyndrylRODashboard proxy entries.

7.11.5 SSL configuration (/etc/httpd/conf.d/ssl.conf)

Provide the following configurations for SSL (specified in bold are configured, you need to specify the certificate and key path as per customer environment):

Comment 443 port https port:

```
#Listen 443 https
```

7.11.6 Server Certificate

Point SSLCertificateFile at a PEM encoded certificate. If the certificate is encrypted, the server prompts for a pass phrase.

kyndryl

> **Note**
>
> A kill-HUP will prompt again. A new certificate can be generated using the genkey(1) command.

Provide the following details to configure the SSL Server certificate.

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
```

Provide SSL Server certificate file path.

For Example, You need to provide the following details to configure the SSL Server certificate in Resiliency Orchestration Server.

```
SSLCertificateFile <certificate file path>/conf/ibm.crt
```

Server Private Key: If the key is not combined with the certificate, you need to specify the key file.

> **Note**
>
> If you have an RSA and a DSA private key, you can configure both in parallel (to also allow the use of DSA ciphers, etc.).

Provide the SSL Server private key file path.

For Example: You need to provide the following details to configure SSL Server private key in Resiliency Orchestration Server.

```
SSLCertificateKeyFile <certificate file path>/conf/ibm.key
```

Enable/Disable SSL for this virtual host: Provide the following details to enable/disable SSL for the virtual host.

```
SSLEngine on

SSLProxyEngine on

SSLProxyVerify none

SSLProxyCheckPeerCN off

SSLProxyCheckPeerName off

SSLProxyCheckPeerExpire off
```

SSL Protocol support: Provide the following details for SSL protocol support:

- List the enable protocol levels with which clients will be able to connect.
- Disable SSLv2 access by default.

- Uncomment the following command to Disable all, enable required

```
#SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
```

- Enable all, disable required as shown in the following command.

```
SSLProtocol all -SSLv2 -SSLv3
```

Inter-Process Session Cache: Configure the SSL Session Cache and timeout as below.

```
# SSLSessionCache          shmcb:/run/httpd/sslcache(512000)

SSLSessionCache          dbm:/run/httpd/sslcache

SSLSessionCacheTimeout   300
```

7.12 Steps to Enable Compression in Tomcat Server

The below tag in the server.xml enables compression.

> **Note**
>
> Compression will be enabled if the file size is more than 2KB.

```
Connector port="8080" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" acceptCount="100"
compressionMinSize="2048"
compression="on"
compressableMimeType="text/html,text/xml,text/plain,text/css,
text/javascript,text/json,application/x-javascript,
application/javascript,application/json"
connectionTimeout="60000" disableUploadTimeout="true"
URIEncoding="utf-8" />
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
compressionMinSize="2048"
compression="on"
compressableMimeType="text/html,text/xml,text/plain,text/css,
text/javascript,text/json,application/x-javascript,
application/javascript,application/json"
```

```
clientAuth="false" sslEnabledProtocols="TLSv1.2"
keystoreFile="{EAMSROOT}/installconfig/keystore/sanovi.keystore"
keystorePass="<Password[1]>"/>
```

[1]Connect with the Support/Delivery team to get the default passwords.

> **Note**
>
> To change security constraints in web.xml, users have to wait till the war is extracted in the first start.

7.13 Configuring Current Events

User can view more/less events by changing the value of "*sanovi.events.displayDuration.hours*" in $EAMSROOT/installconfig/panaces.properties file. If this parameter is not specified or an invalid integer is specified, then it will default to 120hrs. Specifying zero might result in no events or very few events occurrences within the past few seconds to be shown. It should be noted that changing this parameter will also affect the number of events shown on the "Monitor-> Continuity" listing page. The user is expected to use "Event Reports" if he wants to see the history of events for a longer duration (say months) as supposed to increasing this parameter. Changing this value does not require a server restart as the value will take effect during the next page refresh.

The aging period can be configured by editing/adding "*sanovi.closeEventsInDays*" property in $EAMSROOT/installconfig/panaces.properties file. The value for this property should be a numeric value representing the number of days. If this property is not specified or an invalid value is provided, the System defaults it to 5 days. Specifying zero will disable the automatic Closure of events. Altering this property does not require a restart of the Resiliency Orchestration Server.

7.13.1 Logs Retention

Server logs and Site Controller logs are written in $EAMSROOT/var/log and the remote agent logs in Site Controller are written at $EAMSROOT/remote/var/log

The logs retention is by default set to 7 days; however, this is configurable.

To configure the log retention for Resiliency Orchestration Server and Site Controller, update the purge.server.logfiles parameter in $EAMSROOT/installconfig/panaces.properties

kyndryl

To configure the log retention for the remote agents in the Site Controller, update the purge.server.logfiles parameter in $EAMSROOT/remote/installconfig/panaces.properties.

Note: From RO 8.4.9.0, Purge feature has been enhanced to enable you to clean up the high volume of the purged data automatically.

To do this, the following property has been added:

`panaces.db.NrOfRecordsForBatchDeletion` and the default value is 10000.

7.13.2 Fetch Logs /System Capture

When the panaces is running with non-root the system logs are not fetched until read permission is granted for the non-root user. The non-root user, by default, does not have read permission for the system logs (/var/log/messages and so on).

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

7.13.3 Capturing syslog events

One of the most widely used logging systems on Linux systems is **rsyslog.**

Rsyslog is a powerful and secure log processing tool that accepts data from different types of sources such as systems or applications and outputs it in multiple formats. It works in a client/server model; therefore, it can be configured as a client and/or as a central logging server for other servers, network devices, and remote applications.

Follow the steps mentioned in this section to capture syslog events from the Kyndryl Resiliency Orchestration server software.

7.13.3.1 Prerequisites

For the rsyslog setup, we need two machines; one will be set up as a client (this is the machine where the Kyndryl Resiliency Orchestration server software is running) and another one will be configured as a server.

Alternatively, you can configure and capture syslogs on a local machine also, without the syslog server configuration. For steps, refer to section Capture syslogs on the client (without server configuration)

Note – All configurations mentioned below for capturing syslog events have been tested on RHEL 8.0. On systems with lower RHEL versions, these configurations may require some changes.

7.13.3.2 Installation of the package

The rsyslog package needs to be installed in the client and the server machines.

1. Log in as root into the client/server machine.
2. Install rsyslog using the Linux package manager tool. Run the below command to install the rsyslog.

   ```
   sudo yum update && yum install rsyslog
   ```

   If the package is already installed then it will be updated, else it will be installed. After successful installation, a configuration file rsyslog.conf is created under /etc/ folder.

7.13.3.3 Configure Rsyslog as a server

To configure rsyslog as a network/central logging server to collect all log/remote logs, make the following changes in the /etc/rsyslog.conf file in the server machine –

1. Set the protocol (either to UDP or TCP or both) which rsyslog will use for remote syslog reception.

   If you want to use a UDP connection, which is faster but unreliable, search and uncomment the lines below for UDP

   ```
   module(load="imudp") # needs to be done just once
   input(type="imudp" port="514")
   ```

To use a TCP connection, which is slower but more reliable, search and uncomment the lines below for TCP.

```
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

2. Set the port number where the rsyslog will listen on.
3. To search/compare any particular string in the logs, you need to use the filter in the rules section. Below is a sample rule -

   ```
   : msg, contains, "Event=Anomaly" /var/log/sample.log
   ```

where -

"msg" is the log

"contains" is the keyword/condition

"Event-Anomaly" is the sample string to search

/var/log/sample.log is the file where the filtered logs are stored.

If you do not provide any path, the default filtered log file location is /var/log/messages file.
Once a log matches the condition, the filtered log file is either created or updated in the mentioned/default location.

4. Save the rsyslog.conf file and restart the rsyslog services by running the below commands -

```
systemctl stop rsyslog
systemctl start rsyslog
```

Alternately, you can use the restart command instead of stopping and starting rsyslog by using the command –

```
systemctl restart rsyslog
```

Check the status of the rsyslog service using the command -

```
systemctl status rsyslog
```

7.13.3.4 Configure Rsyslog as a client

To configure rsyslog as a client to send all log/remote logs, make the following changes in the /etc/rsyslog.conf file in the client machine –

1. To force the rsyslog daemon to act as a logging client and forward all locally generated log messages to the remote rsyslog server, add this forwarding rule, at the end of the file as shown below

   ```
   *.* @@<Server_IP>:514
   ```

   where Server_IP is the IP address of the rsyslog server machine

2. To send apache level logs to the server, you need to define the below-mentioned rules in the rsyslog.conf file.

   ```
   module(load="imfile" PollingInterval="10")

   # Apache error file:
   ```

```
input(type="imfile"
      File="/opt/panaces/var/log/PanacesServer.log"
      Tag="server"
      Severity="info")
```

This will load the PanacesServer.log file and check all logs w.r.t to the server, as the Tag is set to "server", and Severity is set to "info". Provide the location of the log file (server-side file location) in the File parameter.

3. Save the rsyslog.conf file and restart the rsyslog services.

7.13.3.5 Capture syslogs on the client (without server configuration)

The procedure of installation of rsyslog on the client machine remains the same as mentioned in section Installation of the package.

Note – To capture syslog events on the client itself, do not configure any IP as <Server_IP> in the /etc/rsyslog.conf file. So the local host itself will store the logs captured.

To search/compare any particular string in the logs, use a filter in the rules section in the /etc/rsyslog.conf file in the client machine.

Below is a sample rule -

```
: msg, contains, "Event=Anomaly" /var/log/sample.log
```

where "msg" is the log, "contains" is the keyword/condition, "Event-Anomaly" is the sample string to search, and /var/log/sample.log is the file where the filtered logs are stored.

If you do not provide any path, the default filtered log file location is /var/log/messages file.
Once a log matches the condition, the filtered log file is either created or updated in the mentioned/default location in the client machine itself.

Save the rsyslog.conf file and restart the rsyslog services.

7.14 Integrate RO audit-log with Syslog

By setting the below values in panaces.properties, RO will forward all the Audit logs that it captures (refer to Audit Logging topic in Admin Guide for the exact logs) to the configured Syslog.

This would be useful for any applications that are interested in monitoring RO-specific user activity through the Syslog.

7.14.1 Settings to be done on RO server:

To enable the configuration we need to set the following 2 parameters in the panaces.properties file

```
SYSLOG_SERVER=<SYSLOG-SERVER-IP>
SYSLOG_SERVER_PORT=<SYSLOG-SERVER-PORT >
```

7.14.2 Configuration to receive the AuditInfo and EventLogs on Syslog Server:

To enable the configuration, we need to set the following two parameters in the syslog.properties file.

```
SYSLOG.EVENT.ENABLE=<TRUE>

SYSLOG.AUDITINFO.ENABLE=<TRUE>
```

To disable the configuration, we need to set the following two parameters in syslog.properties file.

```
SYSLOG.EVENT.ENABLE=<FALSE>

SYSLOG.AUDITINFO.ENABLE=<FALSE>
```

Use the below Filter property files once the Syslog properties are enabled.

To receive all the Severity level logs, we need to set the following parameter as EMPTY in syslog.properties file.

```
SYSLOG.EVENT.SEVERITY=
```

To receive all the Object Class logs, we need to set the following parameter as EMPTY in syslog.properties file.

```
SYSLOG.EVENT.OBJCLASS=
```

To receive all the Feature Configuration logs, we need to set the following parameter as EMPTY in syslog.properties file.

```
SYSLOG.EVENT.FEATURE=
```

To enable the specific configuration, we need to set the following parameters in syslog.properties file.

For Example:

```
SYSLOG.EVENT.SEVERITY=CRITICAL,SERIOUS,WARNING

SYSLOG.EVENT.OBJCLASS=COMPONENT,BCS

SYSLOG.EVENT.FEATURE=COMMON,MONITOR,MANAGE,USER_INPUT
```

In this example the user will receive the logs having severity of these values "CRITICAL, SERIOUS, WARNING", objclass of values "COMPONENT, BCS" and feature of values "COMMON, MONITOR, MANAGE, USER_INPUT".

Use the below Filter property files if the user requires to receive ALL the logs:

```
SYSLOG.EVENT.SEVERITY=

SYSLOG.EVENT.OBJCLASS=

SYSLOG.EVENT.FEATURE=
```

7.15 Troubleshooting Proxy Errors

Issue: Once the port forwarding configuration is done, and while accessing the application with https://<IP>/PanacesGUI (accessing with default secure port) you may get the following error:

The proxy server could not handle the request GET /PanacesGUI/

Reason: "Error during SSL Handshake with remote server"

Resolution: The SSL handshake issue will come if remote server certificate name validation fails or the keystore certificate expires. Therefore, update the ssl. conf file with parameters `"SSLProxyCheckPeerName off"` and `"SSLProxyCheckPeerCN off"`

Assuming the keystore for the tomcat has not expired, if it has expired, set `"SSLProxyCheckPeerExpire off"` as a workaround; however, it is recommended to renew the tomcat keystore certificate.

Once set, restart the httpd service using the command: `sudo systemctl restart httpd`

7.15.1 Preset Users for Resiliency File Replicator

During the installation of the Resiliency Orchestration application software, the following Resiliency File Replicator user is created with all privileges:

- `pfradmin`

The Resiliency Orchestration application software is configured to use the `pfradmin` User for accessing the Resiliency File Replicator until you change the user in the Resiliency File Replicator.

7.16 Configuring the Resiliency Orchestration application to use the Resiliency File Replicator

The Resiliency Orchestration application software is installed with preset User credentials for accessing the Resiliency File Replicator. You can configure Kyndryl Resiliency Orchestration application software to use different Resiliency File Replicator user credentials.

You must first set up a new user credential after installing the Resiliency File Replicator. Ensure that the new user you create in the Resiliency File Replicator is set up with all privileges.

To configure the Resiliency Orchestration application software for the new Resiliency File Replicator user, complete the following steps:

1. Navigate to the directory where the Resiliency Orchestration application software is installed, by entering the following command at the command prompt:

```
# cd installconfig
```

86. In this directory, enter the following command at the command prompt to display the properties file for the Resiliency Orchestration application:

```
# vi panaces.properties file
```

87. In the **`panaces.properties`** file, change the preset value for the parameter panaces.mysql.username to the new username that you created in the Resiliency File Replicator. The preset parameter for the Resiliency File Replicator user is set as `pfradmin`.

```
panaces.mysql.username = <new pfr user>
```

88. Save and close the **`panaces.properties`** file.

> **Note –** Kyndryl Resiliency File Replicator is a secure application. By default, File Replicator Service and File Replicator Agent communication are secure with TLS using TLSv1.2 protocol with a strong cipher. For details, refer to the section Configuring Resiliency File Replicator for Security in the Kyndryl Resiliency File Replicator Installation guide.

7.17 Localizing the Kyndryl Resiliency Orchestration Application for languages other than English

You can configure the Kyndryl Resiliency Orchestration components such as the OS, Console, and MariaDB for displaying and storing text in languages other than English.

For example, if you are using the Kyndryl Resiliency Orchestration application installed with Japanese as the language of operation, and you want the interface to display text you enter in Japanese, store data into the MariaDB in Japanese, search for and display records from the MariaDB in Japanese, then you must configure the Kyndryl Resiliency Orchestration application as instructed in the following sections.

- Configuring the OS and VNC console
- Configuring the MariaDB
- Configuring the Resiliency Orchestration Server properties

7.17.1 Prerequisites

You must stop all processes in the Kyndryl Resiliency Orchestration application before you continue with the following procedure.

7.17.2 Configuring the OS and VNC console

> **Note:**
>
> You must have SuperAdmin privileges to do this task.

To configure the OS and VNC Console, perform the following steps:

1. Locate and open the `.bash_profile` file from the path: `/root`

89. Add the following text:

```
export LANG=ja_JP.UTF-8
```

90. Save the `.bash_profile` file

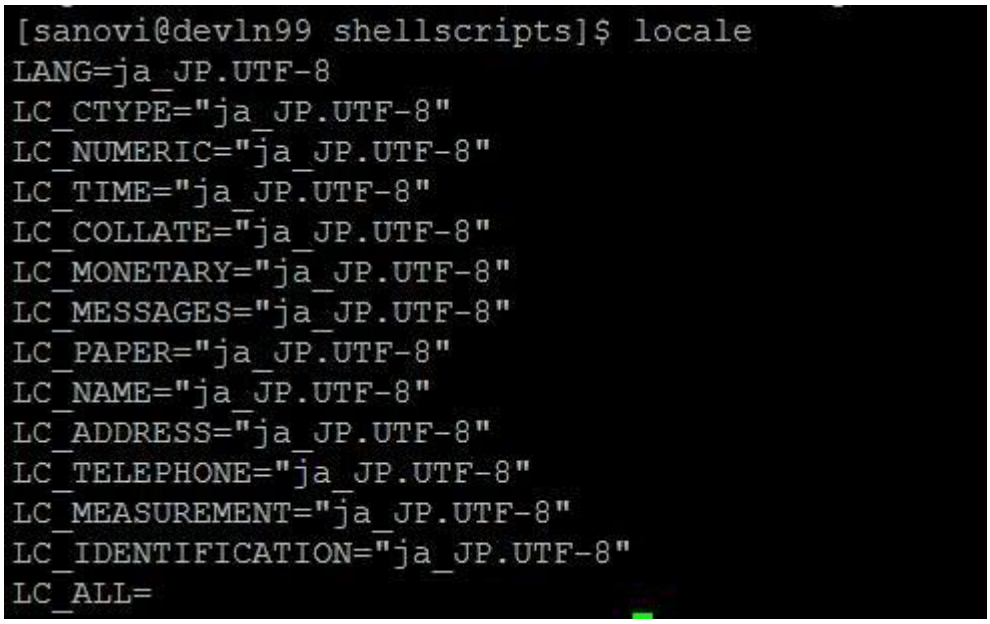
91. Enter the following command:

```
~/.bash_profile
```

92. To verify if the changes are implemented in the Kyndryl Resiliency Orchestration application, enter the following command:

```
$ locale
```

93. The options for the language set (ja_JP.UTF-8) are displayed for the various parameters, as shown in the sample screenshot.



94. Proceed to configure the MariaDB.

7.17.3 Configuring the MariaDB

> **Note:**
>
> You must have SuperAdmin privileges to do this task.

To configure the MariaDB, complete the following steps:

1. Locate and open `my.cnf` file from the path: `/etc/my.cnf`
2. Add **utf8** as the default character set under the following sections in the `my.cnf` file:

```
[client]
default-character-set=utf8

[mysql]
default-character-set=utf8

[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
```

```
user=mysql


character-set-server=utf8
```

95. Save and close `my.cnf` file.
96. Proceed to configure the Resiliency Orchestration Server properties.

7.17.4 Configuring the Resiliency Orchestration Server properties

> **Note:**
>
> You must have SuperAdmin privileges to do this task.

To configure the Resiliency Orchestration Server properties (server.xml file), complete the following steps:

1. After logging in to the Kyndryl Resiliency Orchestration Server using Putty, locate the `server.xml` file in the path: `$TOMCAT_HOME/conf`

97. Open the server.xml file by entering the following command:

```
sudo vi $TOMCAT_HOME/conf/server.xml
```

98. Add the following configuration for the Connector Port (8443)
99. Add URIEncoding="utf-8" after the last entry under the <Connector port="8443" >

    The following is an example with the URI encoding added:

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
compressionMinSize="2048" compression="on"
compressableMimeType="text/html,text/xml,text/plain,text/css,
text/javascript,text/json,application/x-javascript,
application/javascript,application/json"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
keystoreFile="/opt/panaces/installconfig/keystore/sanovi.keystore"
keystorePass="<Password[1]>" URIEncoding="utf-8" xpoweredby="false"
server="Web"/>
```

    [1]Connect with the Support/Delivery team to get the default passwords.

100. You need to save the following cipher value in the `server.xml` file:

```
ciphers="TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES
_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_R
SA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TL
```

```
S_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_
SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256"
```

101. Disable tomcat automatic deployment and add the below line in $TOMCAT_HOME/conf/server.xml. add autoDeploy="false" in server.xml

```
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
```

102. Save and close the `server.xml` file.

7.17.5 Post configuration steps

1. Restart the MySQL service by entering the following command:

```
$ service mysql restart
```

103. Restart the Kyndryl Resiliency Orchestration services by entering the following command:

```
sudo $EAMSROOT/bin/panaces restart
```

7.18 Configuring Kyndryl Resiliency Orchestration Server and Site Controller for Secured Communication by Using the ActiveMQ Broker

After the installation of the Kyndryl Resiliency Orchestration Server and the Site Controller, you must complete the procedures described in this section to enable secure communication between the Resiliency Orchestration and the Site Controller by using the ActiveMQ Broker feature. This feature is enabled in the Kyndryl Resiliency Orchestration application from version 7.2.3.1.

The Resiliency Orchestration provides you with Default Passwords for the following Roles:

- Admin – Is a user with the privileges of an Admin and can view the status of messages and change the message priorities on the ActiveMQ Broker.
- Producer – Is the server with the authority to post messages on the ActiveMQ Broker.
- Consumer - Is the server with the authority to listen to the messages posted on the ActiveMQ Broker.

Important:

Ensure to change the default passwords in the Kyndryl Resiliency Orchestration application after downloading the Service Pack (7.2.3.1) from the Kyndryl Passport Advantage Portal.

Changing the passwords or customizing the passwords will ensure that the secure communication between the Kyndryl Resiliency Orchestration application and the Site Controller in your infrastructure will be contained within your organization and prevent queries from unauthorized Users.

Perform the following procedures in sequence to ensure that you have set up the ActiveMQ Broker for the secured communication between the Kyndryl Resiliency Orchestration application and the Site Controller.

7.18.1 Changing the Default Passwords for the Roles: Admin, Producer, and Consumer

Important:

The Default Passwords for the Roles (Producer and Consumer) must be changed for both the Kyndryl Resiliency Orchestration Server and the Site Controller Server and on the ActiveMQ Broker (on both the Kyndryl Resiliency Orchestration Server and the Site Controller Server). This is to ensure that both (Resiliency Orchestration and Site Controller) can function as the Producer and Consumer and the ActiveMQ Broker recognizes the Producer and Consumer Roles.

In the normal set of communication between the Kyndryl Resiliency Orchestration Server and the Site Controller Server, the following are the roles that are performed:

Kyndryl Resiliency Orchestration will function as the Producer when the messages are generated by the Resiliency Orchestration and the Site Controller will function as the Consumer for the same messages, by receiving them.

The site Controller will function as the Producer when the messages are generated by the Site Controller and the Kyndryl Resiliency Orchestration will function as the Consumer for the same messages, by receiving them.

The ActiveMQ Broker functions as the mediator (on both the Resiliency Orchestration and Site Controller) for receiving and posting messages, recognizing the Producer and Consumer, and allowing the messages to flow to the authentic sender or receiver.

The “activemq” script is used for encrypting passwords for ActiveMQ communication. The “Encryptor.sh” script is used for encrypting passwords for the Kyndryl Resiliency Orchestration server and Site Controller communication. The new passwords passed to both activemq and Encryptor.sh scripts should be the same.

1. Generating encrypted custom passwords. Encrypted Custom Passwords must be generated for the Admin, Producer, and Consumer Roles.

104. Replacing the encrypted custom passwords in the related properties files.

See the following sections for the procedures:

- Changing the Default Admin Password
- Changing the Default Passwords for the ActiveMQ Broker
- Changing the Default Passwords in the Resiliency Orchestration and Site Controller Configurations

7.18.1.1 Changing the Default Admin Password

Complete the following steps to change the default passwords that the Kyndryl Resiliency Orchestration application provides.

1. Changing the Default Admin Password

i. The default Admin Password is <`Password`[1]> and is located in the `jetty-realm.properties` file.

[1]Connect with the Support/Delivery team to get the default passwords.

ii. Choose a custom password.

> **Note:**
>
> *Ensure to choose a password that has a minimum of 20 alpha-numeric characters. Supported characters are Capital Alphabets (A-Z), Lower Alphabets (a-z), and Numbers (0-9). Special characters are not supported.*

iii. Proceed to encrypt the custom password. Go to the next step.

105. Encrypting the new Admin Password

i. The custom or new password must be encrypted. To encrypt the new password, go to the following location:

$EAMSROOT/lib

ii. Run the following command:

```
java -cp jetty-util-9.3.9.v20160517.jar
org.eclipse.jetty.util.security.Password admin <New Password>
```

iii. The new encrypted password is displayed as shown in the following example:

```
CRYPT:PASSWORD
```

iv. Proceed to replace the encrypted custom password in the properties file.

106. Replacing the Encrypted Password in the `jetty-realm.properties` file

i. Go to: `/opt/panaces/tools/apache-activemq-5.13.2/conf/`

ii. Open the jetty-realm.properties file

iii. Under the section:

username: password [,rolename ...]

iv. Update the new encrypted password as shown in the following example:

`admin: CRYPT:PASSWORD, admin`

v. Remove the Line that has the following value:

`user: user, user`

vi. Go to the Next Step.

107. Proceed to change the default passwords for the Resiliency Orchestration Server ActiveMQ Broker. For instructions, see Changing the Default Passwords for the ActiveMQ Broker.

7.18.1.2 Changing the Default Passwords for the ActiveMQ Broker

Complete the following steps to change the default Producer and Consumer passwords that are provided for the ActiveMQ Broker in the Resiliency Orchestration and the Site Controller Servers.

1. Changing the Default Producer and Consumer Passwords

i. The default Producer and Consumer Passwords are located in the `credentials-enc.properties` file in the Resiliency Orchestration and the Site Controller Servers.

ii. Choose a custom password. Ensure that you create custom passwords for the following types:

- producer_ro custom password
- consumer_ro_custom password
- producer_sc_custom password
- consumer_sc_custom password

Note:

*It is recommended to choose a strong password that has a mix of alpha-numeric characters and special characters, with a minimum length of 25. Special characters other than space character is allowed. Special characters supported are - ‘ ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] / < > , . ; ? ' : |*

kyndryl

You must escape the following special characters while entering a password in the command line - ' ~! $ & / < >,. ; ? ': |

*Example – P3t3r\:Pant323\~lkj0@19^jf83 - In this example, and ~ are escaped using *

108. Encrypting the New Passwords

The new passwords for both the Producer and Consumer roles for the Resiliency Orchestration and the Site Controller must be encrypted.

Encrypting passwords for the Resiliency Orchestration and Site Controller ActiveMQ

- To encrypt the new passwords, go to the following location in the Resiliency Orchestration Server:

  ${EAMSROOT}/tools/apache-activemq-5.13.2/bin

- To encrypt the new Producer password for the Resiliency Orchestration, run the following command:

  ```
  ./activemq encrypt --password <Password> --input
  <producer_ro_password>
  ```

  The new encrypted password is displayed and denoted as Encrypted Text: <producer_ro_encrypted_password>

- To encrypt the new Consumer password, run the following command:

  ```
  ./activemq encrypt --password <Password> --input
  <consumer_ro_password>
  ```

  The new encrypted password is displayed and denoted as Encrypted Text: <consumer_ro_encrypted_password>

- To encrypt the new Producer password for the Site Controller, run the following command:

  ```
  ./activemq encrypt --password <Password> --input
  <producer_sc_password>
  ```

  The new encrypted password is displayed and denoted as Encrypted Text: <producer_sc_encrypted_password>

- To encrypt the new Consumer password for the Site Controller, run the following command:

  ```
  ./activemq encrypt --password <Password> --input
  <consumer_sc_password>
  ```

The new encrypted password is displayed and denoted as

Encrypted Text:<consumer_sc_encrypted_password>

- Ensure that you have encrypted the custom passwords and have noted them as shown in the following example:
  - *producer_ro_password* - encrypted as - <producer_ro_encrypted_password>
  - *consumer_ro_password* - encrypted as - <consumer_ro_encrypted_password>
  - *producer_sc_password* - encrypted as - <producer_sc_encrypted_password>
  - *consumer_sc_password* - encrypted as - <consumer_sc_encrypted_password>

7.18.2 Replacing the Encrypted Passwords in the credentials-enc.properties File

7.18.2.1 Replacing Encrypted passwords for the Resiliency Orchestration ActiveMQ

i. Go to the following location in the Resiliency Orchestration Server: `${EAMSROOT}/tools/apache-activemq-5.13.2/conf/`

ii. Open the `credentials-enc.properties` file

iii. Update the encrypted passwords as shown in the following example:

`producer.password=`<Password> (producer_ro_encrypted_password)

`consumer.password=`<Password> (consumer_ro_encrypted_password)

7.18.2.2 Replacing Encrypted passwords for the Site Controller ActiveMQ

i. Go to the following location in the Site Controller Server: `${EAMSROOT}/tools/apache-activemq-5.13.2/conf/`

ii. Open the `credentials-enc.`properties file

iii. Update the encrypted passwords as shown in the following example:

`producer.password=`<Password> (producer_sc_encrypted_password)

`consumer.password=`<Password> (consumer_sc_encrypted_password)

iv. Additionally, for Windows Site Controller, replace the default activemq producer and consumer passwords with new strong encrypted passwords in both the apache-activemq conf directories (unlike in Linux Site controller) in below mentioned Windows Site controller installation directory locations:

kyndryl

```
$EAMSROOT\tools\apache-activemq-5.13.2\conf\credentials-enc.properties
```

```
$EAMSROOT\tools\windows\apache-activemq-5.13.2\conf\credentials-enc.properties
```

Example:

```
C:\SiteController\tools\apache-activemq-5.13.2\conf\credentials-enc.properties

C:\SiteController\tools\windows\apache-activemq-5.13.2\conf\credentials-enc.properties
```

v. After updating the "credentials-enc.properties" files in both the above-mentioned paths, reboot the Windows Site controller machine.

vi. Once the Site Controller machine is up, start the Windows OS Agent service, ActiveMQ, and Site Controller services from services.msc

vii. Proceed with changing the default passwords in the Resiliency Orchestration and Site Controller Configurations. For instructions, see *Changing the Default Passwords in the Resiliency Orchestration and Site Controller Configurations*.

7.18.2.3 Changing the Default Passwords in the Resiliency Orchestration and Site Controller Configurations

Complete the following steps to change the default Producer and Consumer passwords that are provided for the Resiliency Orchestration and Site Controller in their corresponding configuration files.

7.18.2.4 Changing the Default and updating Configurations for the Resiliency Orchestration

1. The default Producer and Consumer Passwords are located in the `panaces.properties` file.

- Use the same new passwords that you used to encrypt for the Resiliency Orchestration and Site Controller in Changing the Default Passwords for the ActiveMQ Broker, as shown in the following example:
- *producer_sc_password*
- *consumer_ro_password*

109. Encrypting the New Passwords

- The new passwords for both the Producer and Consumer roles must be encrypted. To encrypt the new passwords, go to the following location in the Resiliency Orchestration Server:

```
${EAMSROOT}/tools/bin/
```

- To encrypt the new Producer password, run the following command:

  `./Encryptor.sh < producer_sc_password >`

  The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password** and denoted as <producer_sc_enc_password>

- To encrypt the new Consumer password, run the following command:

  `./Encryptor.sh < consumer_ro_password >`

  The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password** and denoted as <consumer_ro_enc_password>

110. Replacing the Encrypted Passwords in the `panaces.properties` file

- Go to `${EAMSROOT}/installconfig/`
- Open the `panaces.properties` file
- Update the encrypted passwords as shown in the following example:
  - `MQ_SC_BROKER_PRODUCER_USERNAME=producer`
  - `MQ_SC_BROKER_PRODUCER_PASSWORD=`<producer_sc_enc_password>
  - `MQ_RO_BROKER_CONSUMER_USERNAME=consumer`
  - `MQ_RO_BROKER_CONSUMER_PASSWORD=`<consumer_ro_enc_password>

7.18.2.5 Changing the Default and updating Configurations for the Site Controller

1. The default Producer and Consumer Passwords are located in the `${EAMSROOT}/installconfig/` directory in `Sitecontroller.cfg` and `panaces.properties` files.

- Use the same new passwords that you used to encrypt for the Resiliency Orchestration and Site Controller in Changing the Default Passwords for the ActiveMQ Broker, as shown in the following example:

  In SiteController.cfg file –

  `producer_ro_password`

  `consumer_sc_password`

  In panaces. properties file –

  `producer_sc_password`

  `consumer_ro_password`

111. Encrypting the New Passwords

- The new passwords for both the Producer and Consumer roles must be encrypted. To encrypt the new passwords, go to the following location in the Site Controller Server:

  `${EAMSROOT}/tools/bin/`

- To encrypt the new passwords, run the following command:

  `./Encryptor.sh <producer_ro_password>`

  The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password** and denoted as <producer_ro_enc_password>

- To encrypt the new Consumer password, run the following command:

  `./Encryptor.sh <consumer_sc_password>`

  The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password** and denoted as <consumer_sc_enc_password>

- To encrypt the new Producer password, run the following command:

  `./Encryptor.sh <producer_sc_password>`

  The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password** and denoted as <producer_sc_enc_password>

- To encrypt the new Consumer password, run the following command:

  `./Encryptor.sh <consumer_ro_password>`

- The result, which is the encrypted password is stored in file $EAMSROOT/var/log/Encryptor.log as a property **Encrypted password** and denoted as <consumer_ro_enc_password>

112. Replacing the Encrypted Passwords in the `Sitecontroller.cfg` file

   i. Go to `${EAMSROOT}/installconfig/`

   ii. Open the `Sitecontroller.cfg` file

   iii. Update the encrypted passwords as shown in the following example:

   ```
   MQ_RO_BROKER_PRODUCER_USERNAME=producer
   MQ_RO_BROKER_PRODUCER_PASSWORD=<producer_ro_enc_password>
   MQ_SC_BROKER_CONSUMER_USERNAME=consumer
   MQ_SC_BROKER_CONSUMER_PASSWORD=<consumer_sc_enc_password>
   ```

   iv. Open the `panaces.properties` file

   v. Update the encrypted passwords as shown in the following example:

kyndryl

```
MQ_SC_BROKER_PRODUCER_USERNAME=producer
MQ_SC_BROKER_PRODUCER_PASSWORD=<producer_sc_enc_password>
MQ_RO_BROKER_CONSUMER_USERNAME=consumer
MQ_RO_BROKER_CONSUMER_PASSWORD=<consumer_ro_enc_password>
```

Note – After updating all the encrypted passwords, delete the log file $EAMSROOT/var/log/Encryptor.log for security reasons.

7.18.3 Accessing ActiveMQ Console

You can access the ActiveMQ Console to view the messages that are queued in the ActiveMQ Brokers on either the Resiliency Orchestration or the Site Controller servers. As an Admin User, you can also set or change the priorities of the messages on the ActiveMQ Broker.

To access the ActiveMQ Console, use the following IP:

https://<HOSTIP>:8162/

Where:

- Host IP is the IP of the Resiliency Orchestration Server or the Site Controller Server depending on which ActiveMQ Broker you want to access
- 8162 is the port that is used to view the messages on the ActiveMQ Broker.

7.18.4 Encrypting the custom store passwords for ActiveMQ

Kyndryl Resiliency Orchestration provides you with default passwords for the keystore and truststore. When a custom keystore/truststore password is generated, it is recommended to encrypt the passwords for enhanced security.

In the case of activemq, scripts to encrypt the custom store passwords are provided as a utility by activemq.

Encrypting passwords for the Kyndryl Resiliency Orchestration server and SiteController ActiveMQ

1. To encrypt the new passwords, go to the following location in the Resiliency Orchestration Server:

   $EAMSROOT/tools/apache-activemq-5.13.2/bin

2. To encrypt the custom store password for Resiliency Orchestration, run the following command:

   ./activemq encrypt --password <Password>--input <storepassword>

Where --password is the secretkey and can be seen in the file $EAMSROOT/tools/apache-activemq-5.13.2/bin/env as a property ACTIVEMQ_ENCRYPTION_PASSWORD=<Password[1]>

[1]Connect with the Support/Delivery team to get the default passwords.

- The new encrypted password is displayed as shown in the following example:

  (store encrypted password)

3. Repeat step 2 for each password to be encrypted on the Resiliency Orchestration server and SiteController.

Note – The script is in the same location on both the Resiliency Orchestration server and SiteController

113. The encrypted custom password should be placed in credentials-enc. properties, which are located in $EAMSROOT/tools/apache-activemq-5.13.2/conf directory in both Kyndryl Resiliency Orchestration server and SiteController.

7.19 Viewing the HTML Dashboard

You can access or switch between the Flex Dashboard and HTML Dashboard (enabled by default) by using the following URLs for the **Manager Dashboard** and the **Operational Dashboard**:

a. Manager Dashboard:

- https://<Resiliency Orchestration IP>:8443/PanacesGUI/flex/SanoviDashboard.jsp [Flex]
- http://< Resiliency Orchestration IP >:8080/PanacesGUI/flex/SanoviDashboardPlain.jsp [HTML]

b. Operational Dashboard:

- http{://< Resiliency Orchestration IP >:8443/PanacesGUI/flex/OperationalDashboard.jsp [Flex]
- http://< Resiliency Orchestration IP >:8080/PanacesGUI/flex/OperationalDashboardPlain.jsp [HTML]

> **Note**
>
> The panaces.properties file is by default configured to HTML [panaces.dashboard=HTML]

7.20 Removing Temp Folders Created in CR Platform

The scanning workflow creates temporary folders in the Site Controller and Staging servers. These folders are configured in the property file. Multiple executions make

the temp folder grow in size and it needs to be removed. The following are steps for removing the temp folders in the Site Controller and Staging servers:

1. Users can utilize the delete commands specific to Linux or Windows to remove the temp folder that is created.
2. The user needs to have appropriate permissions on Linux and Windows to execute these commands.
3. This has to be done on both the Site Controller and the Staging machines.
4. This is an operational activity that the users should execute after making sure that there are no pending alerts that are waiting for user action.
5. For Staging Server, the procedure is the same, however, the user should manually copy the relevant scripts from the Site Controller bin location to Staging Server, as shown in the following procedures:
    - Copy the shell script LinuxScanWorkflowTempCleanup.sh for a Linux staging box.
    - Copy the batch script WindowsScanWorkflowTempCleanup.bat for a Windows staging box.

7.21 Monitoring Health of RO Server

The health monitoring scripts located within $EAMSROOT/tools/monitoring/ will perform automatic log generation which can be found in $EAMSROOT/var/log.Log File Names:

$EAMSROOT/var/log/ThreadDumpROServer-20210827_171202.log.gz - this will take a thread dump of the EamsServer, ideal to detect slowness and deadlocks

$EAMSROOT/var/log/GCClassStatsROServer-20210827_171202.log.gz - this will report the metaspace usage

$EAMSROOT/var/log/GCHistogramROServer-20210827_171202.log.gz - this will report the heap usage

$EAMSROOT/var/log/MariadbConnStats-20210827_171202.log.gz - this will report how the database connections are getting used

$EAMSROOT/var/log/deleted_monitoring.log - this is a cleanup script that deletes all the logs generated by the above scripts

$EAMSROOT/var/log/MariaPanacesDBStats-20210827_171202.log.gz - this will report the database-related information like table size, etc

$EAMSROOT/var/log/ROServerStats-20210827_171202.log.gz - this will report the CPU and memory consumed by the RO Server appNote:

The current date time would be appended to the above logs in YYYYMMDD_HHMMSS format. Following entries should be added by issuing crontab -e. Replace the path /app/panaces below with your respective path for $EAMSROOT. The scripts below are scheduled to run every 12 hours except for the two scripts viz. delete_logs.sh which would execute every 3rd day of the month and MariaDBConnectionStatsForServer.sh which will execute every 5 minutes. These schedules can be adjusted as per your requirements.

You would also need to update the MariaDBConnectionStatsForServer.sh and MariaPanacesDBStats.sh to reflect the correct password. Replace the text 'your password' accordingly.

Please ensure to remove the password from both the files after necessary logs have been captured.

```
* */12 * * * /app/panaces/tools/monitoring/ThreadDumpROServer.sh
0 */12 * * * /app/panaces/tools/monitoring/GCClassStats.sh
0 */12 * * * /app/panaces/tools/monitoring/GCHistogram.sh
0 */12 * * * /app/panaces/tools/monitoring/ROServerStats.sh
*/5 * * * /app/panaces/tools/monitoring/MariaDBConnectionStatsForServer.sh
*/5 * * * /app/panaces/tools/monitoring/MariaPanacesDBStats.sh
0 */12 * * * /app/panaces/tools/monitoring/SarReport.sh
* * */3 * * /app/panaces/tools/monitoring/delete_logs.sh
```

7.22 Standby server configuration

Master Node: XXX.xxx.XXX.XXX

Slave 01: XXX.XXX.xxx.xxx

1. Open /etc/my.cnf file.
2. Add the following three parameters under the [mysqld] section and save it. Replace 10.128.0.11 with your server IP.

```
server-id               = 1
```

```
log_bin                    = mysql-bin
```

3. Restart the MySQL server for the configuration changes to take place.

   ```
   systemctl restart mysqld
   ```

4. Check the MySQL status to make sure all the configurations are applied as expected without any errors.

   ```
   systemctl status mysqld
   ```

5. Login to the MySQL server as the root user.
6. Create a user named replicauser with a strong password. This user will be used by the slaves to replicate the data from the master. Replace 10.128.0.11 with your master IP

   ```
   CREATE USER 'replicauser'@'XXX.xxx.XXX.XXX'
   IDENTIFIED BY '<Password>';
   ```

7. Grant privileges to the slave user for slave replication.

   ```
   GRANT REPLICATION SLAVE ON *.* TO 'replicauser'@'%'
   IDENTIFIED BY '<Password>';
   ```

8. From the MySQL prompt, Check the master status. Note down the file [mysql-bin.000001] and Position[706] parameters from the output. It is required for the slave replication configuration.

   ```
   SHOW MASTER STATUS\G
   ```

The output would look like the following.

```
mysql> SHOW MASTER STATUS\G

*************************** 1. row
***************************

             File: mysql-bin.000001

         Position: 706
```

```
     Binlog_Do_DB:
 Binlog_Ignore_DB:
Executed_Gtid_Set:
1 row in set (0.00 sec)
```

9. Take a backup of the mariadb database and transfer the backup to a slave server.

```
mysqldump -u root -p --databases panaces pfr --
routines=true --triggers > backup.sql
```

```
[root@my_server bin]# scp backup.sql
my_user@slave_server:/tmp/
my_user@slave_server's password:
backup.sql
100% 6256KB 121.1MB/s   00:00
[root@my_server bin]#
```

Slave server steps

```
mysql -u root -p
drop database panaces;
drop database pfr;
exit
```

```
vi /etc/my.cnf and add this line
log_bin_trust_function_creators = 1
```

```
mysql -u root -p


SET GLOBAL log_bin_trust_function_creators = 1;

exit


mysql -u root -p < backup.sql
```

Configure MySQL Replication Slave Node

1. Add the same configurations as the master to the /etc/my.cnf file with the Slave Ip address and unique server ID.

   ```
   server-id               = 2

   log_bin                 = mysql-bin
   ```

2. Restart the MySQL service.

   ```
   systemctl restart mysqld

   Step 3: Login to MySQL with root credentials.

   mysql -uroot -p
   ```

3. Stop the slave threads using the following command.

   ```
   STOP SLAVE;

   mysql -uroot -p

   CREATE USER 'replicauser'@'XXX.XXX.xxx.xxx'
   IDENTIFIED BY '<Password>';
   ```

```
GRANT REPLICATION SLAVE ON *.* TO 'replicauser'@'%'
IDENTIFIED BY '<Password>';
```

4. Execute the following statement from MySQL prompt replacing the master IP [10.128.0.15], replicauser password [replicauser-secret-password].

   Replace MASTER_LOG_FILE & MASTER_LOG_POS with the values, you got from step 8 in the master configuration.

```
CHANGE MASTER TO
MASTER_HOST='XXX.XXX.xxx.xxx',MASTER_USER='replicause
r', MASTER_PASSWORD='<Password>',
MASTER_LOG_FILE='mysql-bin.000???', MASTER_LOG_POS=
???;
```

5. Start the slave threads.

```
START SLAVE;
```

6. Check the MySQL replication slave status.

```
SHOW SLAVE STATUS\G
```

Slave_SQL_Running_State parameter will show the current slave status.

8 Starting and Stopping Resiliency Orchestration Server

8.1.1 Starting Resiliency Orchestration Server

To start the Kyndryl Resiliency Orchestration Server, perform the following steps:

1. Open a terminal using the sanovi user

114. Enter the following command at the command prompt:

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

If you are starting the Kyndryl Resiliency Orchestration Server for the first time, then it would take about five minutes to register its components. Kyndryl Resiliency Orchestration GUI operation will be available after the component registration. Please wait till the GUI becomes available to you.

8.1.2 Starting Resiliency Orchestration Server in Recover Mode

You will need to perform the following steps to start Kyndryl Resiliency Orchestration Server in recover mode:

1. Open a terminal using the sanovi user

115. Enter the following command at the command prompt:

```
sudo $EAMSROOT/bin/panaces recover
```

8.1.3 Stopping Resiliency Orchestration Server

1. Open a terminal using the sanovi user

116. Enter the following command at the command prompt:

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

8.1.4 Restarting Resiliency Orchestration Server

To restart the Kyndryl Resiliency Orchestration Server, perform the following steps:

1. Open a terminal using the sanovi user

117. Enter the following command at the command prompt:

```
sudo $EAMSROOT/bin/panaces restart
```

8.1.5 Checking Resiliency Orchestration Server Status

1. Open a terminal using the sanovi user

118. Enter the following command at the command prompt:

```
sudo $EAMSROOT/bin/panaces status
```

8.1.6 Resiliency Orchestration Server Remote Services

The user needs to confirm that the remote services are running with panaces users.

1. If the services are not running with panaces user, run the following script to stop the services:

```
sudo ./invokeAgentCommand.sh <agent script> stop <IP> LINUXSERVER
```

119. Run the following script to start remote services:

```
sudo ./invokeAgentCommand.sh <agent script> start <IP>
LINUXSERVER
```

> **Note**
>
> The invokeAgentCommand.sh script is available at EAMSROOT/bin

8.1.7 Checking Resiliency Orchestration Server Available Modes

You need to perform the following steps to check the available modes of the Kyndryl Resiliency Orchestration Server:

1. Open a terminal using the sanovi user

120. Enter the following command at the command prompt:

```
sudo $EAMSROOT/bin/panaces help
```

This command will display the following options:

- **start**: Starts the Kyndryl Resiliency Orchestration Server and Tomcat Server
- **restart**: Restarts the Kyndryl Resiliency Orchestration Server and Tomcat Server
- **stop**: Stops the Kyndryl Resiliency Orchestration Server and Tomcat Server
- **recover**: Starts the Kyndryl Resiliency Orchestration Server in recovery mode with Tomcat Server
- **status**: Shows whether Kyndryl Resiliency Orchestration Server and Tomcat are running or not
- **help**: Shows this help
- **debug**: Runs Tomcat and Kyndryl Resiliency Orchestration, with remote debugging enabled (To debug Tomcat, connect to port 8000. To debug Kyndryl Resiliency Orchestration, connect to port 8001)

> **Note**

kyndryl

Do not stop Kyndryl Resiliency Orchestration Server immediately after starting as this might not stop Tomcat, or event registration may not happen properly.

8.1.8 Scenarios that Require a RO Restart Take Effect

The RO restart is required in the following scenarios:

- After discovering the site controllers (both in Linux or Windows) in RO and Mapping is done, the site controllers will be in an active state, but the subsystems mapped with them will be in an unknown state (as SC mapped component OS Agents are not managed by uni agent but a separate OS agent is created) until the RO server is restarted when a defect is found in 8.3 version.
- When a vault (for example, CyberArk) is configured in RO, restart the RO to see the configuration.
- During HA configuration, pause the RO until HA is configured and start again once HA is configured.
- Birt report configuration: Restart the RO once the Post BIRT report is configured.
- AD configuration: Restart the RO during AD configuration.
- Restart a RO if there are any changes in the following property files: panaces.properties, anacesAgentGeneric.properties, SiteController.cfg.

kyndryl

9 Installing Site Controller on Linux

9.1 Installation Overview

The Site Controller Software has the following components for installation:

- Site Controller Server GUI mode installation
- Site Controller Server Silent mode installation

9.2 Client Browser Prerequisites

For browser compatibility, please refer to *Supported Browsers*.

9.3 Ports Used by Linux Based Site Controller

The following default port is used in the communication protocol:

Table 19: Ports Used by Linux Based Site Controller

Port	Description
8162, 42443 and 45443	For communication between Site Controller and Kyndryl Resiliency Orchestration Server, Agents. • Kyndryl Resiliency Orchestration Server to Site Controller, open 45443 and 42443 bi-directional and open 8162 uni-directional. • Kyndryl Resiliency Orchestration Agents to Site Controller open ports as uni-directional.

9.4 Prerequisites

Based on the features, download the GPL dependent binaries from this link *GPL dependent binaries* before Site Controller installation.

For more information about the GPL licenses, see *GPL License Information.*

Note: One Component IP should be configured to only one SC in Linux.

Note: In the case of the co-hosted site controller.

We need to set it within Sitecontroller.cfg. setting as mentioned below

(change default setting 0.0.0.0)

```
PANACES_SITE_CONTROLLER_BIND_ADDRESS=SitecontrollerIP
```

kyndryl

You can perform the following method to install the Site Controller:

- **Graphical Mode**: Graphical mode installation is an interactive, GUI-based method for installing Site Controller. It is supported on the Linux platform. Refer to the following sections for more details on Graphical Mode installation.
  - Installing Site Controller in GUI Mode in Linux
  - MS-Windows
- **Silent Mode:** Silent mode installation is a non-interactive method of installing a Site Controller. This method requires the use of properties files for selecting installation options. It is supported on Linux.
  - Installing Site Controller in Silent Mode in Linux

9.5 Installing Site Controller in GUI Mode in Linux

This section describes the procedure to install the Site Controller on Linux (Refer to Supported OS for Kyndryl Resiliency Orchestration and Site Controller for the version to install). Additional steps that you must perform are also included within.

Note

You must have root or root equivalent privileges to install Site Controller. The Site Controller and Agent Node services are installed when the installation file is executed.

To install the Site Controller, perform the following steps:

1. Download the Site Controller binaries from the given ftp path.
2. Execute the following command (use whichever is applicable):

```
sh SiteController.bin (or) ./SiteController.bin at the command
prompt to run the Site Controller installer.
```

Note

Ensure that free space of approximately 2.5 GB is available in the server where the Site Controller needs to be installed, before executing the above command. In case the/tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.

Example-

Assuming you want to make /opt/temp as the temporary directory.

#export IATEMPDIR=/opt/temp

After exporting the IATEMPDIR environment variable, proceed with the installation.

121. If the command to run the Site Controller installer is executed, the Site Controller installation starts with the screen as shown in the following figure:

Note

If the RHEL version is not 7.x/8.x, a warning message will be displayed on the screen. However, the user can continue with the installation.

Figure 35: Kyndryl Resiliency Orchestration Site Controller Installer

122. After displaying the **Kyndryl Resiliency Orchestration Agent Node** Installer screen, the Introduction window is displayed as shown in the following figure:

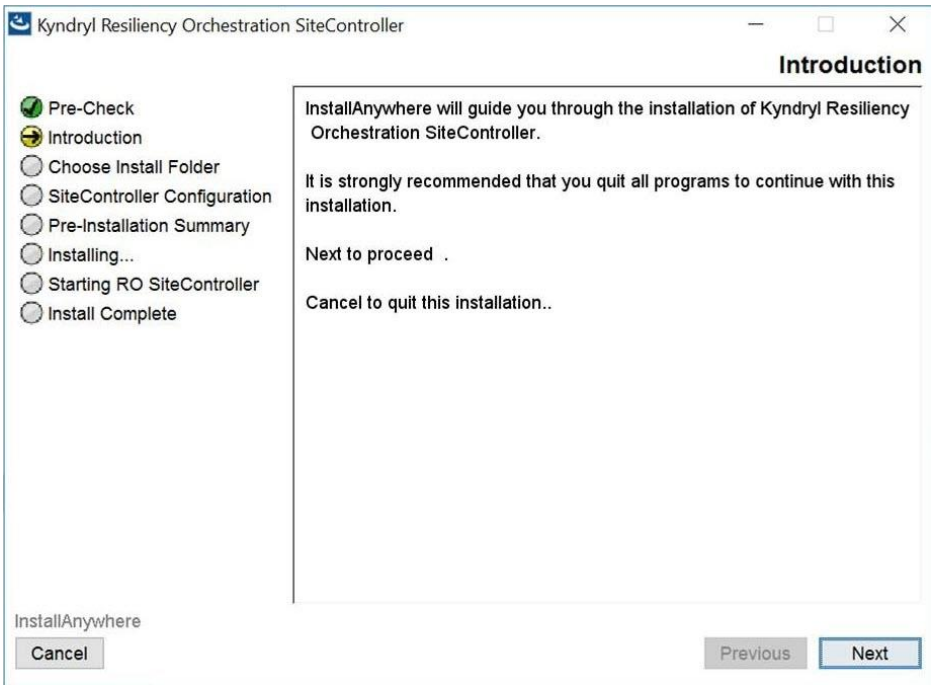


Figure 36: Kyndryl Resiliency Orchestration Site Controller Installation on Linux - Introduction

123. Click **Next**. The **Choose Install Folder** window is displayed.

124. Select a path to install the software by clicking **Choose.** Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is **/opt/panaces**. It is recommended that you use the default path, which is displayed.

125. Click **Next**. The Kyndryl Resiliency Orchestration Agent Node Configuration window is displayed.

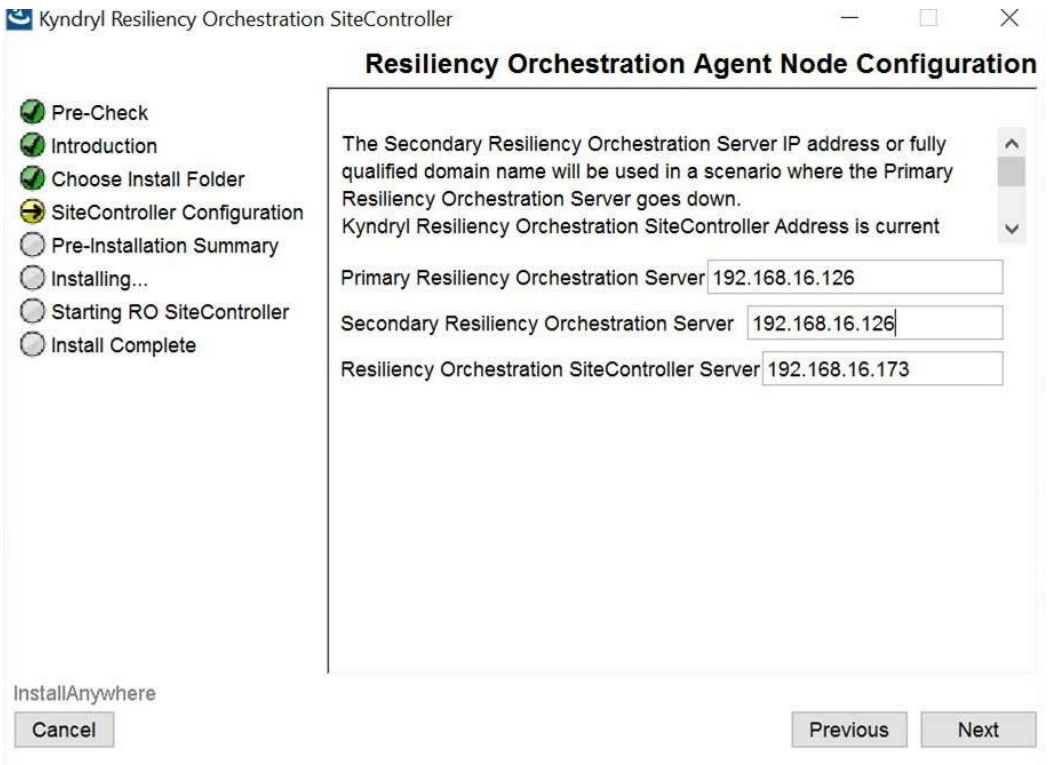


Figure 37: Kyndryl Resiliency Orchestration Site Controller Installation on Linux – Kyndryl Resiliency Orchestration Site Controller Agent Node Configuration

126. Enter the IP addresses/Name of the primary and secondary Kyndryl Resiliency Orchestration servers and Kyndryl Resiliency Orchestration Site Controller Address. In a nonNAT environment, the NAT IP address should be left blank.

> **Note**
>
> In the NAT environment, Primary and secondary Kyndryl Resiliency Orchestration Server public IP should be provided. The site Controller address should be the public IP and the NAT IP address should be the private IP of the server where you are installing.
>
> To change NAT IP configuration after installation or to troubleshoot, refer to the *NAT IP* section in the Troubleshooting chapter in Resiliency Orchestration Installation Guide.

127. Click **Next**. The **Pre-Installation Summary** window is displayed.

128. Verify the inputs provided. If you want to change the inputs, click **Previous** and modify the details.

129. Click **Install.** The Installing **Kyndryl Resiliency Orchestration Agent Node** window is displayed.

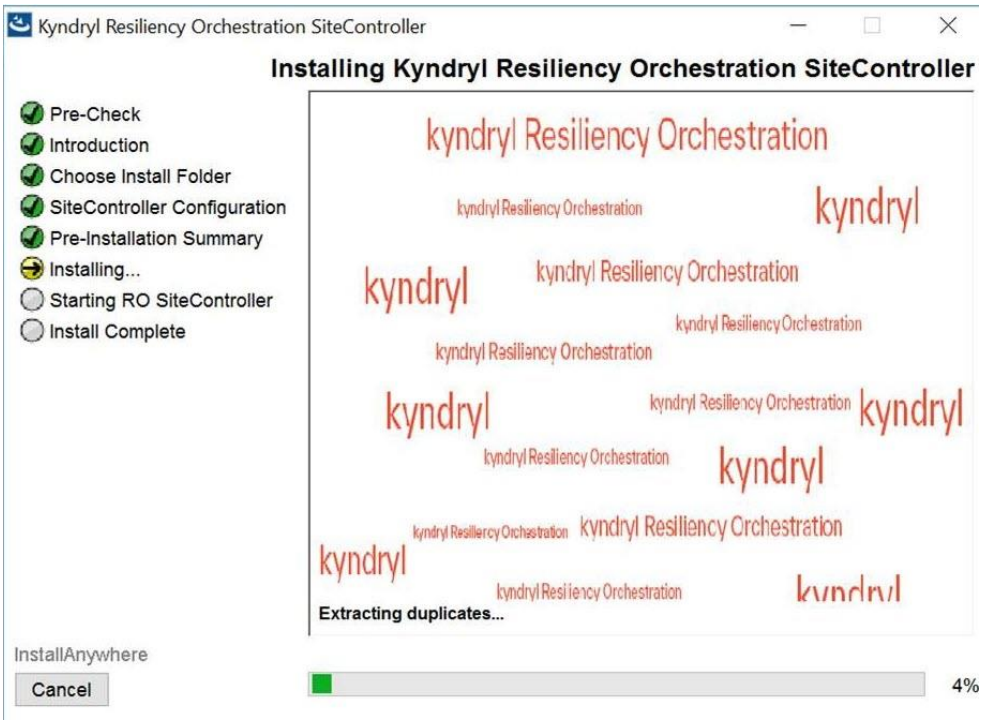


Figure 38: Kyndryl Resiliency Orchestration Site Controller Installation on Linux - Installing Kyndryl Resiliency Orchestration Site Controller

130. Once the installation is complete, the **Starting Kyndryl Resiliency Orchestration Agent Node** window is displayed.

Figure 39: Kyndryl Resiliency Orchestration Site Controller Installation on Linux - Starting Kyndryl Resiliency Orchestration Site Controller

131. On the **Starting Kyndryl Resiliency Orchestration Agents Node** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

> **Note**
>
> The best practice is not to change the default value displayed on the Starting Kyndryl Resiliency Orchestration Agent Node window.

132. Click **Next**. The **Installation Completed** window is displayed indicating successful installation.

133. Click **Done** to complete the installation process.

> **Note**

When the installation is carried on silent mode or GUI mode, restart with a Putty session.

134. Post installation, add the following properties in /opt/panaces/installconfig/SiteController.cfg file:

MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE=50

Note:

Determine the number of agents that will connect to the site controller. Set `MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE` to 1.5 times the number of agents. For example, for 100 agents set `MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE` to 150.

135. Start the Site Controller manually.

9.6 Installing Site Controller in Silent Mode in Linux

In the silent mode installation method, the installation program reads the settings for your configuration from the properties file before installation. The installation program does not display any configuration options during the installation process.

The following sections describe how to install the Site Controller server using the installation program in silent mode on Linux platforms. It is assumed that the user has acquired the installation program and properties file from the FTP server.

Note

Confirm that the hardware and software configuration required for Site Controller installation is in place.

9.6.1 Editing Properties File

When installing Site Controller in silent mode, the installation program uses the **properties** file for the server (PanacesAgentNodeInstaller.properties) to determine which installation options should be implemented. You need to edit the respective properties file to specify the installation options that you want to invoke while performing the Agents installation after which you can run the installation program in silent mode. Perform the following steps to edit the properties files.

1. Get the files from the FTP server and copy properties files by running the following command:

```
cp AgentNode/PanacesAgentNodeInstaller.properties /tmp

cp AgentNode/SiteController.bin  /tmp
```

136. Open the properties file by using the following command:

```
vi /tmp/ PanacesAgentNodeInstaller.properties
```

Modify the respective properties file for the keywords shown in the following tables, to reflect your configuration.

The following table describes the keywords of the PanacesAgentNodeInstaller.properties file.

Table 20: Keywords of PanacesAgentNodeInstaller.properties File

Keyword	Description
INSTALLER_UI	Displays the mode of installation as "silent".
MODIFY_SYSTEM_FILES=1	Setting this property to 1 modifies the following system files: /etc/hosts,/etc/sysconfig/selinux, /etc/sysctl.conf Refer to link MODIFY_SYSTEM_FILES for details.
USER_INSTALL_DIR	Enter the path for the directory to install the Site Controller Server software (default path is /opt/panaces/)
USER_INPUT_RESULT_PRIMARY_PANACES_SERVER	Enter the IP address/Name of the primary server.
USER_INPUT_RESULT_SECONDARY_PANACES_SERVER	Enter the IP address/Name of the secondary server.
PANACES_AGENT_NODE_ADDRESS	Enter the IP address/Name of the Local machine.
AGENTNODE_START_YES	Enter 1 if you want to start the agents automatically after the installation. Enter 0 if you want to start the agent manually.

138. Proceed to the Post-installation procedure. For instructions, see *Post-installation Steps*.

kyndryl

9.6.2 Site Controller Silent Mode Installation

The following section provides steps to install Site Controller in silent mode on a Linux server.

```
/tmp/SiteController.bin –f
/tmp/PanacesAgentNodeInstaller.properties
```

> **Note**
>
> In silent mode, uninstallation does not check whether services are running or not. The user needs to make sure that services are stopped before uninstallation in silent mode.

9.6.3 Post-installation Steps after you install the Site Controller in Linux

1. In the Site Controller installation folder, perform the following steps:
   - Go to the location: `$EAMSROOT/installconfig/`
   - Open the `SiteController.cfg` file
   - Add the following property:

     `MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE=50`

> **Note:**
>
> Determine the number of agents that will connect to the site controller. Set `MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE` to 1.5 times the number of agents.
>
> For example, for 100 agents set `MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE` to 150.

139. Enter the value of the ACP keystore in the \installconfig\SiteController.cfg file.

For Example panaces.acp.keystore=

> **Note**
>
> The value of the ACP keystore will be the path where the ACP key store exists, which means <Site controller installation folder>\installconfig\keystore\panacesACP.keystore. Enter the path with a \\ for

file separator, for example, c:\\Sitecontroller\\installconfig\\keystore\\panacesACP.keystore

140. Enter the path of the truststore in the same SiteController.cfg file.

For Example: panaces.acp.truststore=

> **Note**
>
> This value of the ACP truststore will be the path where the ACP trust store exists, which means <Site controller installation folder>\installconfig\keystore\ panacesACP.truststore. Enter the path with a \\ for file separator, for example, c:\\Sitecontroller\\installconfig\\keystore\\ panacesACP.truststore
>
> Ensure to create your truststore and keystore and use them as the corresponding values for the truststore and keystore.

141. Copy the `Actifio_getStatus.tcl` file from Kyndryl Resiliency Orchestration Server from $EAMSROOT/agents folder to $EAMSROOT/agents folder.

142. If libnsl.so.1 is not available in the/lib64 folder, please perform the following steps

    a. Create a copy of libnsl.so.2 in the /lib64 folder of the root.

    b. Rename copy to libnsl.so.1 in /lib64 folder.

143. When the Site Controller has a NAT IP, and post-installation the Site Controller is in an 'Unknown' state, follow the below steps –

    a. Stop the Site Controller services and the Agents running on the Site Controller.

    b. Update the configurations in `$EAMSROOT/installconfig/SiteController.cfg` file in the below listed properties -

```
PANACES_MASTER_SERVER_ADDRESS=<PRIMARY_RO_IP>
PANACES_SLAVE_SERVER_ADDRESS=<STANDBY_RO_IP>
PANACES_SITE_CONTROLLER_ADDRESS=<NAT_IP>
PANACES_SITE_CONTROLLER_BIND_ADDRESS=0.0.0.0
```

    c. Update the configurations in `$EAMSROOT/installconfig/PanacesAgentGeneric.cfg` file in the below listed properties -

```
PANACES_MASTER_SERVER_ADDRESS=<PRIMARY_RO_IP>
PANACES_SLAVE_SERVER_ADDRESS=<STANDBY_RO_IP>
PANACES_AGENT_NODE_ADDRESS=<NAT_IP>
PANACES_AGENT_NODE_BIND_ADDRESS=<PRIVATE/LOCAL_IP>
PANACES_SITE_CONTROLLER_ADDRESS=<NAT_IP>
PANACES_SITE_CONTROLLER_NATIP_ADDRESS=<PRIVATE/LOCAL_IP>
```

d. Run the Security User Injection script -
`./$EAMSROOT/bin/SecurityUserInjection.sh`

e. Start the Site Controller services and Agents running on Site Controller.

9.6.3.1 Post Validation Steps During Server Startup in Linux

Follow the post validation steps during server startup while performing the procedure "Post-installation Steps after you install the Site Controller in Linux".

1. Navigate to *the* **PanacesAgentGeneric.cfg** file under the `$EAMSROOT/installconfig` folder.
2. Execute the following command:
   `ps -ef | grep <Give AIX IP address>`
3. Locate the PID from the output generated in step 2 and execute the following command:
   `kill -9 <AIX agent PID>`
4. Execute the following script under the **$EAMSROOT/bin** folder.
   `SecurityUserInjection.sh script`
5. Restart the panaces service.
6. Navigate to the **Subsystem Discovery Page** in GUI and modify the AgentNode component from hostname to IPaddress.
7. After modifying the Agent node from hostname to IP address, start the AIX agents from GUI.

9.6.3.2 Limitation for Linux Site controller:

- Linux Site Controller cannot support windows endpoints.
- A different windows SC will be required for the Support of the Windows endpoint.

9.6.4 Starting Site Controller Manually

User can start the Site Controller manually by logging in to the Site Controller server and performing the following steps:

1. Enter in the `$EAMSROOT/bin` folder.
2. Run the following command to start Site Controller.
   `sh SiteController.sh start`

   `or`

```
./SiteController.sh start
```

Run the following command to start Agent Node.

```
sh LinuxOSAgent.sh start

or

./LinuxOSAgent.sh start
```

9.6.5 Stopping Site Controller Manually

User can stop the Site Controller manually by logging in to the Site Controller server and performing the following steps:

1. Enter in the `$EAMSROOT/bin` folder.
2. Run the following command to stop the Site Controller.
   ```
   sh SiteController.sh stop

   or ./SiteController.sh stop
   ```
3. Run the following command to stop the Site Controller.
   ```
   sh LinuxOSAgent.sh stop

   or ./LinuxOSAgent.sh stop
   ```

9.7 Uninstalling Site Controller

This section describes the procedure to uninstall the Site Controller in GUI mode and Silent mode.

9.7.1 Uninstalling Site Controller in GUI Mode

Perform the following steps to uninstall Site Controller e in GUI mode:

1. Enter in the <$EAMSROOT>/UninstallerData folder.

144. Click the `Uninstall_IBM_Resiliency_Orchestration_Agent_Node` file. The **Uninstall Kyndryl Resiliency Orchestration Agent Node** window is displayed, as shown in the following figure:

145. Click **Uninstall**.

146. The uninstallation process begins. When the uninstallation process is complete, the **Uninstall Complete** window is displayed.

147. Click **Done** to close this window.

kyndryl

9.7.2 Uninstalling Site Controller in Silent Mode

Perform the following steps to uninstall Site Controller in silent mode:

1. Enter in the <$EAMSROOT>/UninstallerData folder.

148. Run the following command to uninstall the Site Controller.

```
sh Uninstall_IBM_Resiliency_Orchestration_Agent_Node

or ./ Uninstall_IBM_Resiliency_Orchestration_Agent_Node
```

9.8 Upgrading Site Controller

Perform the following steps to upgrade the Site Controller.

1. Download the latest version of Site Controller binaries from Passport Advantage/ Fix Central.
2. Uninstall the existing version of the Site Controller. To uninstall, refer to the procedure Uninstalling Site Controller.
3. Install the latest version of Site Controller in GUI mode or Silent mode. To install in GUI mode, refer to Installing Site Controller in GUI Mode in Linux. To install in Silent mode, refer to Installing Site Controller in Silent Mode in Linux.

9.9 Monitoring Health of Linux Site Controller

Prerequisite

These scripts need a sysstat package to work. Please make sure you have it installed before moving forward. sudo yum install sysstat
Start sysstat service

```
sudo systemctl start sysstat
sudo systemctl enable sysstat### Crontab
The following entry should be added(by a user with adequate privileges) by issuing crontab -e. Replace the path /app/panaces below with your respective path for $EAMSROOT*/15 * * * *
/app/panaces/tools/monitoring/sitecontroller/linux/SCResourcesStats.sh
0 * * * *
/app/panaces/tools/monitoring/sitecontroller/linux/ThreadDumpSC.sh
0 * * * *
/app/panaces/tools/monitoring/sitecontroller/linux/GCClassStatsSC.sh
0 * * * *
```

```
/app/panaces/tools/monitoring/sitecontroller/linux/GCHistog
ramSC.sh
0 * * * *
/app/panaces/tools/monitoring/sitecontroller/linux/SarRepor
tSC.sh
* * */3 * *
/app/panaces/tools/monitoring/sitecontroller/linux/delete_l
ogsSC.sh
```

9.10 Site Controller with Dual IP Support

Perform the following steps when the Site Controller has a Dual IP's Overlay Network and Underlay Network, and post-installation of the Site Controller is in an Unknown.

1. Stop the site controller services and the agents running on the site controller.
2. Update the configurations in $EAMSROOT/installconfig/SiteController.cfg file in the below listed properties:

```
PANACES_MASTER_SERVER_ADDRESS=<PRIMARY_UNDERLAY_RO_IP>

PANACES_SLAVE_SERVER_ADDRESS=<STANDBY_UNDERLAY_RO_IP>

PANACES_AGENT_NODE_ADDRESS=<DUAL_HOMED_ UNDERLAY _SC_IP>

PANACES_AGENT_NODE_BIND_ADDRESS=<DUAL_HOMED_OVERLAY_SC_IP
>

PANACES_SITE_CONTROLLER_ADDRESS<DUAL_HOMED_UNDERLAY_SC_IP
>

PANACES_SITE_CONTROLLER_NATIP_ADDRESS=<DUAL_HOMED_OVERLAY
_SC_IP>

IS_SERIALCALL_ENABLED=false
```

3. Update the configurations in $EAMSROOT/installconfig/PanacesAgentGeneric.cfg file in the below listed properties:

```
PANACES_MASTER_SERVER_ADDRESS==<PRIMARY_UNDERLAY_RO_IP>

PANACES_SLAVE_SERVER_ADDRESS=<STANDBY_UNDERLAY_RO_IP>

PANACES_SITE_CONTROLLER_ADDRESS=<DUAL_HOMED_UNDERLAY_SC_I
P> PANACES_SITE_CONTROLLER_BIND_ADDRESS=0.0.0.0

PANACES_SITE_CONTROLLER_PORT=45443
```

Perform the following steps when the PFR Agent is in Overlay Network and configured with Dual SC's, and post-installation of the PFR Local Agent is in an Unknown state:

1. Stop the PFR Agent and Windows OS agent services on the Local Agents.
2. Update the configurations in $EAMSROOT/installconfig/PanacesAgentGeneric.cfg file in the below listed properties:

```
PANACES_MASTER_SERVER_ADDRESS=<PRIMARY_UNDERLAY_RO_IP>
PANACES_SLAVE_SERVER_ADDRESS=<STANDBY_UNDERLAY_RO_IP>
PANACES_AGENT_NODE_ADDRESS=<OVERLAY_LOCAL_AGENT_IP>
PANACES_AGENT_NODE_BIND_ADDRESS=<OVERLAY_LOCAL_AGENT_IP>
PANACES_SITE_CONTROLLER_ADDRESS=<DUAL_HOMED_UNDERLAY_SC_IP>
PANACES_SITE_CONTROLLER_NATIP_ADDRESS=<DUAL_HOMED_OVERLAY_SC_IP>
IS_SERIALCALL_ENABLED=false
```

10 Installing Site Controller Server or Site Controller in MS-Windows

10.1 Installation Overview

Site Controller Software has the following components for installation:

- Site Controller Server GUI mode installation (**Graphical Mode**: Graphical mode installation is an interactive, GUI-based method for installing Site Controller. It is supported on the Linux platform.)
- Site Controller Server Silent mode installation (**Silent Mode:** Silent mode installation is a non-interactive method of installing a Site Controller. This method requires the use of properties files for selecting installation options. It is supported on Linux.)

10.2 Installation and Services

Perform installations and services in the following order:

1. Install the Kyndryl Resiliency Orchestration
2. Installation of Site Controller by using either the GUI mode or Silent mode
3. Configuring Agents to use PowerShell framework
4. Start Site Controller
5. Start Agent Node on Site Controller

10.3 Client Browser Prerequisites

For browser compatibility, please refer to Supported Browsers.

10.4 Ports Used by Windows Based Site Controller

The following ports are used in the communication protocol.

Table 21: Ports Used by Windows-Based Site Controller

Port	Description
5985, 5986, 135	For Powershell operations from Windows-based Site Controller to Endpoints. **Note:** This is a unidirectional communication.
42443, 45443	For communication between the Windows-based Site Controller and the IBM Resiliency Orchestration Server.

	Note: This is a bidirectional communication. 42433 is an open port on SC for RO to connect while 45443 is an open port on SC for Remote/Local agents to connect.

Note: 1. The specific ports based on the solution configured need to be opened unidirectional from Windows SiteController to the Endpoints.

For example: For Oracle, MSSQL endpoint servers, for auto-discovery, open 1521, 1433 default ports from source Windows SiteController, and the destination Endpoints. If custom ports are to be configured then those ports are supposed to be opened.

2.Port 135 is used for ping operations on windows endpoints, hence is required to be opened up on the endpoints for the ping operations to be successful.

10.5 Prerequisites

- Based on the features, download the GPL dependent binaries from this link *GPL dependent binaries* before Site Controller installation.

  For more information about the GPL licenses, see *GPL License Information*

- The virtual memory for the windows machine must have a minimum of 1.5 times the RAM configured and a maximum of 3 times.

Note: One Component IP should be configured to only one SC in Windows.

10.6 Installing Site Controller in GUI Mode in Windows

This section describes the procedure to install the Site Controller Server on MS Windows. Additional steps that you must perform are also included within.

> **Note**
>
> You must have root or root equivalent privileges to install Site Controller. The Site Controller and Site Controller services are installed when the installation file is executed.

To install the Site Controller, perform the following steps:

1. Download the Site Controller binaries from the given FTP path.
2. Files are available in the zipped format in the **AgentNode folder.**

3. Right-click on `SiteController.exe` and then, select the option **Run as administrator**.

> **Note**
>
> The user needs a free space of approximately 2.5 GB in the server where the Site Controller needs to be installed, before executing the above command. In case the/tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.
>
> Example-
>
> Assuming you want to make /opt/temp as the temporary directory.
>
> #export IATEMPDIR=/opt/temp
>
> After exporting the IATEMPDIR environment variable, proceed with the installation.

149. If the command to run the Site Controller installer is executed, the Site Controller installation starts with the screen as shown in the following figure:

Figure 40: Kyndryl Resiliency Orchestration Site Controller Installer on Windows

150. After displaying the **Kyndryl Resiliency Orchestration Agent Node** Installer screen, the **Introduction** window is displayed as shown in the following figure:

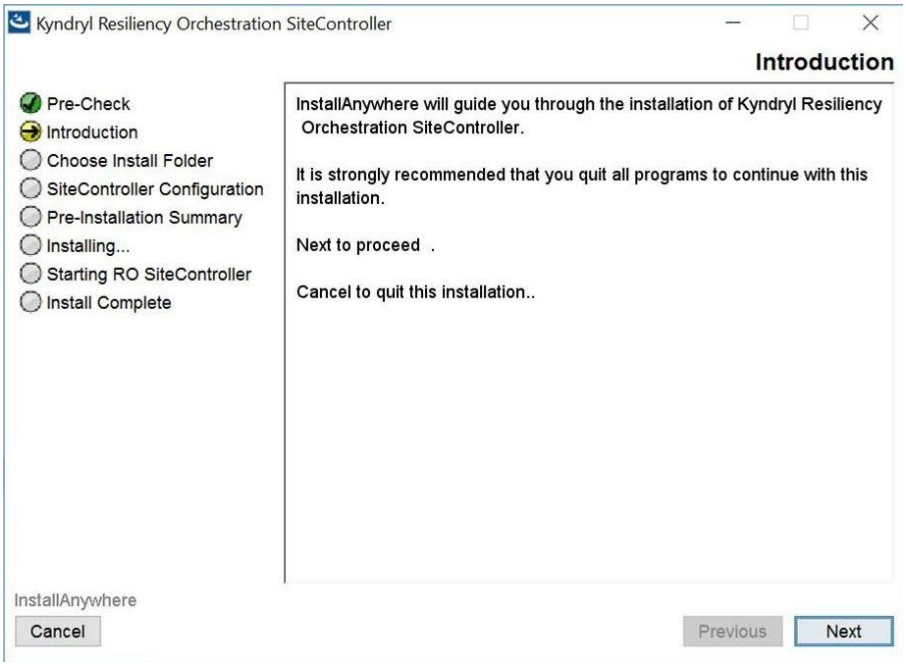


Figure 41: Kyndryl Resiliency Orchestration Agent Node Installation on Windows - Introduction

151. Click **Next**. The **Choose Install Folder** window is displayed.

Figure 42: Kyndryl Resiliency Orchestration Agent Node Installation on Windows- Choose Install Folder

152. Select a path to install the software by clicking **Choose.** Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is **$EAMSROOT**. It is recommended that you use the default path, which is displayed.

153. Click **Next**. The **Kyndryl Resiliency Orchestration Agent Node** Configuration window is displayed.

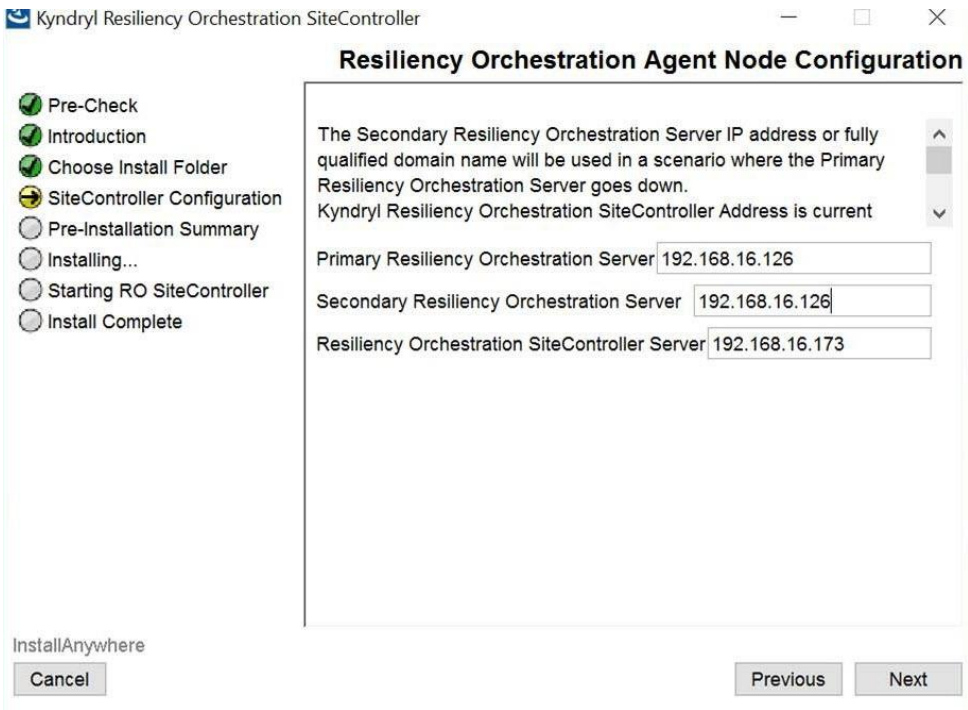


Figure 43: Kyndryl Resiliency Orchestration Agent Node Installation on Windows – Kyndryl Resiliency Orchestration Agent Node Configuration

154. Enter the IP addresses/name of the primary and secondary Kyndryl Resiliency Orchestration servers and Kyndryl Resiliency Orchestration Site Controller Address. In a nonNAT environment, the NAT IP address should be left blank.

> **Note**
>
> - In the NAT environment, Primary and secondary Kyndryl Resiliency Orchestration Server public IP should be provided. The site Controller address should be the public IP and the NAT IP address should be the private IP of the server where you are installing.
> - To change the NAT IP configuration after installation or to troubleshoot, refer to the *NAT IP* section in the Troubleshooting chapter.

155. Click **Next**. The **Pre-Installation Summary** window is displayed.

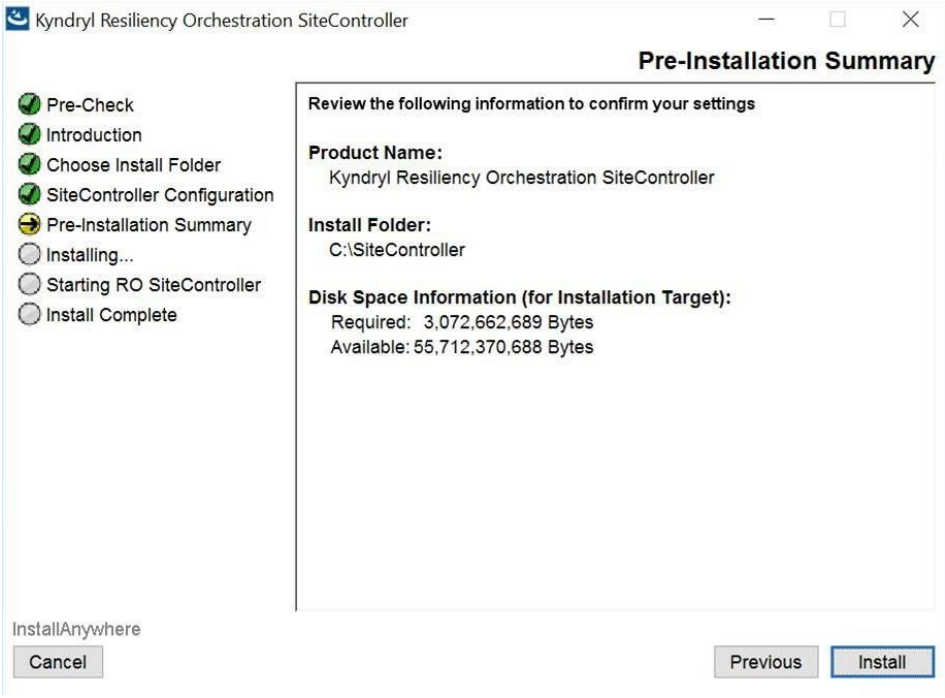


Figure 44: Kyndryl Resiliency Orchestration Site Controller Installation on Windows - Pre-Installation Summary

156. Verify the inputs provided. If you want to change the inputs, click **Previous** and modify the details.

157. Click **Install.** The Installing Kyndryl Resiliency Orchestration Agent Node window is displayed.

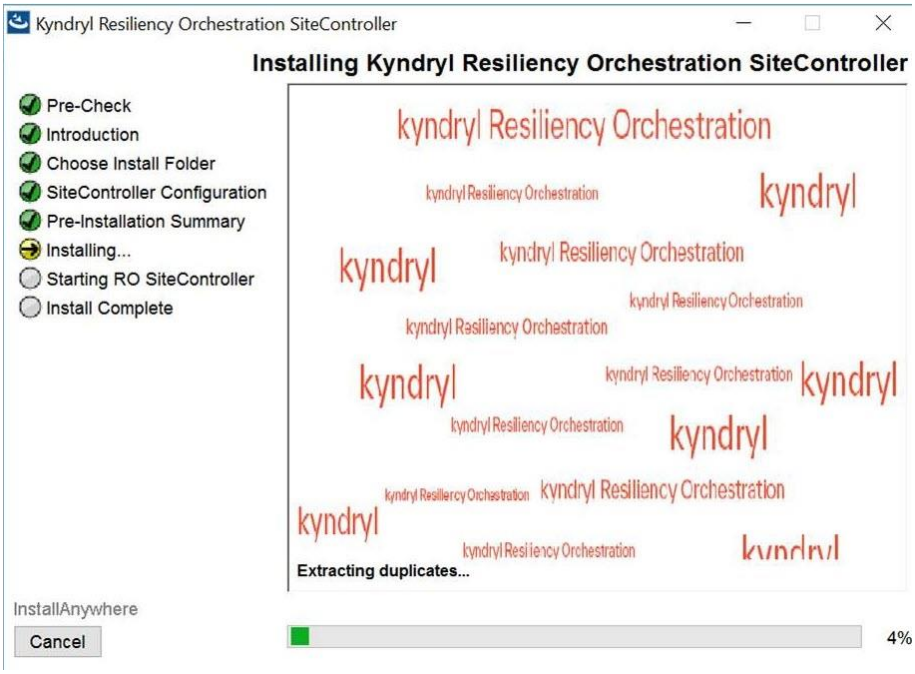


Figure 45: Kyndryl Resiliency Orchestration Site Controller Installation on Windows - Installing Kyndryl Resiliency Orchestration Site Controller

158. Once the installation is complete, the **Starting Kyndryl Resiliency Orchestration Agent Node** window is displayed.

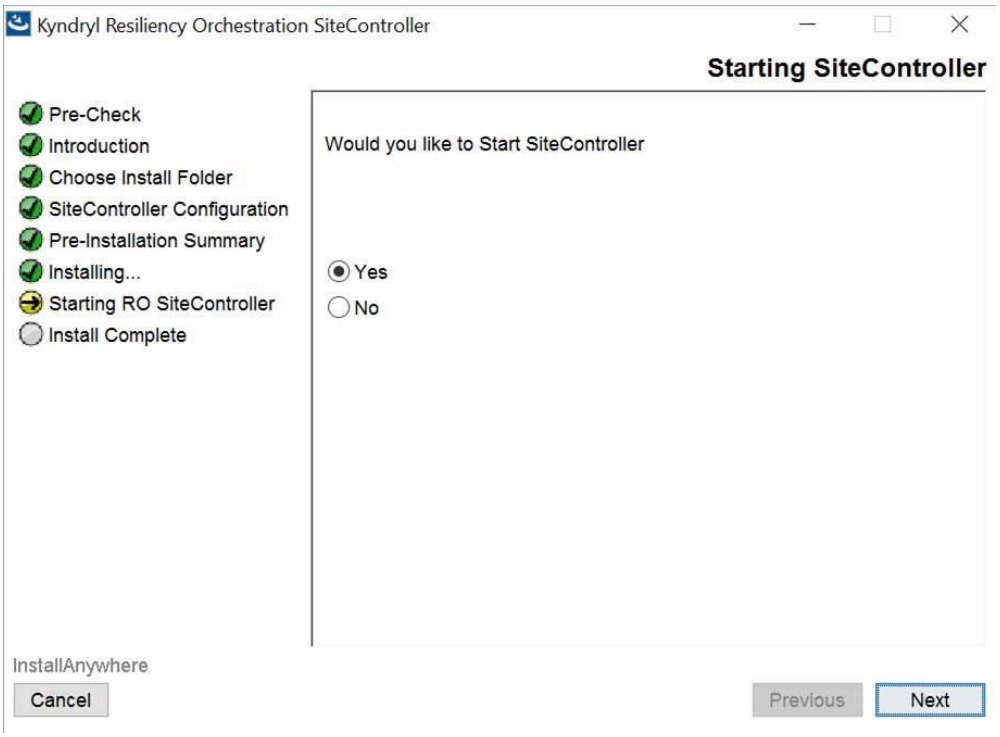


Figure 46: Kyndryl Resiliency Orchestration Site Controller Installation on Windows - Starting Kyndryl Resiliency Orchestration Site Controller

159. On the **Starting Kyndryl Resiliency Orchestration Agents Node** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

> **Note**
>
> There are some post-installation steps so, choose No.

160. Click **Next**. The **Installation Completed** window is displayed indicating successful installation.

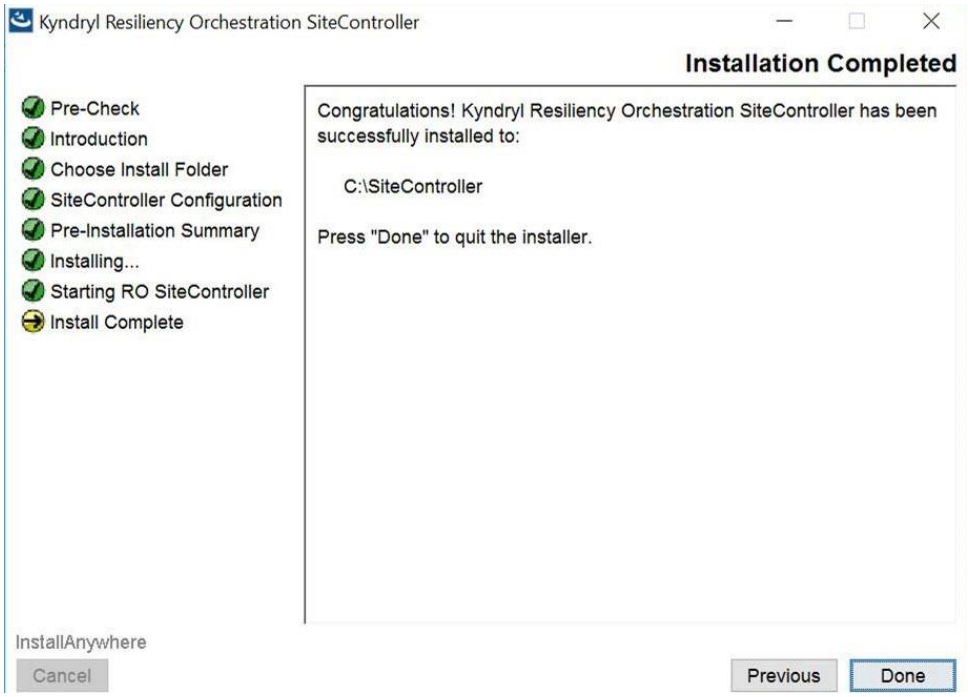


Figure 47: Kyndryl Resiliency Orchestration Site Controller Installation on Windows - Installation Completed

161. Click **Done** to complete the installation process.

> **Note**
>
> When the installation is carried on silent mode or GUI mode, restart with a Putty session.

162. Proceed to the post-installation procedure. For instructions, see the *Post-installation steps after you install the Site Controller in Windows*.

10.7 Installing Site Controller in Windows in Silent Mode

In the silent mode installation method, the installation program reads the settings for your configuration from the properties file before installation. The installation program does not display any configuration options during the installation process.

The following sections describe how to install the Site Controller server using the installation program in silent mode on Linux platforms. It is assumed that the user has acquired the installation program and properties file from the FTP server.

> **Note**

Confirm that the hardware and software configuration required for Site Controller installation is in place.

10.7.1 Editing Properties File

When installing Site Controller in silent mode, the installation program uses the **properties** file for the server (PanacesAgentNodeInstaller.properties) to determine which installation options are to be implemented. You need to edit the respective properties file to specify the installation options that you want to invoke while performing the Agent's installation after which, you can run the installation program in silent mode.

Perform the following steps to edit the properties files.

1. Get the files from the FIX Central server/ Passport Advantage and copy properties files by running the following command:

```
cp AgentNode/PanacesAgentNodeInstaller.properties /tmp

cp AgentNode/SiteController.exe  /tmp
```

163. Open the properties file by using the following command:

```
vi /tmp/ PanacesAgentNodeInstaller.properties
```

Modify the respective properties file for the keywords shown in the following tables, to reflect your configuration.

`PanacesAgentNodeInstaller.properties` file:

Table 22: Keywords in PanacesAgentNodeInstallaer.properties File

Keyword	Description
INSTALLER_UI	Displays the mode of installation as "silent".
MODIFY_SYSTEM_FILES=1	Setting this property to 1 modifies the following system files: /etc/hosts,/etc/sysconfig/selinux, /etc/sysctl.conf Refer link MODIFY_SYSTEM_FILESfor details.
USER_INSTALL_DIR	Enter the path for the directory to install the Site Controller Server software (default path is /opt/panaceas/)

Keyword	Description
USER_INPUT_RESULT_PRIMARY_PANACES_SERVER	Enter the IP address/Name of the primary server.
USER_INPUT_RESULT_SECONDARY_PANACES_SERVER	Enter the IP address/Name of the secondary server.
PANACES_AGENT_NODE_ADDRESS	Enter the IP address/Name of the Local machine.
AGENTNODE_START_YES	Enter 1 if you want to start the agents automatically after the installation. Enter 0 if you want to start the agent manually. Set this property to manual as there are some post-installation steps.

165. Proceed to the Post-installation procedure. For instructions, see the *Post-installation steps after you install the Site Controller in Windows*.

10.8 Post-installation Steps after you install the Site Controller in Windows

1. In the Site Controller installation folder, perform the following steps:
   a. Go to the location: $EAMSROOT/installconfig/ where $EAMSROOT is the location where the Site Controller is installed.
   b. Open the SiteController.cfg file
   c. Add the following property:

   ```
   MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE=50
   ```

Note:

Determine the number of agents that will connect to the site controller. Set `MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE` to 1.5 times the number of agents.

For example, for 100 agents set `MAX_SC_CONNECTION_REQUEST_HANDLING_SIZE` to 150.

166. Enter the value of the ACP keystore in the \installconfig\SiteController.cfg file.

For Example: `panaces.acp.keystore=`

kyndryl

> **Note**
>
> The value of the ACP keystore will be the path where the ACP key store exists, which means <Site controller installation folder>\installconfig\keystore\panacesACP.keystore. Enter the path with a \\ for file separator, for example, c:\\Sitecontroller\\installconfig\\keystore\\panacesACP.keystore

167. Enter the path of the truststore in the same SiteController.cfg file.

For Example: `panaces.acp.truststore=`

> **Note**
>
> - This value of the ACP truststore will be the path where the ACP trust store exists, for example <Site controller installation folder>\installconfig\keystore\ panacesACP.truststore. Enter the path with a \\ for file separator, for example, c:\\Sitecontroller\\installconfig\\keystore\\ panacesACP.truststore
> - Ensure that you create your truststore and keystore and use them as the corresponding values for the truststore and keystore.

168. Post installation, the site controller should start automatically. In case it does not start, perform the following steps.

    a. Check for special characters similar to "~ //RS" under the service property "**Path to executable.**"

    b. Delete the first character and update it to "//RS" in the registry by following the below steps.

        i. Open registry editor.

        ii. Edit --> find --> "KyndrylROActiveMQ" and "KyndrylROWindowsOSAgent_"

        iii. Find the imagepath subkey and click on modify.

        iv. Update the special character to "//RS" in the data value.

    c. Enable the KyndrylROSiteController service, by following the below steps.

        i. Goto <install location>sitecontroller/bin.

        ii. Run SiteController.bat and start on the command prompt.

        iii. Open registry editor.

        iv. Edit --> find --> "KyndrylROSiteController"

v. Find the imagepath subkey and click on modify.

vi. Update the special character to "//RS" in the data value.

vii. Post update of imagepath data value, start the KyndrylROSiteController service by right-clicking and selecting the **Start** menu item.

d. Start KyndrylROWindowsOSAgent services by right-clicking and selecting the Start menu item.

169. For Oracle solutions using remote agent model - Post-Windows SiteController installation, the installer will install the sqlplus but some of the .dll files will be missing. The user needs to install the Microsoft visual c++ distributable package 2015 based on the OS bits and connect to sqlplus. Refer to https://www.microsoft.com/en-in/download/details.aspx?id=48145.

170. When the Site Controller has a NAT IP, and post-installation the Site Controller is in an 'Unknown' state, follow the below steps –

i. Stop the Site Controller services and the Agents running on the Site Controller.

ii. Update the configurations in `$EAMSROOT/installconfig/SiteController.cfg` file in the below listed properties -

PANACES_MASTER_SERVER_ADDRESS=<PRIMARY_RO_IP>
PANACES_SLAVE_SERVER_ADDRESS=<STANDBY_RO_IP>
PANACES_SITE_CONTROLLER_ADDRESS=<NAT_IP>
PANACES_SITE_CONTROLLER_BIND_ADDRESS=0.0.0.0

iii. Update the configurations in `$EAMSROOT/installconfig/PanacesAgentGeneric.cfg` file in the below listed properties -

PANACES_MASTER_SERVER_ADDRESS=<PRIMARY_RO_IP>
PANACES_SLAVE_SERVER_ADDRESS=<STANDBY_RO_IP>
PANACES_AGENT_NODE_ADDRESS=<NAT_IP>
PANACES_AGENT_NODE_BIND_ADDRESS=<PRIVATE/LOCAL_IP>
PANACES_SITE_CONTROLLER_ADDRESS=<NAT_IP>
PANACES_SITE_CONTROLLER_NATIP_ADDRESS=<PRIVATE/LOCAL_IP>

iv. Start the Site Controller services and Agents running on Site Controller.

10.8.1 Post Validation Steps During Server Startup in Windows

A. Follow the post validation steps during server startup while performing the procedure "Post-installation Steps after you install the Site Controller in Windows".

1. Navigate to *the* **PanacesAgentGeneric.cfg** file under the `$EAMSROOT/installconfig` folder.
2. Execute the following command:

   ```
   ps -ef | grep <Give AIX IP address>
   ```

3. Locate the PID from the output generated in step 2 and execute the following command:

   ```
   kill -9 <AIX agent PID>
   ```

4. Execute the following script under the **$EAMSROOT/bin** folder.

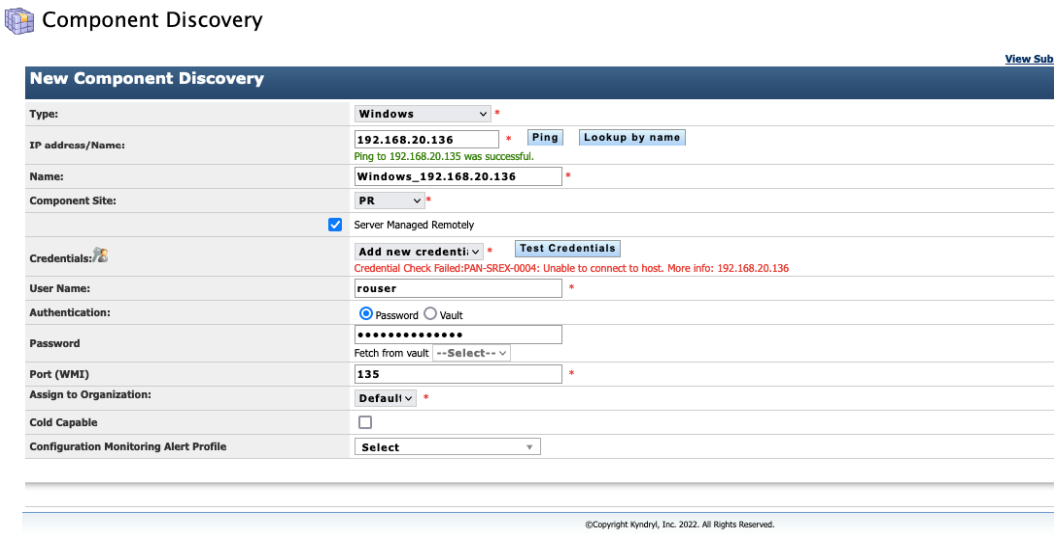
   ```
   SecurityUserInjection.sh script
   ```

5. Restart the panaces service.
6. Navigate to the **Subsystem Discovery Page** in GUI and modify the AgentNode component from hostname to IPaddress.
7. After modifying the Agent node from hostname to IP address, start the AIX agents from GUI.

B. Windows machine Connection/ Test Credential issue on RO server

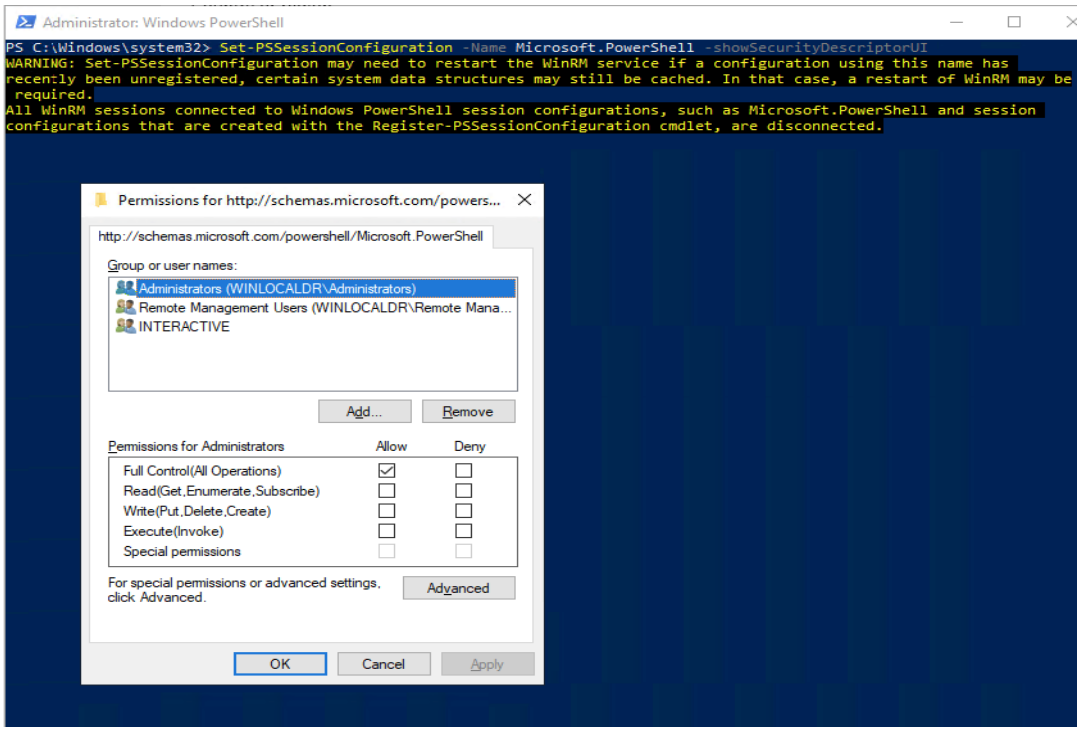
Troubleshooting steps:

If the user hits the issue of component test credential failure for username other than administrator as shown in the pic below. Example: rouser



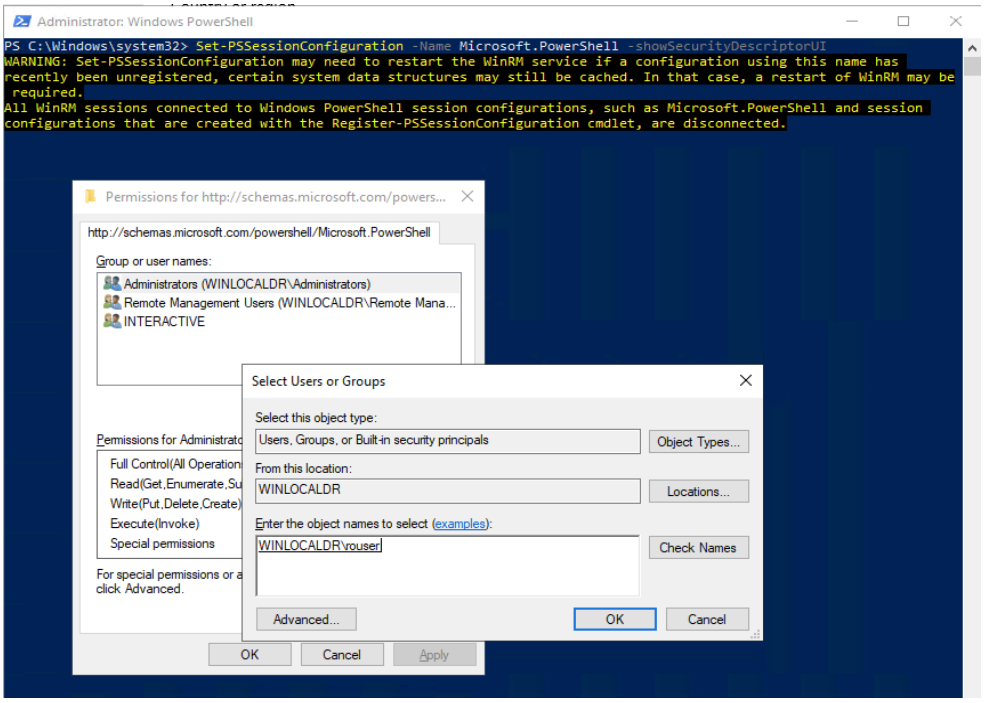
Go to the endpoint and run Windows PowerShell as Administrator. Execute below command in power shell to provide execute invoke permission for the username.

Set-PSSessionConfiguration -Name Microsoft.PowerShell -showSecurityDescriptorUI

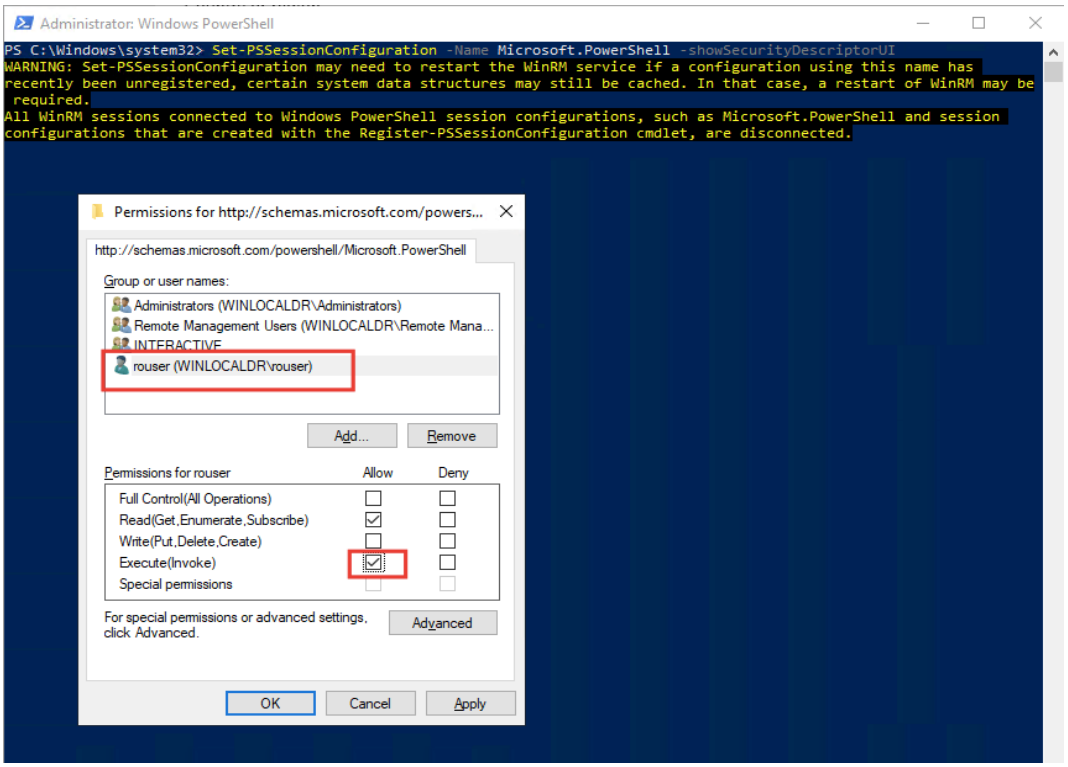


When the Permission window opens, add the username for which test credential is failing.

Example: rouser

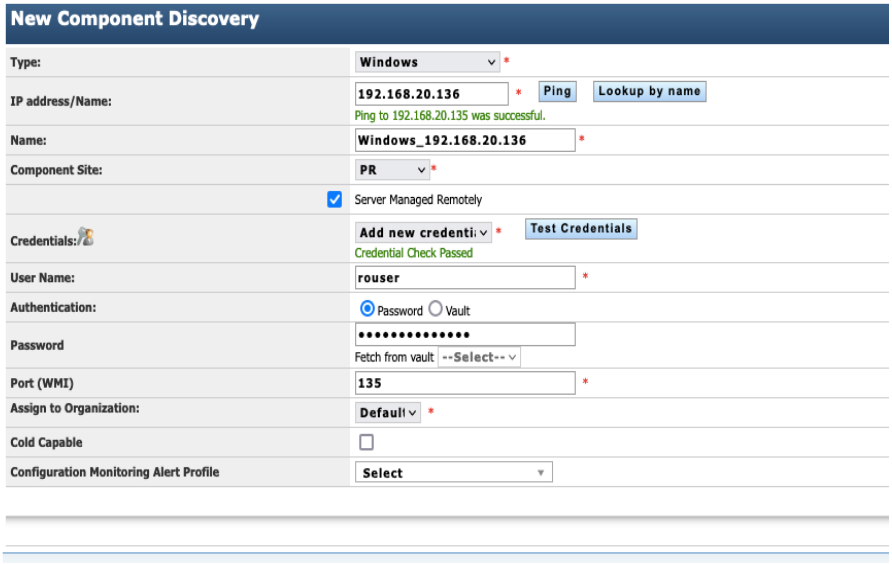


Give the Execute (Invoke) permission to the user. Click on the checkbox and save.



Now check the test credentials for component on RO server, it should pass.

Component Discovery



kyndryl

10.8.2 Dependency for RBR Solution deployment:

1) If there are no windows VMs to be protected, there is no need for Windows SC.
2) If there are Windows VMs involved, then Windows SC needs to be deployed. As deployment optimization, this can be deployed on the same Windows Server where DMC is deployed.

10.9 Starting or Stopping Site Controller Manually

Users can start, stop, or view the status of the Site Controller manually by using the following methods:

- Windows Command Prompt
- Windows GUI

10.9.2 Using the Windows Command Prompt

You can start, stop, or view the status of the Site Controller by using the Windows Command Prompt.

10.9.2.1 Starting the Site Controller by using Windows Command Prompt

Perform the following steps to Start the Site Controller:

1. Log in to the Site Controller Server.

171. Enter in the `$EAMSROOT/bin` folder.

172. To Start the Site Controller, run the following commands:

```
$EAMSROOT/bin>ActiveMQ.bat start

$EAMSROOT/bin>SiteController.bat start

$EAMSROOT/bin>WindowsOSAgent.bat start
```

10.9.2.2 Stopping the Site Controller by using Windows Command Prompt

Perform the following steps to Stop the Site Controller:

1. Log in to the Site Controller Server.
2. Enter in the `$EAMSROOT/bin` folder.
3. To stop the Site Controller, run the following commands:

```
$EAMSROOT/bin>WindowsOSAgent.bat stop

$EAMSROOT/bin>SiteController.bat stop

$EAMSROOT/bin>ActiveMQ.bat stop
```

kyndryl

10.9.2.3 Viewing the Status of the Site Controller by using Windows Command Prompt

Perform the following steps to View the Status of the Site Controller:

1. Log in to the Site Controller Server.

173. Enter in the `$EAMSROOT/bin` folder

174. To start the Site Controller, run the following commands:

```
$EAMSROOT/bin>SiteController.bat status

$EAMSROOT/bin>ActiveMQ.bat status

$EAMSROOT/bin>WindowsOSAgent.bat status
```

10.9.3 Using the Windows GUI

You can start or stop the Site Controller by using the Windows GUI.

10.9.3.1 Starting the Site Controller by using the GUI

Complete the following steps to Start the Site Controller:

1. Click **Start** from Windows Task Bar

175. Click **Run**, and then, enter Services.msc in the **Search** Bar.

176. Press **Enter**.

177. Look for the service **Kyndryl Resiliency Orchestration ActiveMQ** and select it. Right-click to see the options, navigate, and then, click **Start**.

178. Look for the service **Kyndryl Resiliency Orchestration SiteController** and select it. Right-click to see the options, navigate, and then, click **Start**.

179. Look for the service **Kyndryl Resiliency Orchestration WindowsOSAgent** and select it. Right-click to see the options, navigate, and then, click **Start**.

10.9.3.2 Stopping the Site Controller by using the GUI

Complete the following steps to Stop the Site Controller:

1. Click **Start** from Windows Task Bar

180. Click **Run**, and then, enter Services.msc in the **Search** Bar.

181. Press **Enter**.

182. Look for the service **Kyndryl Resiliency Orchestration WindowsOSAgent** and select it. Right-click to see the options, navigate, and then, click **Stop**.

183. Look for the service **Kyndryl Resiliency Orchestration SiteController** and select it. Right-click to see the options, navigate, and then, click **Stop**.

184. Look for the service **Kyndryl Resiliency Orchestration ActiveMQ** and select it. Right-click to see the options, navigate, and then, click **Stop**.

10.10 Configuring End Points and Site Controller to use the PowerShell framework

Ensure to complete the following steps to enable the PowerShell framework, on all the systems that have the Agents installed and on the systems that function as the Windows End Points (PR, DR, and Site Controller).

1. Select **Start** in the Windows system and then enter **PowerShell**.

185. From the listed programs, navigate to **Windows PowerShell,** right-click, and then select **Run as administrator**.

186. In the Windows PowerShell command prompt, enter the following commands:

```
Enable-PSRemoting –Force

Set-Item wsman:\localhost\client\trustedhosts *

Restart-Service WinRM
```

187. Execute the following command on the SC to make .ps1 script to work

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```

10.11 Uninstalling Site Controller

This section describes the procedure to uninstall the Site Controller in GUI mode and Silent mode.

10.11.2 Uninstalling Site Controller in GUI Mode

Perform the following steps to uninstall Site Controller in GUI mode:

1. Navigate to the location: $EAMSROOT\Bin and click **UninstallerSiteController.bat**
2. Navigate to the location: `$EAMSROOT\UninstallerData`
3. Select **Uninstall Kyndryl Resiliency Orchestration SiteController.exe**, right-click, and then, click **Run as administrator**.
4. The **Uninstall Kyndryl Resiliency Orchestration Agent Node** window displays, as shown in the following figure:

188. Click **Uninstall**.

189. The uninstallation process begins. When the process is complete, the **Uninstall Complete** window is displayed.

190. Click **Done** to close this window.

10.11.3 Uninstalling Site Controller in Silent Mode

Perform the following steps to uninstall Site Controller in silent mode:

1. From the command prompt, go to the location: $EAMSROOT\Bin
2. Run the **UninstallerSiteController.bat** file
3. Run the following command to uninstall the Site Controller.

```
$EAMSROOT\UninstallerData>Uninstall IBM Resiliency Orchestration
SiteController.exe
```

10.12 Upgrading Site Controller

Perform the following steps to upgrade the Site Controller.

1. Download the latest version of Site Controller binaries from Passport Advantage/ Fix Central.

10.13 Monitoring health of Windows Site Controller

The windows scripts will be found at $EAMSROOT/tools/monitoring/sitecontroller/windows

Please find below script names for windows,

delete_logs.ps1, GCClassStats.ps1, SCpidstat.ps1,

SCResourcesStats.ps1, ThreadDump.ps1

```
### Task Scheduler

 1. Open Task Scheduler
 2. Click on Create a new task and Name it.
 3. Check Run only when the user is logged in for the first time (if checked
this will execute the script interactively if already tested then select Run
whether the user is logged in or not)
 4. Go to the Triggers tab click new and select daily: recur 1 day. Check
Repeat tasks every and select occurrence as per requirement. Click Ok.
 5. Go to action tab->new->Action: Start a program.
```

```
   Program/Script: Powershell.exe
   Add arguments: -ExecutionPolicy Bypass "path to your script"
6. Save the schedule and run it.
```

10.14 Known Limitations

- One Site Controller can manage up to 625 end points. This has been verified with a maximum of 25 uni-agents running for a given Windows Site Controller (regardless of the processors or memory).

kyndryl

11 Uninstall the existing version of the Site Controller. To uninstall the Site Controller, refer to Uninstalling Site Controller

12 Install the latest version of Site Controller in GUI mode or Silent mode. To install in GUI mode, Installing Site Controller in GUI Mode in Windows

To install in Silent mode, refer to Installing Site Controller in Windows in Silent Mode.

12.1 NAT IP support

If you need to support the site controller for NATed IP endpoints, the below changes need to be performed in the site controller.

1. Navigate to the site controller file SiteController.cfg located at $SiteContorllerInstallationLocation/installconfig/SiteController.cfg file: and edit the **PANACES_SITE_CONTROLLER_ADDRESS** with NAT ip address as shown in the example below.

   Example:

   ```
   PANACES_MASTER_SERVER_ADDRESS=<MASTER_RO_IP>
   PANACES_SLAVE_SERVER_ADDRESS=<SLAVE_RO_IP>
   PANACES_SITE_CONTROLLER_ADDRESS=<NAT_IP>
   PANACES_SITE_CONTROLLER_BIND_ADDRESS=<IP>
   ```

2. Navigate to the site controller file PanacesAgentGeneric.cfg located at $SiteContorllerInstallationLocation/installconfig/PanacesAgentGeneric.cfg file: and edit the PANACES_AGENT_NODE_ADDRESS with NAT ip address as shown in the example below.

   Example:

   ```
   PANACES_MASTER_SERVER_ADDRESS=<MASTER_RO_IP>
   PANACES_SLAVE_SERVER_ADDRESS=<SLAVE_RO_IP>
   PANACES_AGENT_NODE_ADDRESS=<NAT_IP>
   PANACES_AGENT_NODE_BIND_ADDRESS=<PRIVATE/LOCAL_IP>
   PANACES_SITE_CONTROLLER_ADDRESS=<NAT_IP>
   PANACES_SITE_CONTROLLER_NATIP_ADDRESS=<PRIVATE/LOCAL_IP>
   ```

kyndryl

13 Installing Agents on MS Windows Server

The agent software is bundled into multiple installation packages which are available at the Kyndryl Passport Advantage site. It contains all the binaries and packages to run the Kyndryl Resiliency Orchestration agent software.

Note

- MS Windows OS Agent is automatically installed during the installation of agents.
- Kyndryl Resiliency File Replicator is automatically installed during the installation of the Kyndryl Resiliency File Replicator Agent.

13.1 Prerequisites for Installing Resiliency Orchestration Agents

The Kyndryl Resiliency Orchestration Agent Software packages are available for each supported application, protection software, and operating system. These agents are installed on the servers involved in the Disaster Recovery solution. The installer installs the Kyndryl Resiliency Orchestration Agent Platform package, required for the agent software installation, on the same server and is done automatically during agent installation. Ensure that you have local system administrative privilege during the installation.

For the installer to install the Kyndryl Resiliency Orchestration Agent Platform package on MS Windows successfully, the following prerequisites must be fulfilled.

Note

- A single bundle with all agents in one binary to be downloaded from CRO 8.4.0 onwards.

13.2 MS Windows Server Requirements

The server participating in the DR infrastructure needs to incorporate the following requirements:

a. **Hardware / Software Requirements:** The following are the Windows Server Hardware / Software requirements:
   - The server must have a minimum of 2 GB RAM.
   - C drive should have an additional 10GB disk size for Agent Software

b. **Logs Directory:** There must be enough disk space allocated on the server to hold MSSQL transaction logs for up to 5 business days. Take the assistance of the consultant to create the directory size appropriately. This directory can reside on either direct attached storage or external attached storage.

For Example: Assume that a log of 2MB is generated every 10 minutes. Then, this will require 2MB/log * 6logs/hour * 24 hr/day * 5 days =☐ 1.5GB of log device size.

The replication of database dump from the primary server to the remote server and vice versa may be done manually either on tapes, or any other backup device. It is assumed that the server is configured with appropriate backup software to do the same. If the database dump size is small, the replication may be performed on WAN/LAN itself. In this case, backup software is not required.

If required, reboot the server after completing the following operations:

13.3 Installation of supported JRE

For information on the supported JRE, refer to *GPL dependent binaries* for Kyndryl Resiliency Orchestration in the Prerequisites topic.

For more information about the GPL licenses, see *GPL License Information*

13.4 Host Machines with Virtual IP Address

If there is a virtual IP address for the host, or if the host is part of an OS Cluster, add the entry `PANACES_AGENT_NODE_ADDRESS=<IP Address of the Node>` in `$EAMSROOT\installconfig\PanacesAgentGeneric.cfg`. Using this entry, Kyndryl Resiliency Orchestration Server will always communicate to all agents on this IP address. This could be the Virtual IP or the original IP assigned to the interface.

13.5 Specific Prerequisites

The following are the prerequisites for specific agents; ensure that these prerequisites are met before starting the agents' installation.

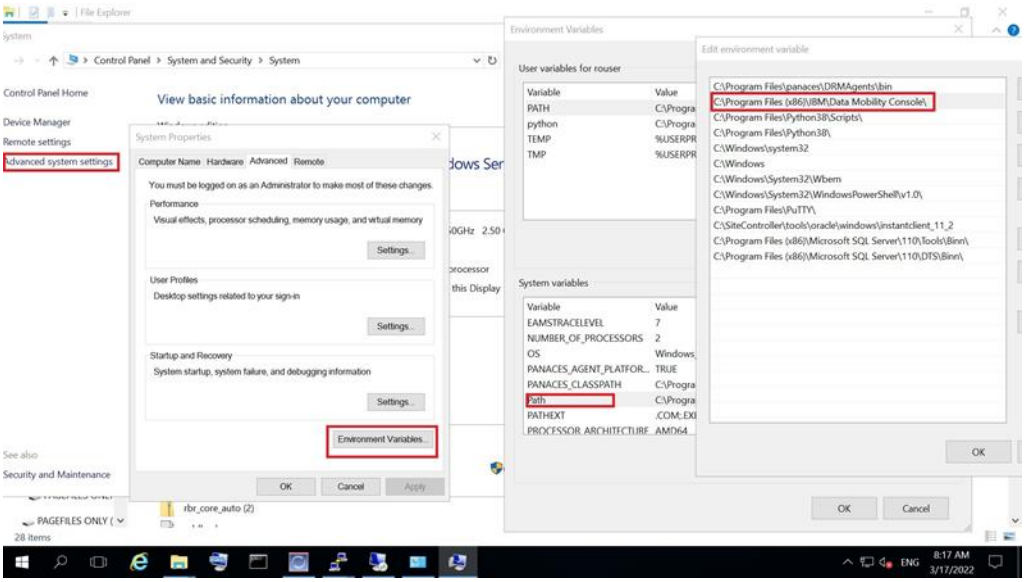
13.5.1 MSSQL Agent

Download the MSSQL JDBC driver MSSQL Jar file and save it locally to be used at the time of MS SQL local agent installation.

13.5.2 Blockreplicator Agent

For the blockreplicator agent,

- DMC should be installed
- And DMC path should be specified during installation when prompted.
- **The user has to set the dmc.exe path in the system environment variable and restart the dmc**



13.5.3 Oracle Agent

Refer to the following path to download the .jar files:

%ORACLE_ HOME%/jdbc/lib/ojdbc8.jar

%ORACLE_ HOME%/jdbc/lib/orai18n.jar

It is recommended to refer to the

Download the following JDBC jar files for Oracle Agents and place them in the %ORACLE_ HOME%\jdbc\lib directory:

- nls_charset12.jar
- ojdbc14.jar
- **Oracle DG Agent**

Download the following JDBC jar files for Oracle Agents and place them in the %ORACLE_ HOME%\jdbc\lib directory:

- nls_charset12.jar
- ojdbc14.jar

Note

If there are some agents already installed and the user tries to install additional agents, the installer will not continue with the installation. Install the additional agents in a different location.

***Important*:**

As a part of every agent installation, the OS agent will be installed automatically without any user input. During the installation process, there will be an option to start the installed agents automatically. These additional agents should not be started automatically from the installer option since the installer will start the new OS agent also. After the installation is completed, the additional agent can be started from the services panel.

13.6 Installation of Agents

This section outlines the steps to install all agents on Windows Server. Additional steps that you must perform for specific agents are also included.

Note

You must have administrator, root, or equivalent privileges to install Kyndryl Resiliency Orchestration Agents.

To install the agents, perform the following steps:

1. Download the Agent Installer executable files from the Kyndryl Passport Advantage site.

191. Files are available in the zipped format in the **Agents folder.** Extract Files from **WindowsDRMAgents.zip** for 32-bit Windows Operating Systems and **Windows64DRMAgents.zip** for 64-bit Windows Operating Systems.

192. Go to the extracted folder and double-click the **install.exe** file. The following are the limitations for installing Kyndryl Resiliency Orchestration Agents on Windows:

- Services can only be registered and started by users having local administrator privileges on the physical target machine, and not remotely.
- If Services have to be registered and started from remote machines, such as Terminal Server, then the user must be an Administrator having necessary privileges to the registry and Agents\Windows\System32 directories.
- Make sure that you have free space of approximately 2.5 GB in /tmp directory, before installation.
- Cloud-based RO supports only Private IP for communication with SC and DMC.

kyndryl

Note - In case the antivirus does not permit the agent software installation, add an exclusion in the antivirus for the agent installer. Ensure that the two-way communication between the agent and Kyndryl Resiliency Orchestration is enabled post the installation of the agent.

After executing the file, the Kyndryl Resiliency Orchestration Agent installation starts with the following screen.

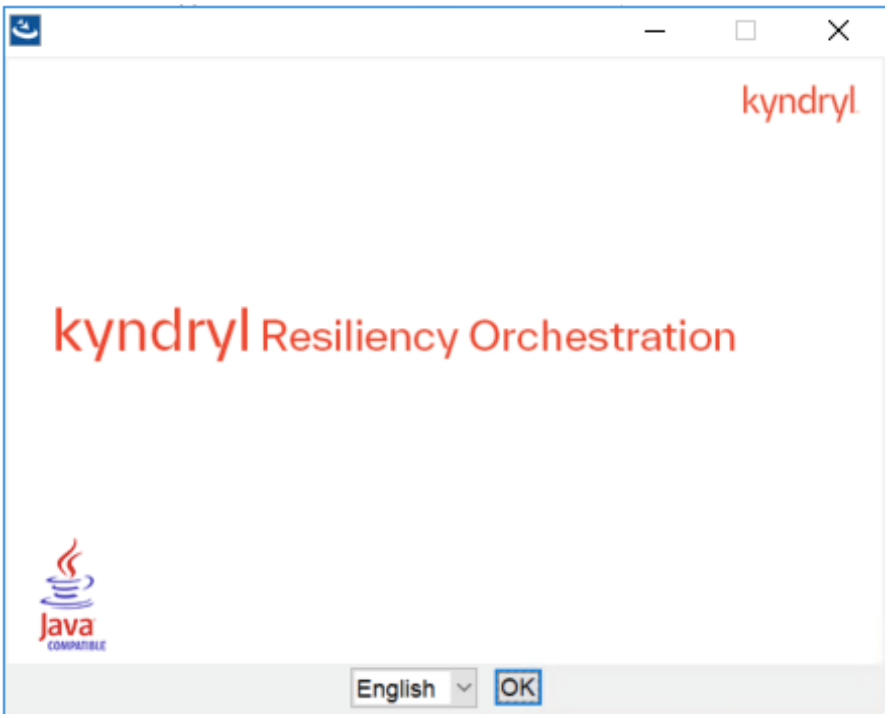


Figure 48: Kyndryl Resiliency Orchestration Agent Installer

After displaying the Kyndryl Resiliency Orchestration Agent Installer screen, the Introduction window is displayed.

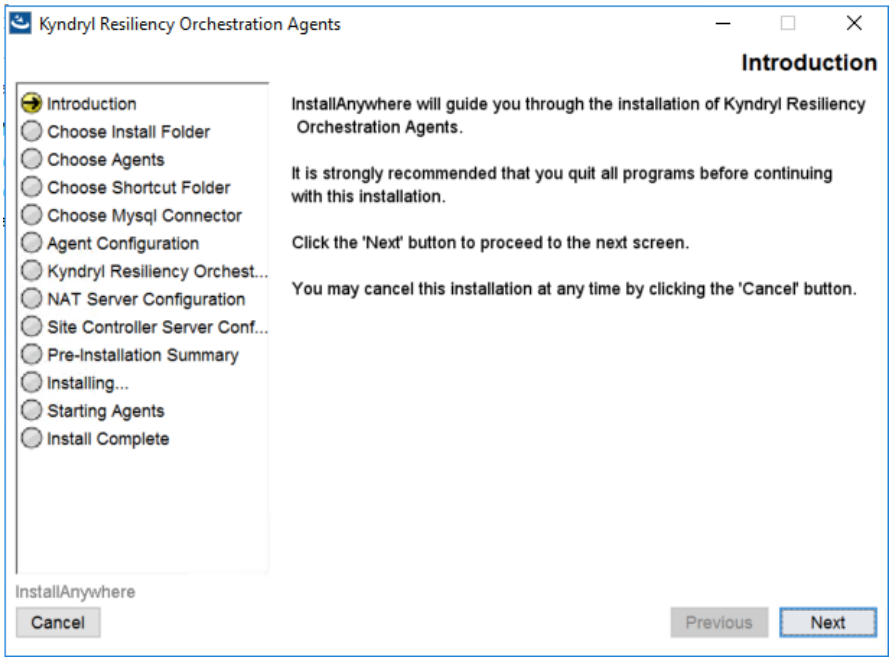


Figure 49: Kyndryl Resiliency Orchestration Agents Installation on Windows Server - Introduction

193. Go through the installation procedure and click **Next**. The **Choose Install Folder** window is displayed.

194. Select a path to install the software by clicking **Choose.** Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is **C:\Program Files\panaces**. It is recommended that you use the default path displayed.

195. Click **Next**. The **Choose Agents - Windows** window is displayed.

The list of agents available is displayed on the **Choose Agents - Windows** window.

196. Select the checkbox next to the specific agent to install that agent. You can choose to install any or all of the agents.

197. Click **Next**. The **Choose Shortcut Folder** window is displayed.

198. Select an option to create a product icon in the required location. For example, select the **Other** option button to create a product icon in a specific path, or select the **Don't create icons** button to avoid creating shortcut folders.

kyndryl

> **Note:**
>
> During installation, if In a new Program Group option is selected and no name is given for the program group, the option will be ignored and shortcuts will not be created. Please make sure that the selected path has all the JDBC driver jar files.

199. Click **Next.**

Note: In case you had selected **Generic Agent** as the agent, then you will be prompted with the Generic Agent Configuration window as shown in. Agent configuration is different for different selected agents.

200. Depending on the agent you have selected for installation, perform the steps for the Generic Agent:

For RBR (Agent-based):

I. In the DMC server, during CRO local agent installation, "Generic Agent" only has to be selected. The generic agent

will ask for two key values as below that needs to be provided.

Generic Agent Object Type : BLOCKREPLICATOR-V2

Generic Agent Object Class : MANAGEMENT_SERVICE

II. The value given above goes into "PanacesAgentGeneric.cfg" file as below in entries

GENERIC_AGENT_OBJ_TYPE=BLOCKREPLICATOR-V2

GENERIC_AGENT_OBJ_CLASS=MANAGEMENT_SERVICE

III. With the selection of a generic agent, two Windows services will be plugged in as below.

For RBR (Agentless):

I. In the CRO portal, the management service needs to be discovered with a type of "Block Replicator"
   a. for the agentless model.

II. In the DMC server, during CRO local agent installation, "BlockReplicator agent" only has to be selected.

III. With a selection of BlockReplicator agents, only one Windows service "Panaces Agent For BlockReplicator" will be plugged in.

Note: The "Panaces Agent for MS Windows OS" will NOT get deployed.

201. Enter the IP addresses/Name of the primary and secondary Kyndryl Resiliency Orchestration servers and Kyndryl Resiliency Orchestration Site Controller Address. In a non-NAT environment, the NAT IP address should be left blank.

202. In a NAT environment, enter the primary and secondary Resiliency Orchestration Server's public IP. Resiliency Orchestration Site Controller address should be the public IP and the NAT IP address should be the private IP of the server where you are installing.

203. Click **Next.** Enter Site Controller IP Address/Name if required.

204. Click **Next**. The Pre-Installation Summary window is displayed.

205. Go through the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify.

206. Click **Install.** The Installing Kyndryl Resiliency Orchestration Agents window is displayed.

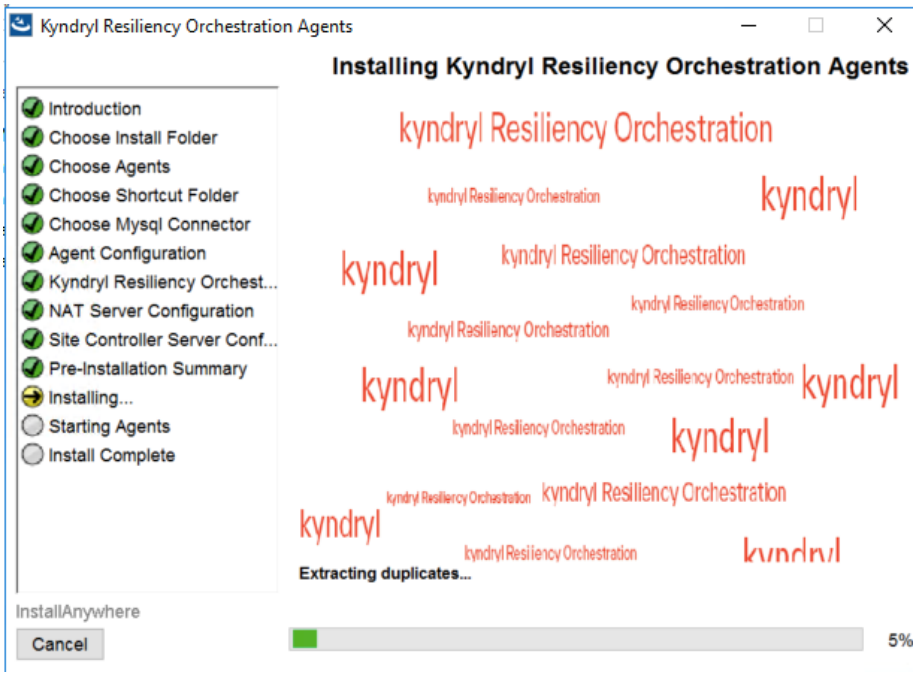
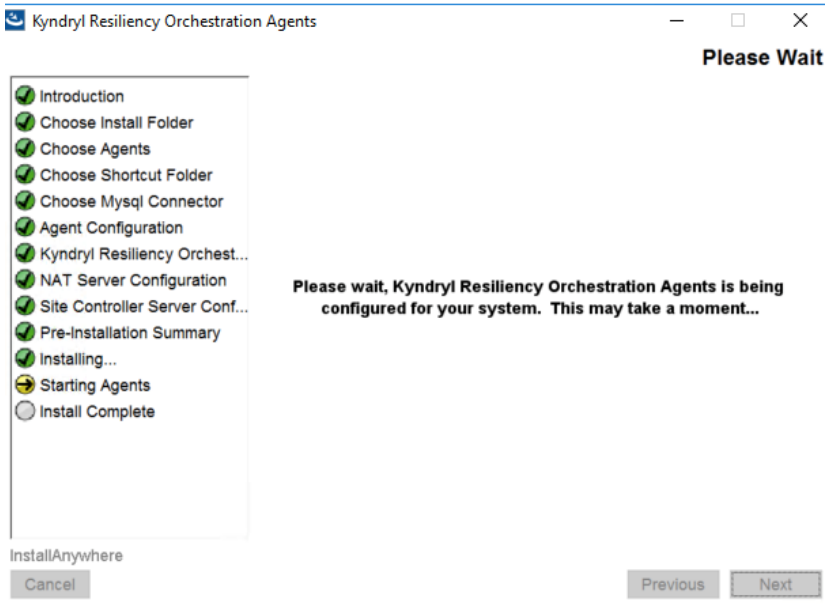


Figure 50: Kyndryl Resiliency Orchestration Agents Installation on Windows Server - Installing Kyndryl Resiliency Orchestration Agents

Once the installation is complete, the **Starting Agents** window is displayed.



207. On the **Starting Agents** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

> **Note**
>
> The best practice is not to change the default value displayed on the Starting Agents window.

208. Restart the agent machine, if the agents do not start after agent installation is complete.

When the installation is carried on silent mode or GUI mode, restart with a Remote Desktop session for Windows.

209. Click **Next**. The **Install Complete** window is displayed, indicating a successful installation.

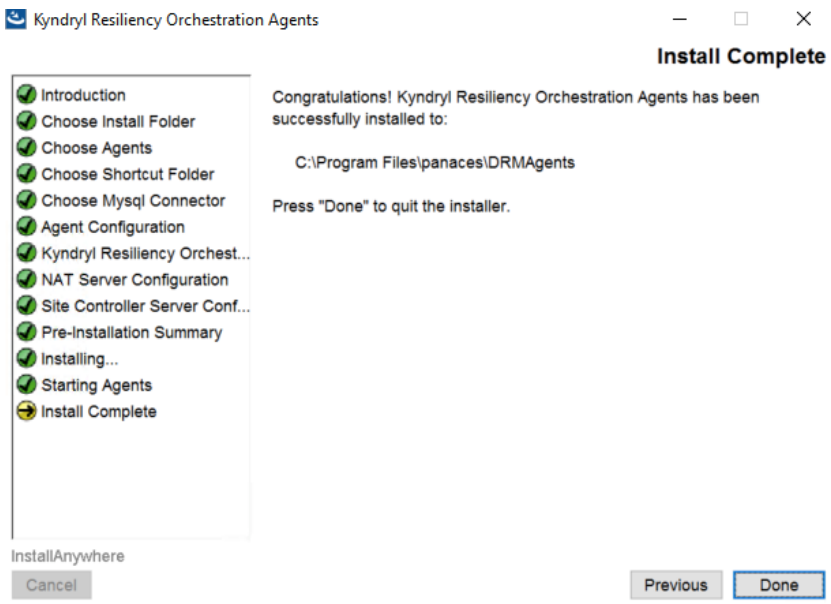


Figure 51: Kyndryl Resiliency Orchestration Agents Installation on Windows Server - Install Complete

210. Click **Done** to complete the installation process.

211. Download GPL-dependent binaries for Windows OS Agent as mentioned in the table below.

For more information about the GPL licenses, see *GPL License Information*

Table 23: GPL Dependent Binaries for Windows OS Agent

Windows -32 BIT
installedlocation/bin/cyggcc_s-1.dll
installedlocation/bin/cygiconv-2.dll
installedlocation/bin/cygintl-8.dll
installedlocation/bin/cygwin1.dll
Windows-64-BIT
installedlocation/bin/cyggcc_s-1.dll
installedlocation/bin/cygiconv-2.dll

installedlocation/bin/cygintl-8.dll
installedlocation/bin/cygwin1.dll

Once the installation is complete, verify the individual agent service installation manually, by clicking the **Services** icon on the **Administrative tools** group in **Control Panel**.

kyndryl

Note:

- For the MS Exchange solution, Remote Agent installation is also supported. Perform the following:
- The remote agent is supported, however, while the agent process runs on Agent Node (Resiliency Orchestration Server), the Kyndryl Resiliency Orchestration MS Exchange Extensions (powershell extensions) need to be deployed on the client servers. To install the extensions, the user has to install the MS Exchange agent (local agent kit). During installation, do not start any agents, or after installation disable the installed agent services (from the service list).

213. Note that there will be no separate installer to install extensions as the number of installations is always going to be very few (only one or two). Hence, we will reuse the agent installer itself to deploy local agents as well as Extensions for remote agents.

214. The traditional remote agent model where everything is deployed and executed on the agent node (or Resiliency Orchestration Server) is not supported due to security restrictions by MS Domain Management and PowerShell.

215. Have to import replication workflow from $EAMSROOT/workflows/MSExch/MSExchReplicationInfo_Remote.xml

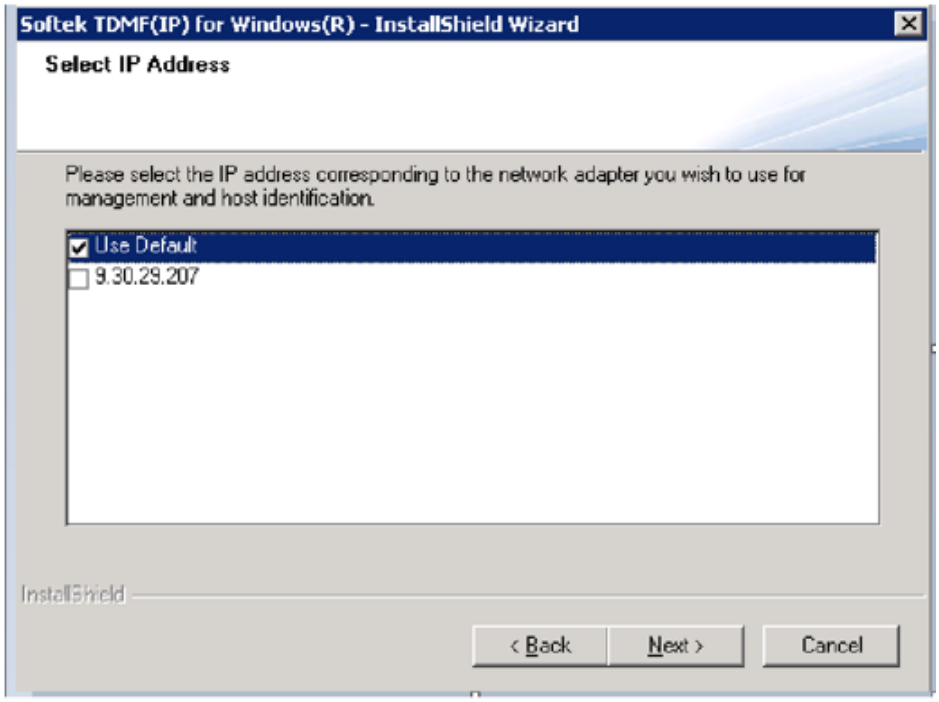
216. When the installation is carried on silent mode or GUI mode, restart with a Remote Desktop session for Windows.

13.7 Installing TDMF (GUI)

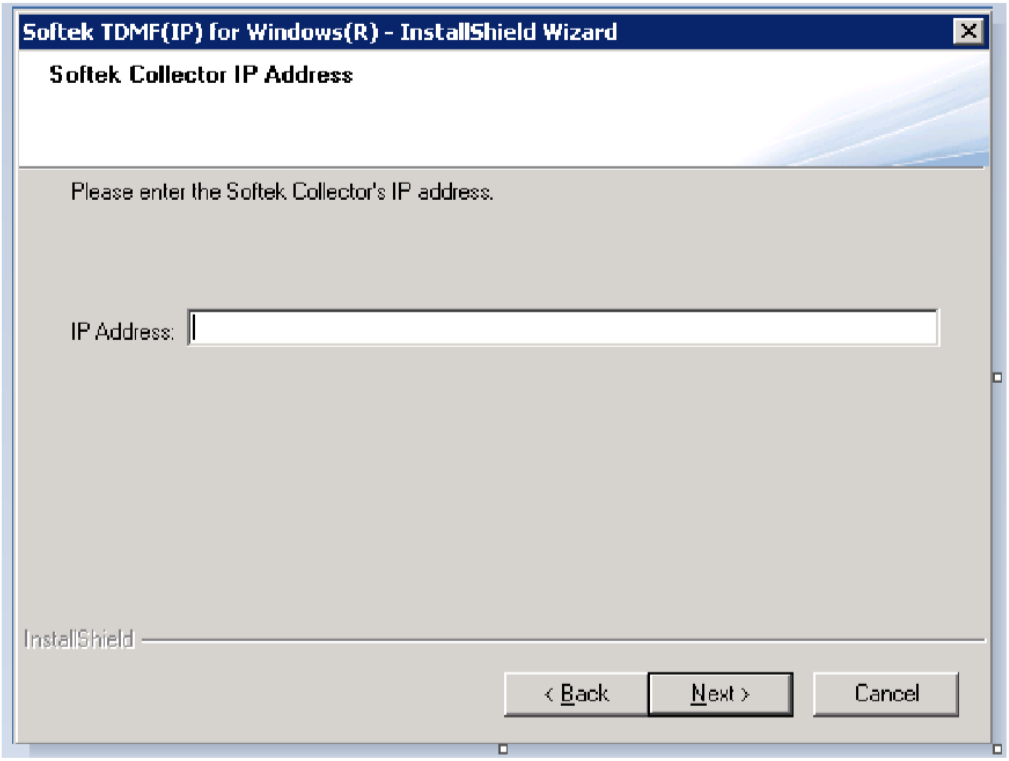
1. Launch the TDMF install shield.

217. On the welcome screen, click the **Next** button to continue.

218. On the select IP address screen, select the desired IP and click next.

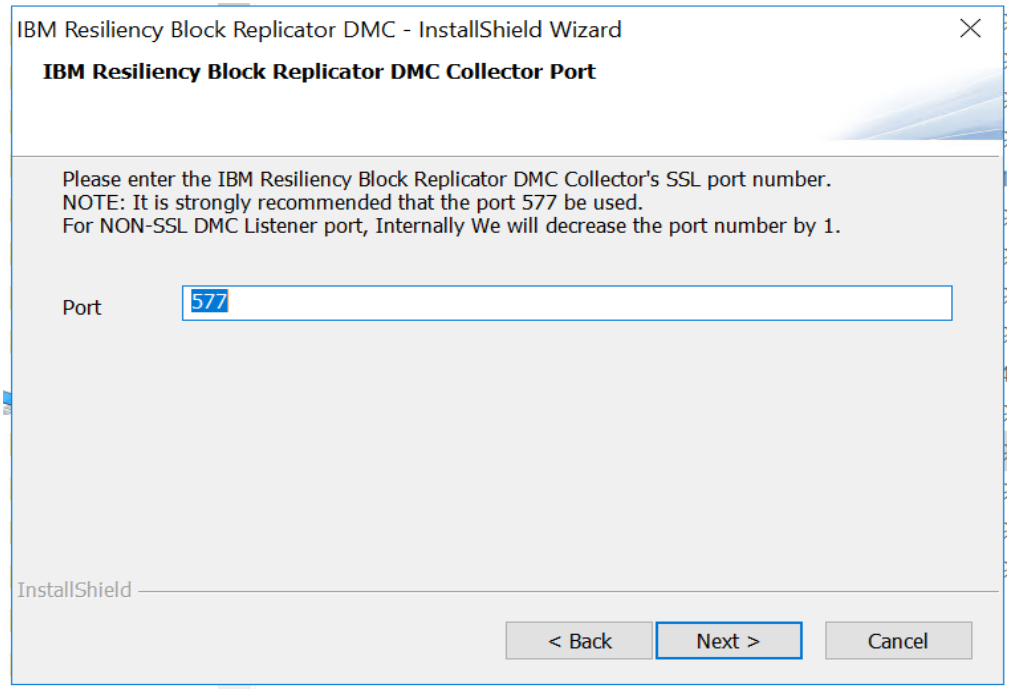


219. The Data Mobility Console Collector screen provides the IP address of the server where DMC is installed.



220. Click the **Next** button to continue.

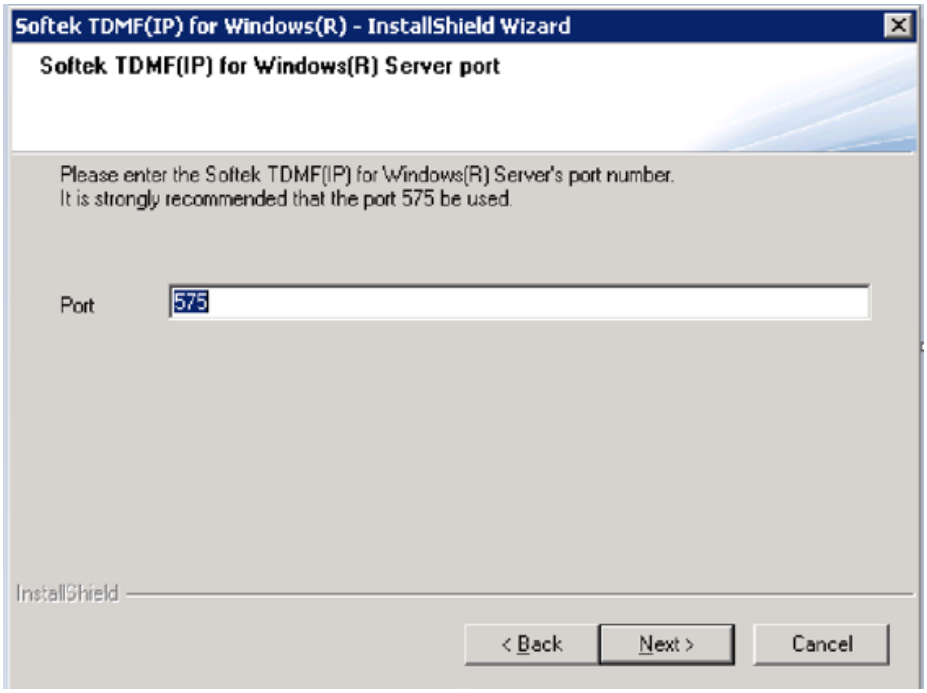
221. In the Softek data mobility console collector Port, Type the port number that is used by the DMC collector. Recommend port is 577.



222. Click the **Next** button to continue.

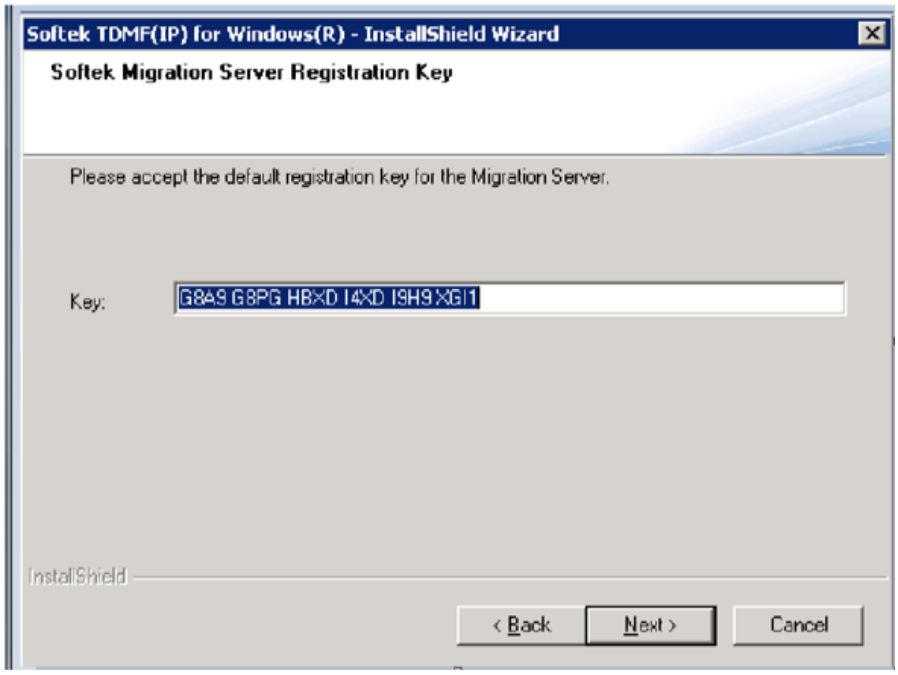
223. In the mobility server port screen, type the port number used by the Mobility server.

Note: The recommended port is 575.

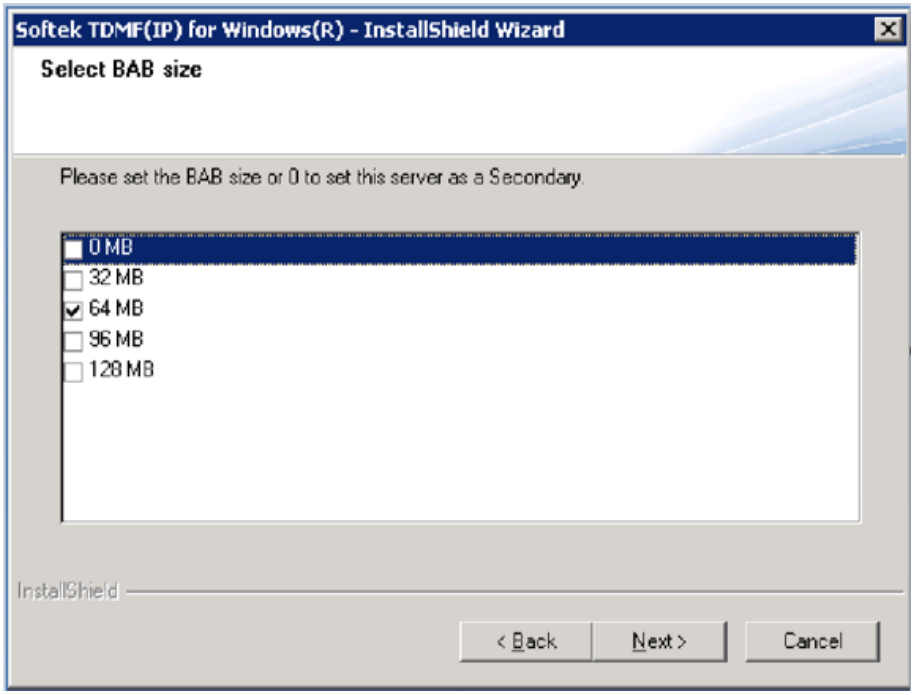


224. Click **Next** to continue.

225. At the server registration key, accept the prepopulated default registration key and click the **Next** button to continue.



226. On the Select BAB Size screen, select the BAB size.

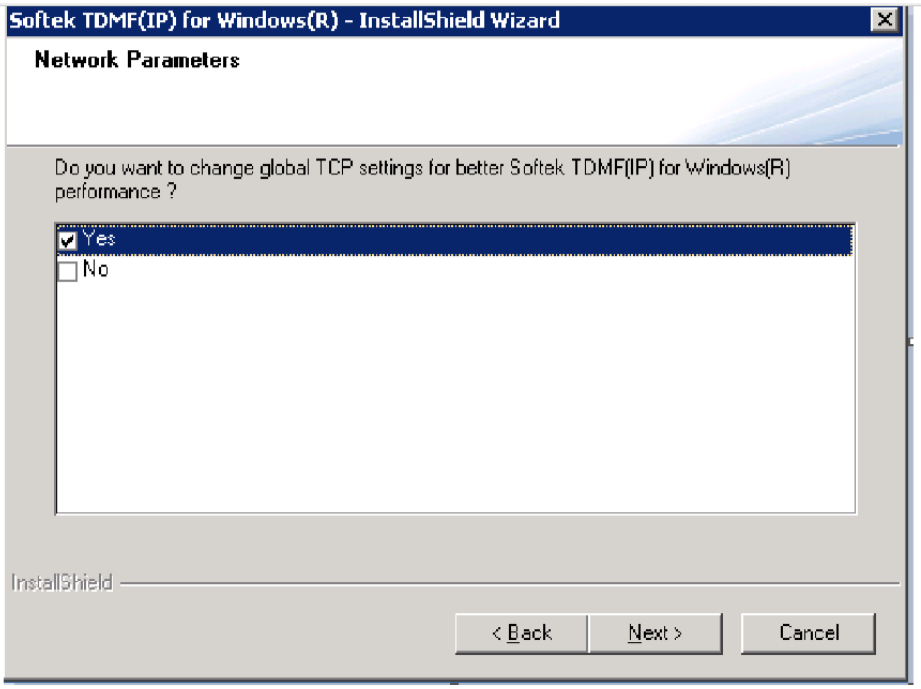


Note:

- Recommend BAB is 128MB.
- BAB size is applicable only in the case of primary.
- Select BAB size as zero if it is a secondary server.

227. Click the **Next** button to continue

228. In the **Network Parameters** screen select the **Yes** or **No** check boxes for better performance.



229. Click the **Next** button to continue.

230. In the **Choose Destination Location** screen, select the default location or browse the custom path for TDMF softtek installation.

231. On the **Ready to Install** screen click on the **Install** button.

13.8 Debugging Agent Installation on Windows Server

To debug the installation on Windows Server and to view or capture the debug output from a Win32 installer, keep the CTRL key pressed immediately after launching the installer until a console window appears. Before exiting the installer, copy the console output to a text file for later review.

13.9 Starting and Stopping of Agent Services on Windows Server

> **Note**
>
> Make sure that the clock settings on Kyndryl Resiliency Orchestration Server and the agent server are in sync.

Perform the following steps to view the agents installed on the server:

1. Go to **Control Panel**.

232. Click **Administrative Tools** on the **Control Panel**.

233. Click the **Services** icon on the **Administrative Tools** window. You can see the agents installed on the server.

The following are the agents supported by Kyndryl Resiliency Orchestration on Windows Server. Depending on the installed agents, the services window will show some of the following options:

- Panaces Agent for MS Windows OS
- Panaces Agent for Kyndryl Resiliency File Replicator
- Panaces Agent for MS SQL Server
- Kyndryl Resiliency File Replicator
- Panaces Agent for Oracle
- Panaces Agent for Oracle DataGuard
- SRDF Agent

234. Right-click on the respective service in the **Services** window and perform the following steps:

- Select **Start** to start the service.
- Select **Stop** to stop the service.
- Select **Restart** to restart the service.

14 Installing Agents on Solaris Server

This software is available on the Kyndryl Passport Advantage site. The Agents.zip when unzipped will result in the creation of the Agents folder which contains the Kyndryl Resiliency File Replicator, SRS, and Sybase Agents. It contains all the binaries and packages to run Kyndryl Resiliency Orchestration agents software. This software installation involves installing Kyndryl Resiliency Orchestration agents' binaries, and a few miscellaneous software binaries.

> **Note**
>
> Solaris OS Agent is automatically installed during the installation of agents. Kyndryl Resiliency File Replicator is automatically installed during the installation of the Kyndryl Resiliency File Replicator Agent.

14.1 Prerequisites for Installing Resiliency Orchestration Agents

Kyndryl Resiliency Orchestration Agent Software packages are available for each supported application, protection software, and operating system. These agents are installed on the servers involved in the Disaster Recovery solution. The installer installs the Kyndryl Resiliency Orchestration Agent Platform package, required for the installation of agent software, on the same server. This installation happens automatically during agent installation.

For the installer to install the Kyndryl Resiliency Orchestration Agent Platform package successfully on Solaris, the following prerequisites must be fulfilled.

14.2 Solaris Server Requirements

The server participating in the DR infrastructure must incorporate the following requirements.

Hardware / Software Requirements: The following are the Solaris Server Hardware / Software requirements:

1. The server must have a minimum of 2 GB RAM.

235. If the server is running Sybase, it must have Sybase ASE 12.5 or 15 data center editions.

236. Set the Solaris machine time to the desired time zone. If the desired time zone to which the Solaris machine is to be set is not available, import the time zone from another Solaris machine into /usr/share/lib/zoneinfo directory.

> **Note**
>
> Ensure that the time settings on Kyndryl Resiliency Orchestration Server and the agent server are in sync.

237. **Logs Directory:** The server should have enough allocated disk space to hold Sybase transaction logs, for up to 5 business days. Take the assistance of a consultant to size the directory appropriately. This directory can reside on either direct attached storage or externally attached storage.

    For Example: Consider that a log of 2MB is generated every 10 minutes. This will require 2MB/log * 6logs/hour * 24 hr/day * 5 days = 1.5GB of log device size.

The replication of the database dump from the primary server to the secondary server and vice versa must be manually done, either on tapes or any other backup devices. It is assumed that the server is configured with appropriate backup software to do the same. If the database dump size is small, and primary and remote servers are connected over LAN, the replication may be performed on LAN itself. In this case, backup software is not required.

14.3 Host Machines with Virtual IP Address

If there is a virtual IP address for the host or if the host is part of an OS Cluster, then add the following entry in
`$EAMSROOT/installconfig/PanacesAgentGeneric.cfg`
`PANACES_AGENT_NODE_ADDRESS=<IP Address of the Node>.`

Using this entry, Kyndryl Resiliency Orchestration Server always communicates to all agents on this IP address. This could be a Virtual IP or the original IP assigned to the interface.

14.4 Installation of Agents

This section outlines the steps to install all agents on Solaris Server. Additional steps that you must perform for specific agents are also included.

> **Note**
>
> You must have administrator, root, or equivalent privileges to install Kyndryl Resiliency Orchestration Agents.

To install the agents, perform the following steps:

1. Download the Agent Installer executable files from the Kyndryl Passport Advantage site.
2. Files are available in the zipped format in the Agents folder**.** Extract Files from `SolarisIntel_DRMAgent_<release_version>.zip` for Intel based architecture and `SolarisSparc_DRMAgent_<release_version>.zip`.
3. Go to the extracted folder and execute the following command (Use whichever is applicable):

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

Note

Make sure that you have free space of approximately 2.5 GB in /tmp directory, before executing the above command. In case /tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.

Example-

Assuming you want to make /opt/temp as the temporary directory.

#export IATEMPDIR=/opt/temp

After exporting the IATEMPDIR environment variable, proceed with the installation.

- The user should be root/administrator or have root/administrator privileges to install agents as the user should have access to the installation directory, /tmp directory, /etc/profile, etc.

238. After executing the command Kyndryl Resiliency Orchestration Agent installation starts with the following screen.

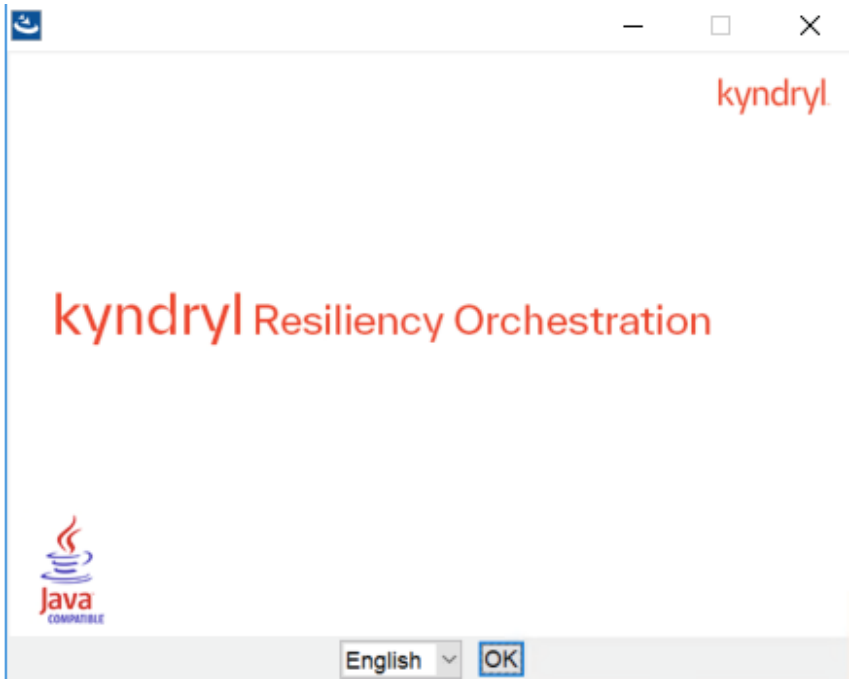


Figure 52: Kyndryl Resiliency Orchestration Agent Installer

239. After displaying the **Kyndryl Resiliency Orchestration Agent Installer** screen, the **Introduction** window is displayed.

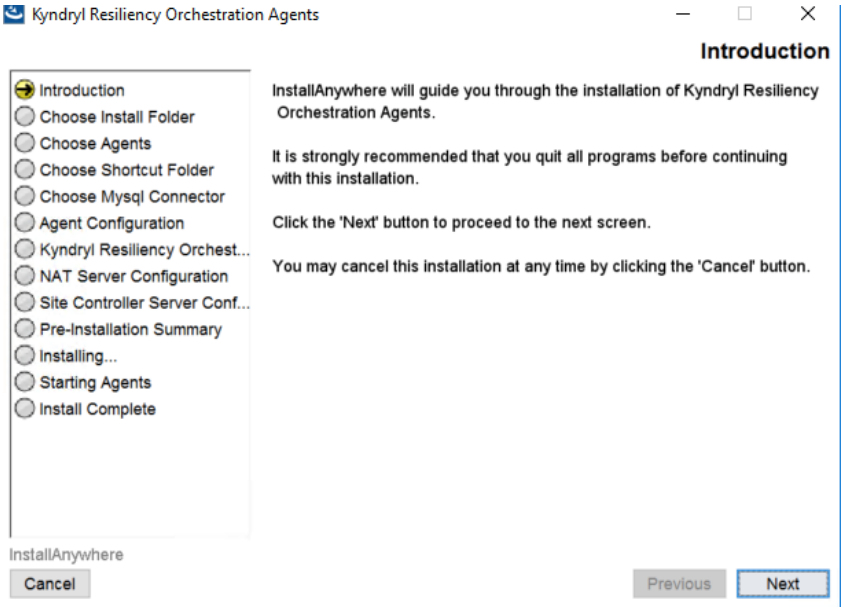


Figure 53: Kyndryl Resiliency Orchestration Agents Installation on Solaris Server - Introduction

240. Go through the installation procedure and click **Next**. The **Choose Install Folder** window is displayed.

241. Select a path to install the software by clicking **Choose.** Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is **/opt/panaces**. It is recommended that you use the default path displayed.

242. Click **Next**. The **Choose Agents - Solaris** window is displayed.

The list of agents available is displayed on the **Choose Agents - Solaris** window.

243. Select the check box next to the specific agent to install that agent. You can choose to install any or all of the agents.

244. Click **Next**. The **Choose Link Folder** window is displayed.

245. Choose a path for creating links in the **Choose Link Folder** window.

- Select **In your home folder** for creating a link in the home folder.
- Select **Other** to enter a specific path.
- Select **Don't create links** for not creating shortcut folders.

246. Click **Next**. The **Agent Configuration** window is displayed.

247. Enter Sybase JDBC driver jar file location.

248. Click the **Choose** button to select the jar file location.

> **Note**
>
> Confirm that the selected path has all the JDBC driver jar files.

249. Click **Next.** For the Sybase agent, enter the **Sybase Admin login ID** for the Sybase database.

250. Enter the IP addresses/Names of the primary and secondary Kyndryl Resiliency Orchestration servers and Kyndryl Resiliency Orchestration Agent Node Address. In a non-NAT environment, the NAT IP address should be left blank.

251. In a NAT environment, provide the Primary and secondary Resiliency Orchestration Server's public IP. Resiliency Orchestration Agent node address should be the public IP & NAT IP address should be the private IP of the server where you are installing.

> **Note**
>
> To change the Nat IP configuration after installation or to troubleshoot the issue refer to NAT IP in the Troubleshooting section.

252. Click **Next.** Enter Site Controller IP Address/Name if required.

19. Click **Next**. The **Pre-Installation Summary** window is displayed.
20. **Go** through the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify.
21. Click **Install.** The Installing Kyndryl Resiliency Orchestration Agents window is displayed.
22. Once the installation is complete, the **Starting Agents** window is displayed.

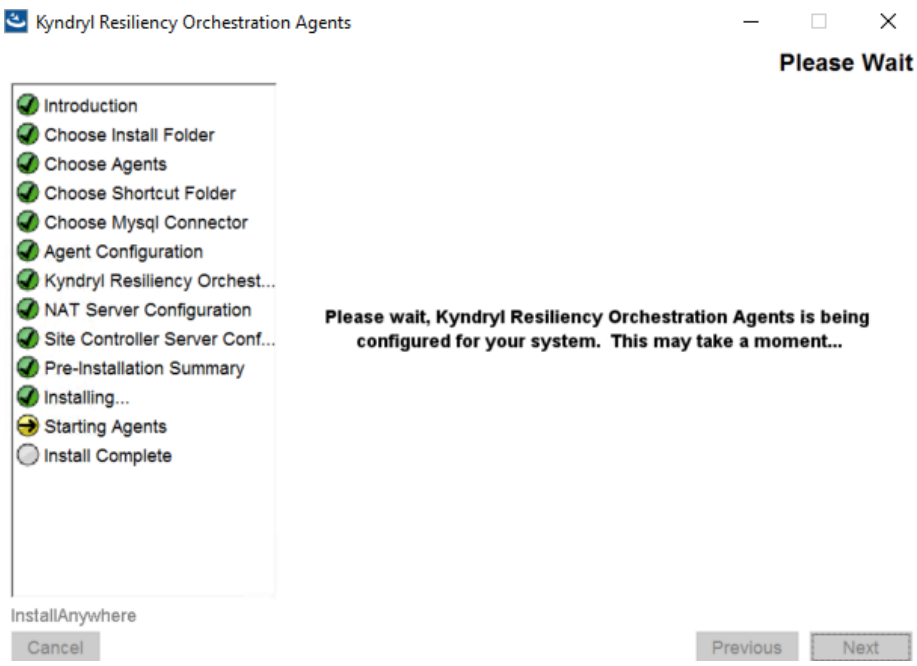


Figure 54: Kyndryl Resiliency Orchestration Agents Installation on Solaris Server – Starting Agents

23. On the **Starting Agents** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

> **Note**
>
> The best practice is not to change the default value displayed on the Starting Agents window.

24. Restart the agent machine, if the agents do not start after agent installation is complete.
25. Click **Next**. The **Install Complete** window is displayed, indicating the successful installation.

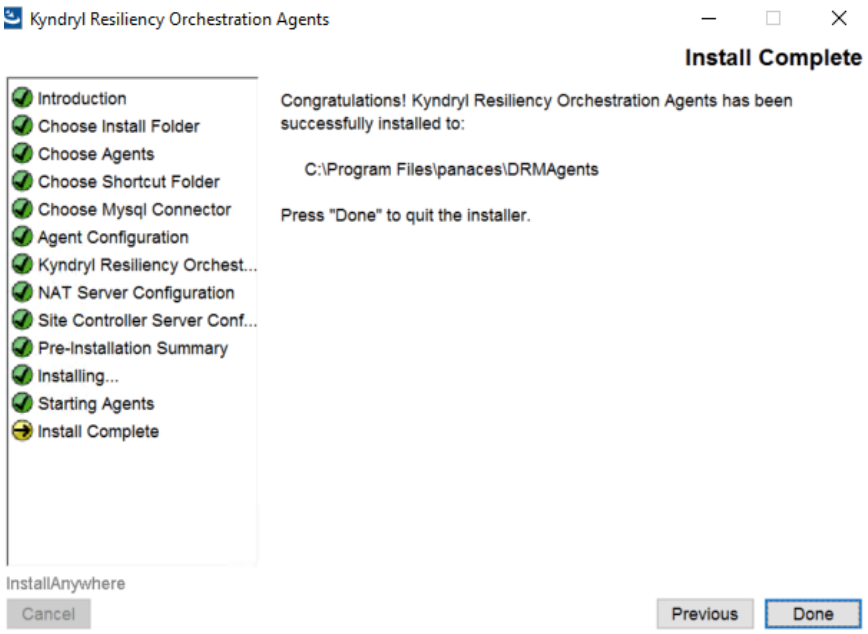


Figure 55: Kyndryl Resiliency Orchestration Agents Installation on Solaris Server – Install Complete

26. Click **Done** to complete the installation process.

> **Note**
>
> After the agent installation, log off and log in again to your computer to affect the Kyndryl Resiliency Orchestration environment variables settings permanently.
>
> When the installation is carried on silent mode or GUI mode, restart with a Putty session for Unix and Remote Desktop session for Windows.
>
> In the panaces.properties file present in both locations $EAMSROOT/UpgradeAssist/installconfig/ and $EAMSROOT/DRMAgents/installconfig/, the following values needs to be set.
>
> *panaces.acp.communicationTLSCipher=default*

14.5 Debugging Agent Installation on Solaris Server

To debug the Agent installation on Solaris Server, refer to the log entries made in the file *PanacesAgentdebug.log.* The file is located in /opt directory.

In case you encounter "Java.lang.IllegalArgumentException: Malformed \uxxxxx encoding," perform the following steps.

kyndryl

1. Open the .profile file.
2. Update the default value of the PS1 variable as below.

```
PS1="\e[0;33m[\u@\h \W]\$\e[m "
```

Note: You may see no value for PS1, even in this case, you will need to add the above line in the `.profile` file.

14.6 Starting and Stopping Agents on Solaris Server

The script for starting and stopping the agents resides at the following location on the Solaris Server:

```
/etc/rc3.d
```

14.6.1 Solaris OS Agent

The script **S99PanOSAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually –

Go to $EAMSROOT and enter the following command:

```
# nohup ./SolarisOSAgent.sh start &

# nohup. /SolarisOSAgent.sh stop &
```

> **Note**
>
> Java is not bundled with the installer for Intel Solaris systems. Instead, the system uses Java installed with the Operating System (OS).

For Intel Solaris machines, the following steps are performed to use Java installed with the OS:

253. Rename installer bundled java

```
mv /opt/panaces/jre /opt/panaces/orig_jre
```

254. Create a softlink to the os java:

```
ln -s /usr/bin/java/jre /opt/panaces/jre
```

> **Note:**
>
> $EAMSROOT is /opt/panaces as explained in this guide. This is the default location. However, you can install the agents at any other location.

14.6.2 PFR Agent

The script **S99PanPFRAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually –

Go to $EAMSROOT and enter the following command:

```
# nohup ./PFRAgent.sh start &

# nohup ./PFRAgent.sh stop &
```

14.6.3 Sybase Agent

The script **S99PanSybAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually –

Go to $EAMSROOT and enter the following command:

```
# nohup ./SybaseAgent.sh start &

# nohup ./SybaseAgent.sh stop &
```

14.6.4 SRS Agent

The script **S99PanSRSAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually –

Go to $EAMSROOT and enter the following command:

```
# nohup ./SRSAgent.sh start &

# nohup ./SRSAgent.sh stop &
```

14.6.5 Oracle Agent

The script **S99PanOraAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually –

Go to $EAMSROOT and enter the following command:

```
# nohup ./OracleAgent.sh start &

# nohup ./OracleAgent.sh stop &
```

14.6.6 TrueCopy

The script **S99PanTrueCopyAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually –

Go to $EAMSROOT and enter the following command:

```
$nohup ./TrueCopyAgent.sh start &

$nohup ./TrueCopyAgent.sh stop &
```

14.6.7 Listing the Running Agents

Enter the following command to check whether the agents installed have been started or not:

```
# ps –ef | grep –I LAX
```

This command will list the names of the agents that have been started.

15 Installing Agents on Linux Server

This software is available on the Kyndryl Passport Advantage site and can be accessed by the customer with the given credentials. This software installation involves installing Kyndryl Resiliency Orchestration agents' binaries, and a few miscellaneous software binaries.

> **Note**
>
> Linux OS Agent is automatically installed during the installation of agents. Kyndryl Resiliency File Replicator is automatically installed during the installation of the Kyndryl Resiliency File Replicator Agent.

15.1 Installation of Agents

This section outlines the steps to install all agents on Linux Server. Additional steps that you must perform for specific agents are also included.

> **Note**
>
> You must have administrator, root, or equivalent privileges to install Kyndryl Resiliency Orchestration Agents.
>
> Refer to the note about unzip utility on RHEL 7.9 at Unzip Note.

To install the agents, perform the following steps:

1. Download the server binaries from the Kyndryl Passport Advantage site.
2. Browse through Kyndryl Resiliency Orchestration software from the downloaded path and go to the folder **Agent/**Linux_DRMAgent_<release_version>.zip for 32-bit Linux Operating Systems or **Agents/** Linux64_DRMAgent_<release_version>.zip for 64-bit Linux Operating Systems.
3. Execute the following command: (Use whichever is applicable)

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

> **Note**
>
> Make sure that you have free space of approximately 2.5 GB in /tmp directory, before executing the above command. In case /tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.
>
> Example-
>
> Assuming you want to make /opt/temp as the temporary directory.

#export IATEMPDIR=/opt/temp

After exporting the IATEMPDIR environment variable, proceed with the installation.

The user should be root/administrator or have root/administrator privileges to install agents as the user should have access to the installation directory, /tmp directory, /etc/profile, etc.

4. After executing the command, the Kyndryl Resiliency Orchestration Agent installation starts with the following screen.

Note

If the RHEL version is not 7.x/8.x, then a warning message will be displayed on the screen. However, the user can continue with the installation.

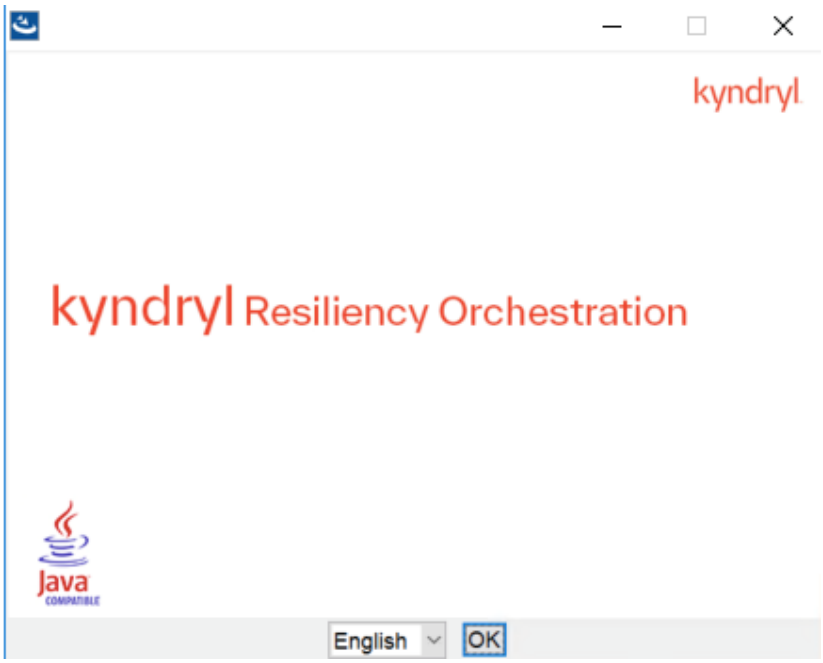


Figure 56: Kyndryl Resiliency Orchestration Agent Installer

5. After displaying the Kyndryl Resiliency Orchestration Agent Installer screen, the Introduction window is displayed.

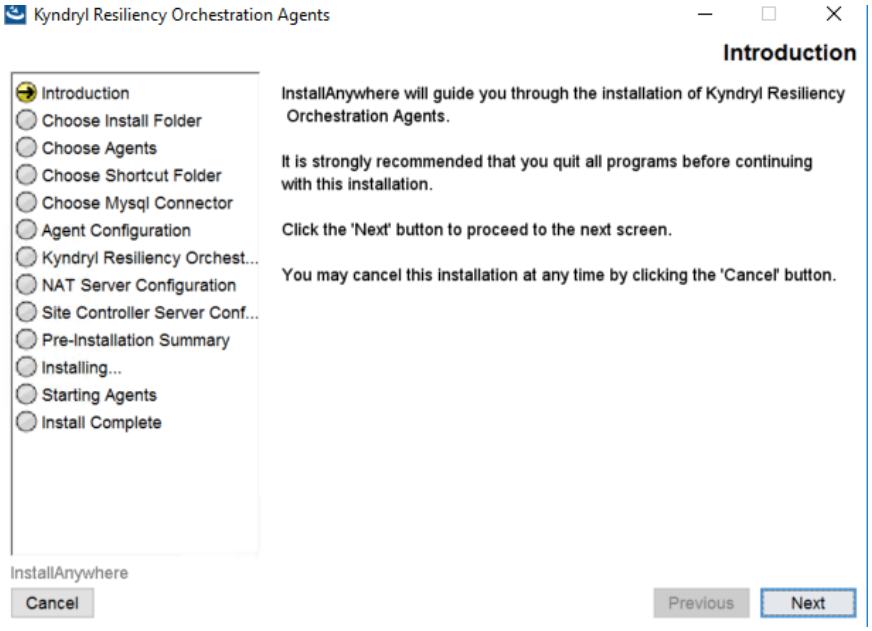


Figure 57: Kyndryl Resiliency Orchestration Agents Installation on Linux Server – Introduction

6. Go through the installation procedure and click **Next**. The **Choose Install Folder** window is displayed.
7. Select a path to install the software by clicking **Choose.** Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is **/opt/panaces**. It is recommended that you use the default path displayed.
8. Click **Next. The Choose Agents - Linux window is displayed.**
9. The list of agents available is displayed on the **Choose Agents - Linux** window. Select the check box next to the specific agent to install that agent. The user can choose to install any or all of the agents.
10. Click **Next.** The **Choose Link Folder** window is displayed.
11. Choose a path for creating links in the **Choose Link Folder** window.

- Select **In your home folder** for creating a link in the home folder.
- Select **Other** to enter a specific path.
- Click **Don't create links** for not creating shortcut folders.

12. Click **Next**. The **Agent Configuration** window is displayed.
13. Enter the Oracle home directory location. Click **Choose** button to select the file location.

14. Click **Next**. Enter the Oracle JDBC driver jar directory. Click **Choose** button to select the jar file location.

> **Note**
>
> Confirm that the selected path has all the JDBC driver jar files.

15. Click **Next**. Enter the **Oracle Java lib directory location.** Click the **Choose** button to select the file location.
16. Enter the IP address/Name of the primary and secondary Kyndryl Resiliency Orchestration servers and Kyndryl Resiliency Orchestration Agent Node Address.

> **Note:**
>
> - In a non-NAT environment, the NAT IP address field should be left blank.
> - In a NAT environment, the Primary and secondary Resiliency Orchestration Server's public IP should be given. Resiliency Orchestration Agent node address should be the public IP and the NAT IP address should be the private IP of the server where you are installing.
> - For changing NAT IP configuration when installation is complete or troubleshooting NAT IP, refer to NAT IP. Post Metadata replication, standby server status can display the following error in the standby server:
>
>   ```
>   Unable to load replication GTID slave state from mysql.gtid_slave_pos: Table 'mysql.gtid_slave_pos' doesn't exist
>   ```
>
>   In case this error is displayed, run the following command in the primary and standby server:
>
>   ```
>   sudo mysql_upgrade
>   ```

17. Click **Next.** Enter Site Controller IP Address/Name, if required.
18. Click **Next**. The **Pre-Installation Summary** window is displayed.
19. Go through the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify.
20. Click **Install.** The Installing Kyndryl Resiliency Orchestration Agents window is displayed.

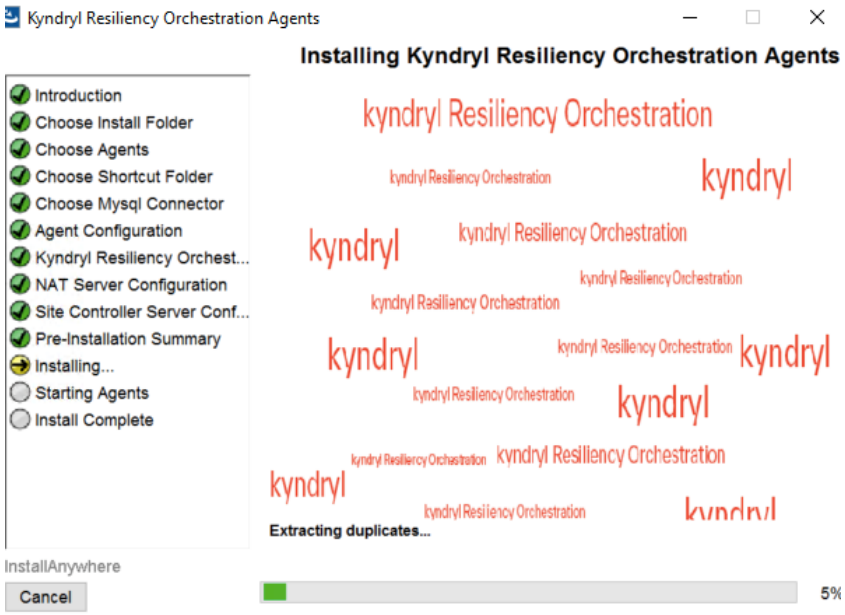


Figure 58: Kyndryl Resiliency Orchestration Agents Installation on Linux Server - Installing Kyndryl Resiliency Orchestration Agents

21. Once the installation is complete, the **Starting Agents** window is displayed.

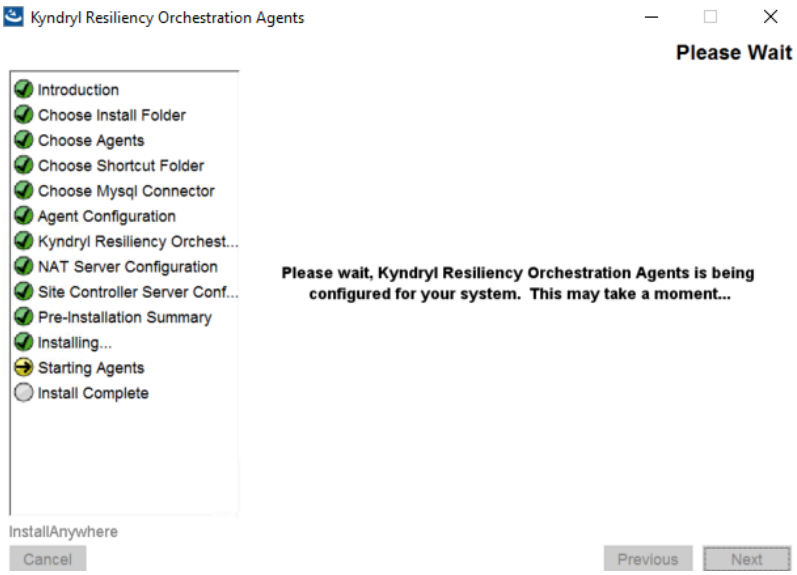


Figure 59: Kyndryl Resiliency Orchestration Agents Installation on Linux Server - Starting Agents

22. On the **Starting Agents** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

Note

- The best practice is not to change the default value displayed on the Starting Agents window.
- Restart the agent machine, if the agents do not start after agent installation is complete.

23. Click **Next**. The **Install Complete** window is displayed, indicating a successful installation.

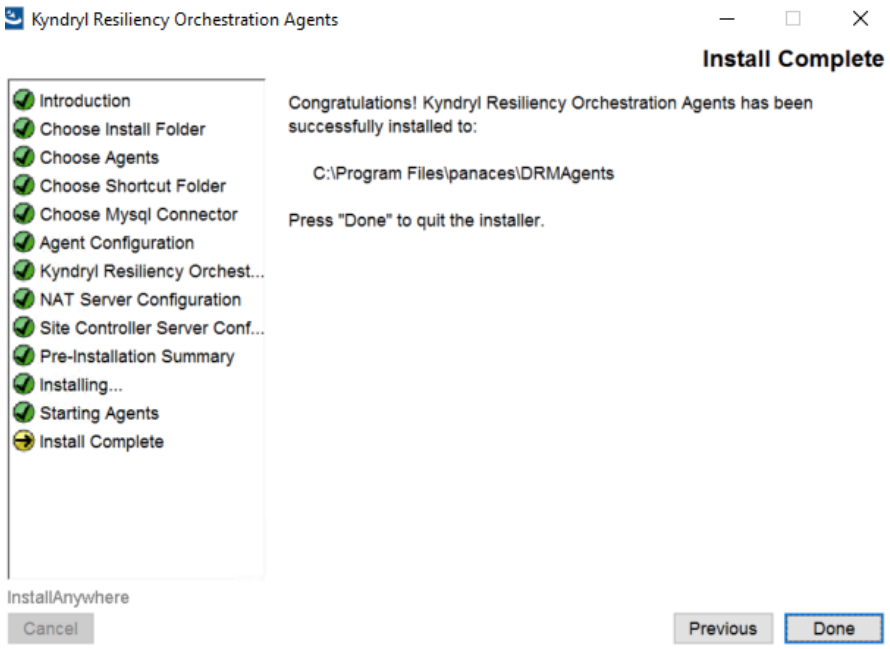


Figure 60: Kyndryl Resiliency Orchestration Agents Installation on Linux Server - Install Complete

24. Click **Done** to complete the installation process.
25. Download GPL dependent binaries for MySQL Agent as listed in the below table.

For more information about the GPL licenses, see *GPL License Information*

My SQL

kyndryl

$EAMSROOT/lib/mysql-connector-java-5.1.20-bin.jar

Note

The GPL dependant binaries are only for local agents required post-installation.

After the agent installation, log off and log in again to your computer to effect Kyndryl Resiliency Orchestration environment variables settings permanently.

When the installation is carried on silent mode or GUI mode, log off and log in with a Putty session for Unix as well as for Windows.

15.2 Debugging Agent Installation on Linux Server

To debug the Agent installation on Linux Server, refer to the log entries made in the file *PanacesAgentDebug.log*. The file is located in the /opt directory.

15.3 Starting and Stopping Agents on Linux Server

The script for starting and stopping agents is located at the following location on Linux Server:

```
/etc/rc3.d
```

15.3.1 Linux OS Agent

The script **S99PanOSAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./LinuxOSAgent.sh start &

# nohup ./LinuxOSAgent.sh stop &
```

Note that $EAMSROOT is /opt/panaces as explained in this guide. This is the default location. However, you can install the agents at any other location.

15.3.2 PFR Agent

The script **S99PanPFRAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./PFRAgent.sh start &

# nohup ./PFRAgent.sh stop &
```

15.3.3 Oracle Agent

The script **S99PanOraAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./OracleAgent.sh start &

# nohup ./OracleAgent.sh stop &
```

15.3.4 Oracle Data Guard Agent

The script **S99PanOraAgt** starts the service automatically when the server is rebooted. Alternatively, the following steps can be used to start or stop the agent manually:

1. Go to $EAMSROOT and enter the following command to start the agent manually:

```
# nohup ./dataguardagent.sh start &
```

2. Enter the following command to start the agent manually:

```
# nohup ./dataguardagent.sh stop &
```

15.3.5 PostgreSQL Agent

The script **S99PanPostgresAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./PostgresAgent.sh start &

# nohup ./PostgresAgent.sh stop &
```

15.3.6 Listing the Agents that are Running

Enter the following command to check whether the agents installed have been started or not:

```
# ps –ef | grep –i LAX
```

This command will list the names of the agents that have been started.

15.3.7 Installing TDMF Agent on Linux

Prerequisites:

Ensure that the redhat-lsb version is 3.0 or later.

Steps

1. Copy the TDMF agent installer to the Linux host.
2. Install the rpm using the command “rpm -ivh tdmf-rpm”
3. Provide the collector information using the dtcagentset command

   - `cd /opt/IBMRBRdtc/bin`
   - `./dtcagentset -e x.x.x.x -i y.y.y.y -b 256`

   where x.x.x.x is DMC IP(collector IP) and y.y.y.y is the system where TDMF is installed.
4. Reboot the machine using the command “init 6” or “reboot”
5. After a successful reboot check for the Linux host discovery in DMC

   Note: The DMC the online status for the VM should show up as “yes”

16 Installing Agents on HPUX Server

This software is available on the Kyndryl Passport Advantage site. It contains all the binaries and packages to run Kyndryl Resiliency Orchestration agents software. This software installation involves installing Kyndryl Resiliency Orchestration agents' binaries, and a few miscellaneous software binaries.

> **Note**
>
> HPUX OS Agent is automatically installed during the installation of agents. Kyndryl Resiliency File Replicator is automatically installed during the installation of the Kyndryl Resiliency File Replicator Agent. Kyndryl Resiliency File Replicator replication may not work on Itanium machines.

1. Install gnu-tar for HPUX for Itanium:
2. Download and manually install the GNU tar files.
3. Create the following soft links, after the installation of gnu tar:

```
ln -s <agent_install_dir>/tool/usr/local/lib/libiconv.sl

/usr/local/lib/libiconv.sl

ln -s <agent_install_dir>/tool/usr/local/lib/libintl.sl

/usr/local/lib/libintl.sl
```

16.1 Installation of Agents

This section outlines the steps to install all agents on HPUX Server. Additional steps that you must perform for specific agents are also included.

> **Note**
>
> You must have root or root equivalent privileges to install Kyndryl Resiliency Orchestration Agents.

To install the agents, perform the following steps:

1. Download the server binaries from the Kyndryl Passport Advantage site.
2. Browse through Kyndryl Resiliency Orchestration software from the downloaded path and go to the folder **Agent/**HPUX_DRMAgent_<release_version>.zip.
3. Go to the extracted folder and execute the following command: (Use whichever is applicable)

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

kyndryl

Note

- Make sure that you have free space of approximately 2.5 GB in /tmp directory, before executing the above command. In case /tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.

Example-

Assuming you want to make /opt/temp as the temporary directory.

#export IATEMPDIR=/opt/temp

After exporting the IATEMPDIR environment variable, proceed with the installation.

- The user should be root/administrator or have root/administrator privileges to install agents as the user should have access to the installation directory, /tmp directory, /etc/profile, etc.

4. After executing the command, the Kyndryl Resiliency Orchestration Agent installation starts with the following screen.

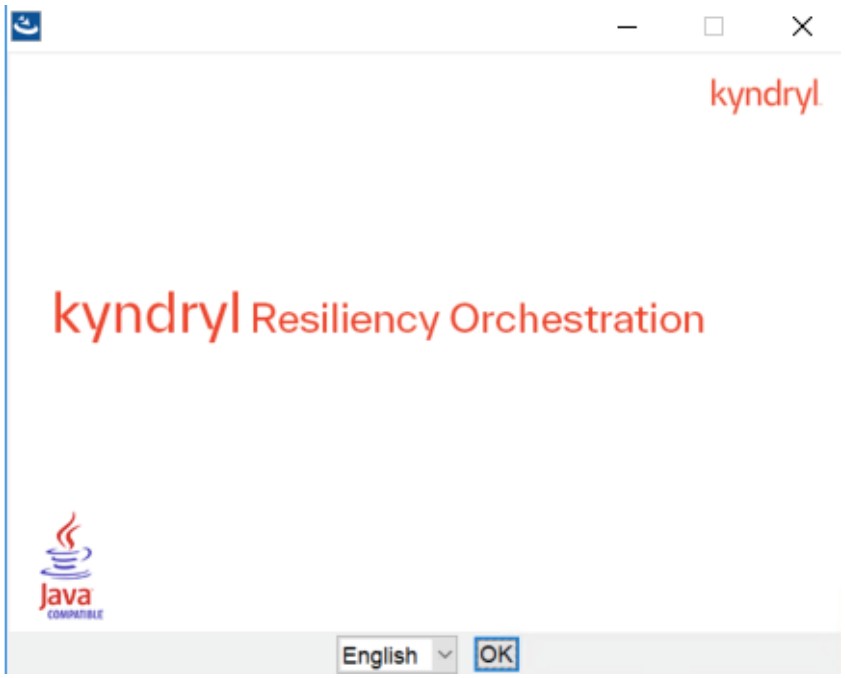


Figure 61: Kyndryl Resiliency Orchestration Agent Installer

5. After displaying the Kyndryl Resiliency Orchestration Agent Installer screen, the Introduction window is displayed.

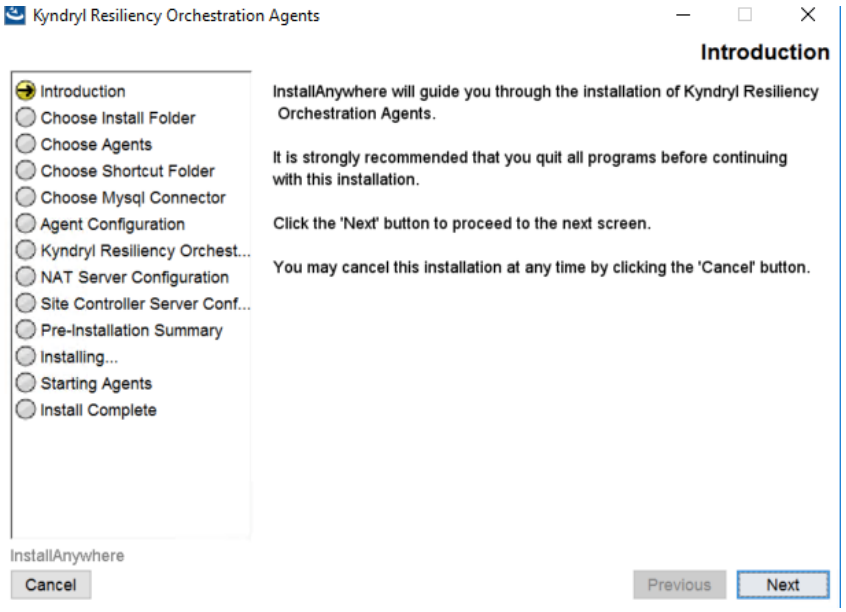


Figure 62: Kyndryl Resiliency Orchestration Agents Installation on HPUX Server - Introduction

6. Go through the installation procedure and click **Next**. The **Choose Install Folder** window is displayed.
7. Select a path to install the software by clicking **Choose.** Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is **/opt/panaces**. It is recommended that you use the default path displayed.
8. Click **Next.** The **Choose Agents - HPUX** window is displayed.
9. The list of agents available is displayed on the **Choose Agents - HPUX** window. Select the checkbox next to the specific agent to install that agent. You can choose to install any or all of the agents.
10. Click **Next**. **The Choose Link Folder window is displayed.**

kyndryl

11. Choose a path for creating links in the **Choose Link Folder** window.
- Select **In your home folder** for creating a link in the home folder.
- Select **Other** to enter a specific path.
- Click **Don't create links** for not creating shortcut folders.
12. Click **Next**. The **Agent Configuration** window is displayed.
13. Enter the Oracle home directory location. Click **Choose** button to select the file location.
14. Click **Next**. Enter the Oracle JDBC driver jar directory. Click **Choose** button to select the jar file location.

Note

Confirm that the selected path has all the JDBC driver jar files.

15. Click **Next**. Enter the **Oracle Java lib directory location.** Click the **Choose** button to select the file location.
16. Enter the IP address/Name of the primary and secondary Kyndryl Resiliency Orchestration servers and Kyndryl Resiliency Orchestration Agent Node Address.

Note:

- In a non-NAT environment, the NAT IP address should be left blank.
- In a NAT environment, the Primary and secondary Resiliency Orchestration server's public IP should be given. Resiliency Orchestration Agent node address should be the public IP & NAT IP address should be the private IP of the server where you are installing.
- For changing NAT IP configuration post-installation or troubleshooting, refer to Troubleshooting NAT IP. Post Metadata replication, standby server status can display the following error in the standby server:

```
Unable to load replication GTID slave state from
mysql.gtid_slave_pos: Table 'mysql.gtid_slave_pos' doesn't
exist
```

In case this error is displayed, run the following command in the Primary and Standby server:

```
sudo mysql_upgrade
```

17. Click **Next.** Enter Site Controller IP Address/Name if required.
18. Click **Next**. The **Pre-Installation Summary** window is displayed.
19. Go through the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify.
20. Click **Install.** The Installing **Kyndryl Resiliency Orchestration Agents** window is displayed.

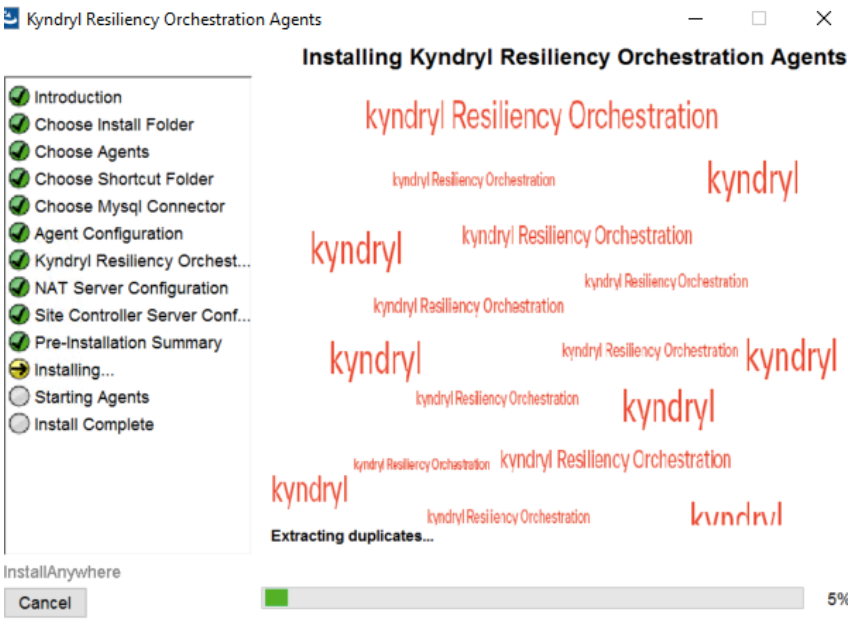


Figure 63: Kyndryl Resiliency Orchestration Agents Installation on HPUX Server - Installing Kyndryl Resiliency Orchestration Agents

21. Once the installation is complete, the **Starting Agents** window is displayed.
22. On the **Starting Agents** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

> **Note**
>
> The best practice is not to change the default value displayed on the Starting Agents window.

23. Restart the agent machine, if the agents do not start after agent installation is complete.
24. Click **Next**. The **Install Complete** window is displayed, indicating the successful installation.

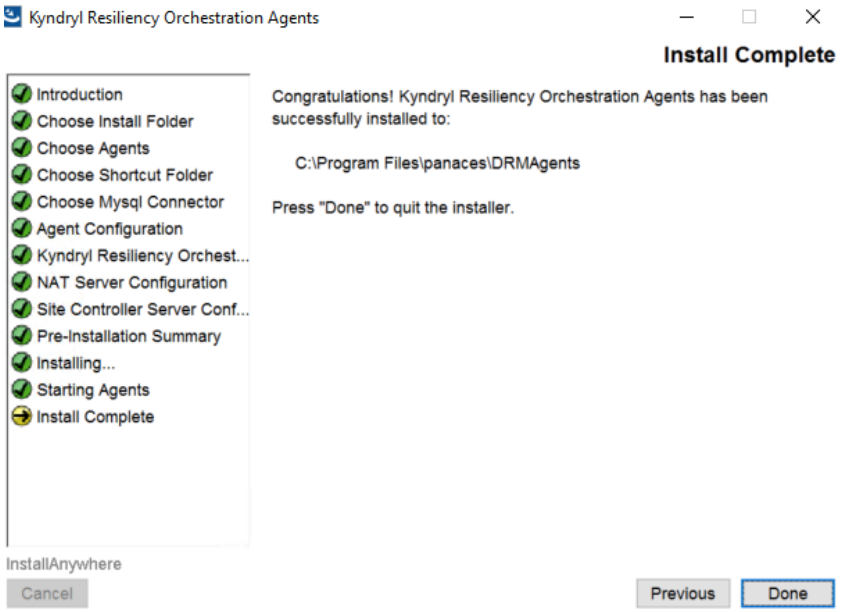


Figure 64: Kyndryl Resiliency Orchestration Agents Installation on HPUX Server - Install Complete

25. Click **Done** to complete the installation process.

Note

- After the agent installation, you need to log off and log on again for the Kyndryl Resiliency Orchestration environment variables settings to take effect permanently.
- When the installation is carried on silent mode or GUI mode, restart with a Putty session for Unix and Remote Desktop session for Windows.

In the panaces.properties file present in both locations $EAMSROOT/UpgradeAssist/installconfig/ and $EAMSROOT/DRMAgents/installconfig/, the following value need to be set.

panaces.acp.communicationTLSCipher=default

16.2 Debugging Agent Installation on HPUX Server

To debug the Agent installation on HPUX Server, refer to the log entries made in the file *PanacesAgentDebug.log*. The file is located in the /opt directory.

16.3 Starting and Stopping Agents on HPUX Server

16.3.1 HPUX OS Agent

The following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./HPUXOSAgent.sh start &

# nohup ./HPUXOSAgent.sh stop &
```

> **Note:**
>
> $EAMSROOT is /opt/panaces as explained in this guide. This is the default location. However, you can install the agents at any other location.

16.3.2 PFR Agent

The following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./PFRAgent.sh start &

# nohup ./PFRAgent.sh stop &
```

16.3.3 Oracle Agent

The following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./OracleAgent.sh start &

# nohup ./OracleAgent.sh stop &
```

16.3.4 Oracle Data Guard Agent

The following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./DataGuardAgent.sh start &

# nohup ./DataGuardAgent.sh stop &
```

16.3.5 Listing the Agents that are Running

Enter the following command to check whether the agents installed have been started or not:

```
# ps –ef | grep –i LAX
```

This command will list the names of the agents that have been started.

17 Installing Agents on AIX Server

This software is available on the Kyndryl Passport Advantage site. It contains all the binaries and packages to run Kyndryl Resiliency Orchestration agents software. This software installation involves installing Kyndryl Resiliency Orchestration agents' binaries, and a few miscellaneous software binaries.

> **Note**
>
> AIX OS Agent is automatically installed during the installation of agents. Kyndryl Resiliency File Replicator is automatically installed during the installation of the Kyndryl Resiliency File Replicator Agent.

17.1 Prerequisites for Installing Resiliency Orchestration Agents

Kyndryl Resiliency Orchestration Agent Software packages are available for each supported application, protection software, and operating system. These agents are installed on the servers involved in the Disaster Recovery solution. The installer also installs the Kyndryl Resiliency Orchestration Agent Platform package, required for agent software to be installed, on the same server. This installation happens automatically during agent installation.

For the installer to install the Kyndryl Resiliency Orchestration Agent Platform package successfully on AIX, the following prerequisites must be fulfilled.

17.2 AIX Server Requirements

The server participating in the DR infrastructure must incorporate the following requirements:

Hardware / Software Requirements: The following are the AIX Server Hardware / Software requirements:

- The server must have a minimum of 2 GB RAM.
- Confirm that the AIX machine is set to the desired time zone.

AIX 6.1 TL7 (6100-07) or later is required to work with Java 8. For details, refer to https://www-01.ibm.com/support/docview.wss?uid=isg3T1022644#requirements

> **Note**
>
> Confirm that the time settings on Kyndryl Resiliency Orchestration Server and the agent server are in sync.

kyndryl

17.3 Host Machines with Virtual IP Address

If there is a virtual IP address for the host or if the host is part of an OS Cluster, add the following entry in `$EAMSROOT/installconfig/PanacesAgentGeneric.cfg` `PANACES_AGENT_NODE_ADDRESS=<IP Address of the Node>`. Using this entry, Kyndryl Resiliency Orchestration Server always communicates to all agents on this IP address. This could be a Virtual IP or the original IP assigned to the interface.

17.4 Install TDMF on AIX:

To install TDMF on AIX, perform the below steps.

1. Copy TDMF build to the VM's using SCP or winscp etc.
2. Use the below command to create a directory.

   ```
   mkdir /var/dtc
   ```

3. Go to the directory the where TDMF build is copied and run the following command.

   ```
   tar -xvf TDMFIP-AIX72-02.08.0000.0000-
   DEV20200702120915.rs600.tar
   ```

4. Add the entry in /etc/hosts, on Production and SAVM machines.

   ```
   Eg:192.168.131.214        rovps9-2
    eg:192.168.131.213        ropvm3
   ```

5. Installp -a -V 4 -e /var/dtc/dtc_install.log -d . dtc.rte 6) open all ports for ipv4 and v6

   ```
   # chfilt -v 4 -n '0' -a 'P'
   # chfilt -v 6 -n '0' -a 'P'
   ```

17.5 Installation of Agents

This section outlines the steps to install all agents on AIX Server. Additional steps that you must perform for specific agents are also included.

> **Note**
>
> You must have administrator, root, or equivalent privileges to install Kyndryl Resiliency Orchestration Agents.

To install the agents, perform the following steps:

1. Download the server binaries from the Kyndryl Passport Advantage site.

2. Browse through Kyndryl Resiliency Orchestration software from the downloaded path and go to the folder Agent/AIX_DRMAgent_<release_version>.zip.
3. Go to the extracted folder and execute the following command: (Use whichever is applicable)

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

> **Note**
>
> Ensure that you have free space of approximately 2.5GB in /tmp directory, before executing the above command.
>
> In case /tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.
>
> Example-
>
> Assuming you want to make /opt/temp as the temporary directory.
>
> #export IATEMPDIR=/opt/temp
>
> After exporting the IATEMPDIR environment variable, proceed with the installation.
>
> The user should be root/administrator or have root/administrator privileges to install agents as the user should have access to the installation directory, /tmp directory, /etc/profile, etc.

4. After executing the command, the Kyndryl Resiliency Orchestration Agent installation starts with the following screen.

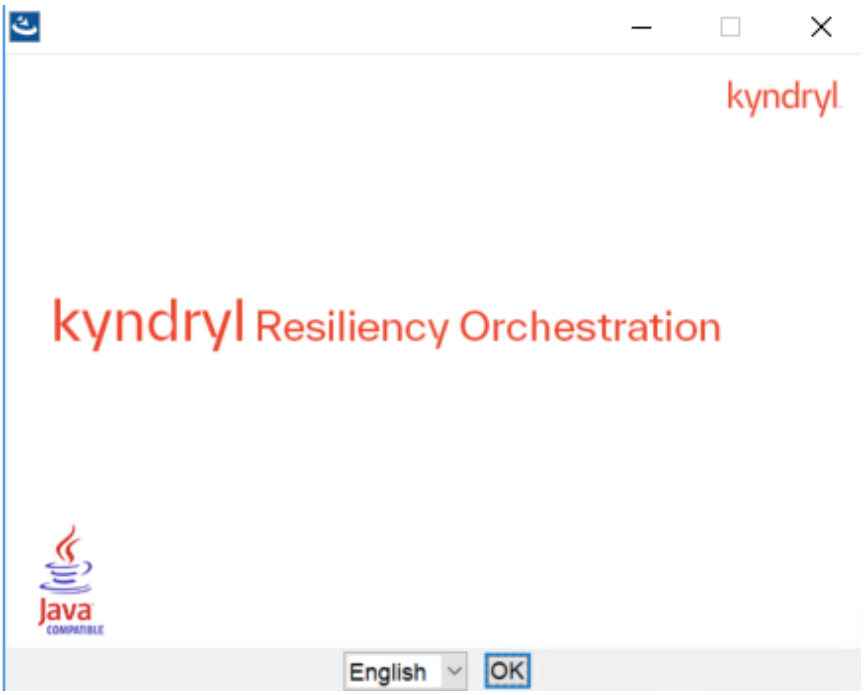


Figure 65: Kyndryl Resiliency Orchestration Agent Installer

5. After displaying the Kyndryl Resiliency Orchestration Agent Installer screen, the Introduction window is displayed.

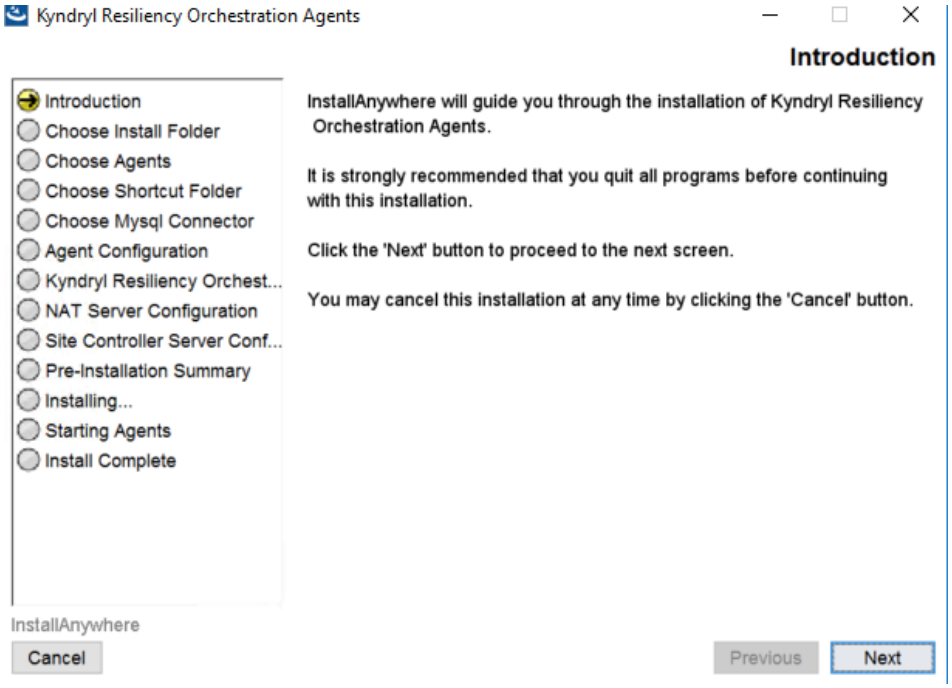


Figure 66: Kyndryl Resiliency Orchestration Agents Installation on AIX Server - Introduction

6. Go through the installation procedure and click **Next**. The **Choose Install Folder** window is displayed.
7. Select a path to install the software by clicking **Choose.** Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is **/opt/panaces**. It is recommended that you use the default path displayed.
8. Click **Next.** The **Choose Agents - AIX** window is displayed.
9. The list of agents available is displayed on the **Choose Agents - AIX** window. Select the checkbox next to the specific agent to install that agent. You can choose to install any or all of the agents.
10. Click **Next**. **The Choose Link Folder window is displayed.**
11. Choose a path for creating links on the **Choose Link Folder** window.
    - Select **In your home folder** for creating a link in the home folder.
    - Select **Other** to enter a specific path.
    - Click **Don't create links** for not creating shortcut folders.
12. Click **Next**. The **Agent Configuration** window is displayed.
13. Enter the DB2 Instance user login ID. Click **Next**.

kyndryl

> **Note**
>
> If the PFR agent is selected, then the installer skips this step and displays the Kyndryl Resiliency Orchestration Server IP Address Configuration window as PFR Agent does not require any configuration.

14. Enter the IP address/Name of the primary and secondary Kyndryl Resiliency Orchestration servers and Kyndryl Resiliency Orchestration Agent Node Address.

> **Note:**
>
> - In a non-NAT environment, the NAT IP address should be left blank.
> - In a NAT environment, the Primary and secondary Resiliency Orchestration Server's public IP should be given. Resiliency Orchestration Agent node address should be the public IP and the NAT IP address should be the private IP of the server where you are installing
> - For changing NAT IP configuration post-installation or troubleshooting, refer to Troubleshooting NAT IP. Post Metadata replication, standby server status can display the following error in the standby server:
>
>   ```
>   Unable to load replication GTID slave state from
>   mysql.gtid_slave_pos: Table 'mysql.gtid_slave_pos' doesn't
>   exist
>   ```
>
>   In case this error is displayed, run the following command in the primary and standby server:
>
>   ```
>   sudo mysql_upgrade
>   ```

15. Click **Next.** Enter Site Controller IP Address/Name if required.
16. Click **Next**. The **Pre-Installation Summary** window is displayed.
17. Go through the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify.
18. Click Install. The Installing Kyndryl Resiliency Orchestration Agents window is displayed.
19. Once the installation is complete, the **Starting Agents** window is displayed.
20. On the **Starting Agents** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

> **Note**
>
> The best practice is not to change the default value displayed on the Starting Agents window.

21. Restart the agent machine, if the agents do not start after agent installation is complete.
22. Click **Next**. The **Install Complete** window is displayed, indicating successful installation.
23. Click **Done** to complete the installation process.
24. After Agents installation, create the following directory manually in the following directory:

UpgradeAssist directory.

Note: The default UpgradeAssist directory path is as follows: `/opt/panaces/UpgradeAssist`

Navigate to the UpgradeAssist directory ($SASROOT) in the Agent installation server.

Note: $SASROOT is an environment variable having the UpgradeAssist path

```
cd /opt/panaces/UpgradeAssist
```

Execute the following commands for the creation of the directory:

```
mkdir -p    target
chmod -R 755 target
```

kyndryl

> **Note**
>
> After the Agent installation, log off and log in again to your computer to affect the Kyndryl Resiliency Orchestration environment variables settings permanently.

When the installation is carried on silent mode or GUI mode, restart with a Putty session for UNIX and Remote Desktop session for Windows.

In the panaces.properties file present in both locations `$EAMSROOT/UpgradeAssist/installconfig/` and `$EAMSROOT/DRMAgents/installconfig/`, the following value need to be set.

panaces.acp.communicationTLSCipher=default

17.6 Starting and Stopping of Agents on AIX Server

The script for starting and stopping the agents resides at the following location on AIX Server:

/etc/rc.d/rc2.d

17.6.1 AIX OS Agent

The script **S99PanOSAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./AIXOSAgent.sh start &

# nohup ./AIXOSAgent.sh stop &
```

Note that $EAMSROOT is /opt/panaces as explained in this guide. This is the default location. However, you can install the agents at any other location.

17.6.2 PFR Agent

The script **S99PanPFRAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./PFRAgent.sh start &

# nohup ./PFRAgent.sh stop &
```

17.6.3 Oracle Agent

The script **S99PanOraAgt** starts the service automatically when the server is rebooted.

Alternatively, the following steps can be used to start or stop the agent manually -

Go to $EAMSROOT and enter the following command:

```
# nohup ./OracleAgent.sh start &

# nohup ./OracleAgent.sh stop &
```

17.6.4 Oracle Data Guard Agent

The script **S99PanOraAgt** starts the service automatically when the server is rebooted. Alternatively, the following perform the following steps to start or stop the agent manually:

1. Go to $EAMSROOT and enter the following command to start the agent manually:

```
# nohup ./DataGuardAgent.sh start &
```

Enter the following command to stop the agent manually:

```
# nohup ./DataGuardAgent.sh stop &
```

17.6.5 Listing the Agents that are Running

Enter the following command to check whether the agents installed have been started or not:

```
# ps –ef | grep –i LAX
```

This command will list the names of the agents that have been started.

18 Installing Kyndryl Resiliency Orchestration Server OVA Manually

You can create the NICRA/SA Ova manually or automatically via a script.

- To create NICRA/OVA manually, refer to the topic Creating Nicra/SA OVA Manually.
- To create NICRA/OVA automatically with a script, refer to the topic Creating NICRA/SA OVA Using Automation Script.
- Refer Section 18.6 for creating NICRA/SA on RHEL 7.4 OS

18.1 Creating NICRA/SA OVA Manually (RHEL 8.4/8.6/8.8)

Prerequisite:

You must have Rhel8.4: OS kernel version **4.18.0-305**

Installed in a Virtual Machine with an RHEL OS license/subscription.

The corresponding versions are listed below:

Rhel8.6: OS Kernel version **4.18.0-372.32.1.el8_6**

Rhel8.8: OS Kernel version **4.18.0-477.27.1.el8_8**

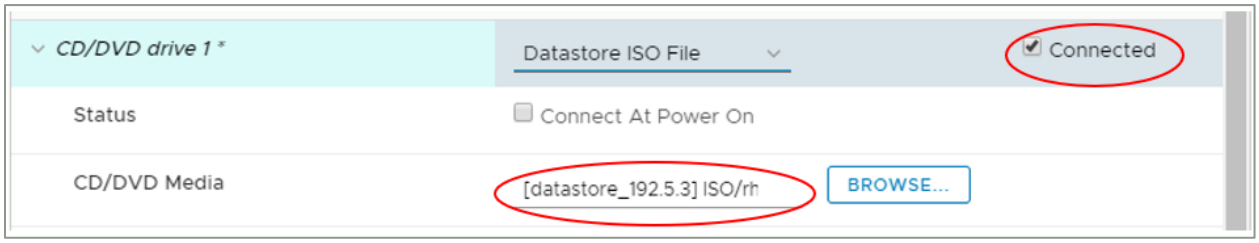
Note: If RHEL8.4 OS Volume is under Linux-based LVM volumeGroup management, the LVM VolumeGroup name should be different from that of workload VM volumeGroup.

VM configuration required is as listed below:

- 8 vCPU
- 8 GB RAM,
- 32 GB VMDK disk for OS disk,
- 32 GB VMDK disk for Persistent Store (Kyndryl RBR requirement),
- 15 GB VMDK for Journal Disk (Kyndryl RBR requirement),
- 4 x SCSI controller and
- 1 temporary IP (to copy the NICRA bundle to VM) with internet connectivity enabled.
- In case you would want to deploy the below created NICRA OVA in 6.7 ESXi, it is mandatory to generate NICRA OVA in 6.7 ESXi (To ensure the VM version is 14). The same condition applies to all ESXi versions.

Note:

- For NICRA/SA OVA upgrade, refer to the topic **Upgrading NICRA/Staging Appliance** in **VM Protection with Kyndryl Resiliency Block Replicator** user guide.
- In the VM "Edit Settings" for CD/DVD Media, make sure to select the same .iso image used for RHEL OS installation. Select the "connected" option checkbox for the CD/DVD drive as shown in the below snapshot. It will be used for LSB installation later.



Steps:

1. Copy the Kyndryl Resiliency Block Replicator-NICRA.tar available in passport advantage to /opt directory in the VM created. This NICRA bundle contains:

   a) NICRA rpm - Latest RPM

   b) NicraSetup script - which installs rpm and runs prerequisites required.

   c) Firstboot script - Enables for deployment.

2. Untar the NICRA bundle, to extract the files required for OVA creation.

3. Make a note of the network interface in your VM by running the command "ifconfig -a".

```
[root@localhost ~]# ifconfig -a
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 192.168.5.84  netmask 255.255.255.255  broadcast 192.168.5.84
inet6 fe80::d7fe:e545:70e6:b62c  prefixlen 64  scopeid 0x20<link>
ether 00:50:56:a8:ed:d9  txqueuelen 1000  (Ethernet)
RX packets 83838  bytes 663793721 (633.0 MiB)
RX errors 0  dropped 20  overruns 0  frame 0
TX packets 85109  bytes 664728852 (633.9 MiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

If the network interface is not ens161 in your deployed VM, use the below sed command to replace it with the one (ens192) which is present in your VM. This will update the first boot.sh script with your network interface.

For example, to update ens192 in the firstboot.sh □ sed -i 's/ens161/ens192/g' firstboot.sh

3.1. Boot option is not mentioned.

Here we have two optiions available, Right CLick on VM > Edit Setting > VM Options > Boot Options

Set BIOS as the boot option for RHEL version 8.4 & 8.6.

For version 8.8 set the boot option as EFI.

3.2. Removal of ipv6

Kindly disable ipv6. Only allow IPv4.

Disable ipv6 setting:

https://www.thegeekdiary.com/centos-rhel-7-how-to-disable-ipv6/

1. Edit /etc/default/grub and add ipv6.disable=1 in line GRUB_CMDLINE_LINUX, e.g.:

cat /etc/default/grub

GRUB_CMDLINE_LINUX="ipv6.disable=1 crashkernel=auto rhgb quiet"

2. Regenerate a GRUB configuration file and overwrite existing one:

grub2-mkconfig -o /boot/grub2/grub.cfg

3. Restart system and verify no line “inet6” in “ip addr show” command output.

shutdown -r now

3.3. Following Installation pakages are mandatory,

1.gdb

#yum install gdb

2.crash utility

#yum install crash

3.kernel-modules-extra-4.18.0-305.el8.x86_64

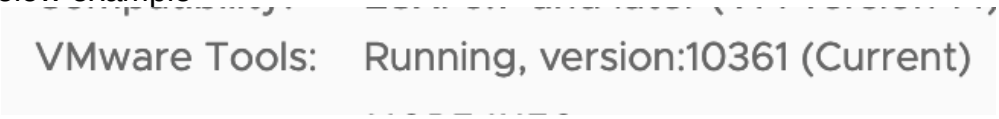
#yum install kernel-modules-extra-4.18.0-305.el8.x86_64

3.4. vmtoolsd - should be set with sbin i.e /usr/sbin/vmtoolsd

Note: With the latest vmtools it is found that vmtools is present inside /usr/bin/vmtoolsd

1.So to make the above change first we have to uninstall the latest vmtools.
2.Install the vm tools from VMwareTools-10.3.10-*

Example VMwareTools-10.3.10-12406962.tar.gz
3. Reboot
4. Check this command - "which vmtoolsd"
5. Now from the vCenter, upgrade the vmtools to current version. Something like below example



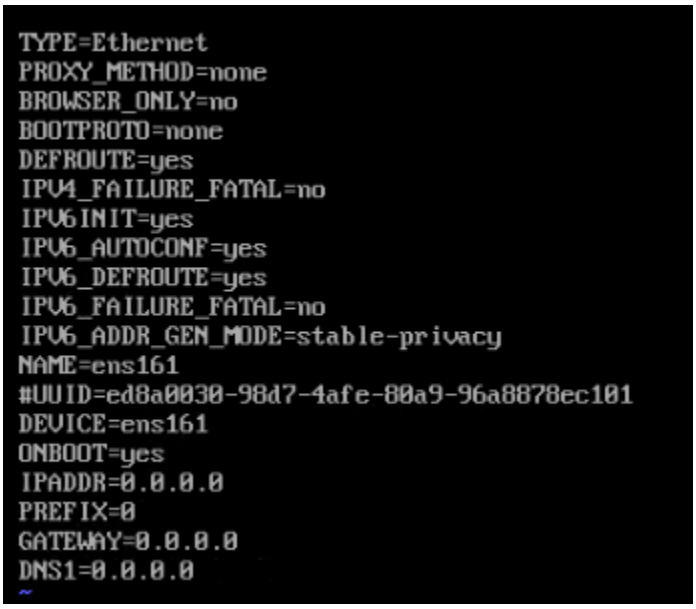
1.5 Remove unwanted packages as listed below

- yum remove gnome*
- yum remove qemu*
- yum remove libvirt *

4. Run the NicraSetup script.

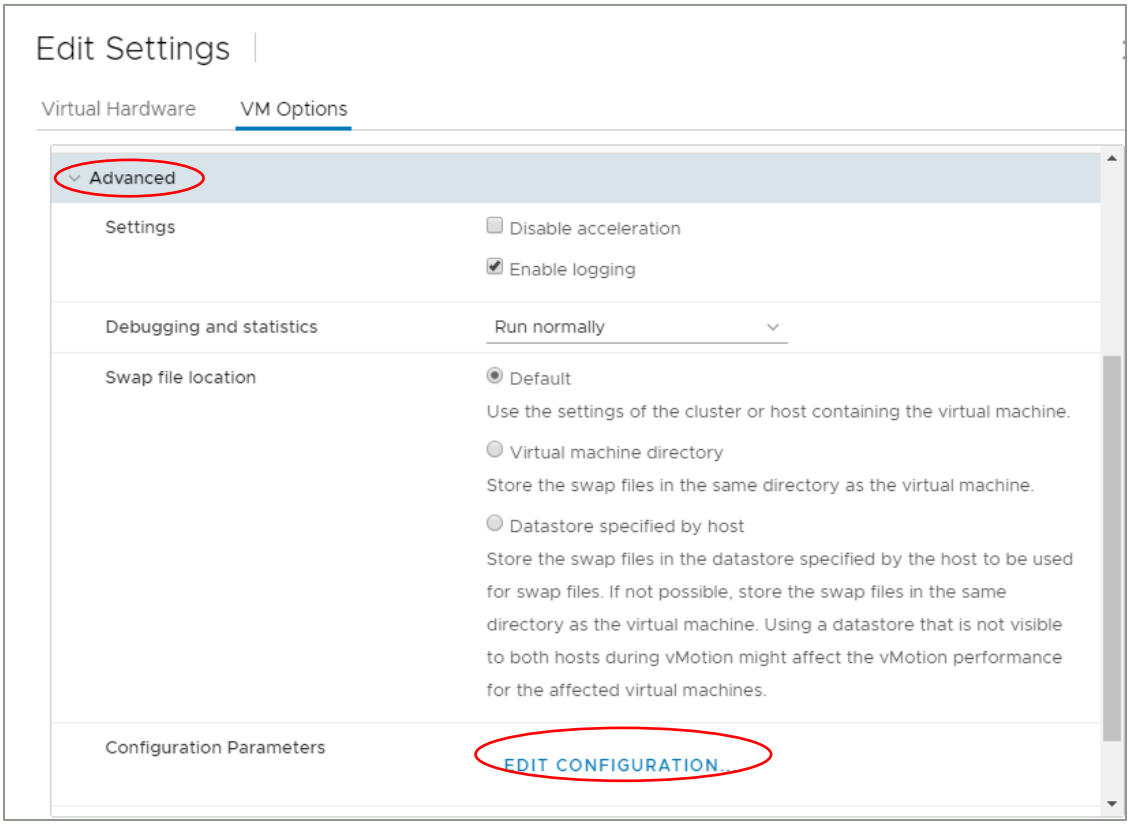
For example -> `./NicraSetup.sh 2>&1 | tee NicraSetup_out`

5. Remove the temporary IP configured and make it zeros as shown below in the network file.

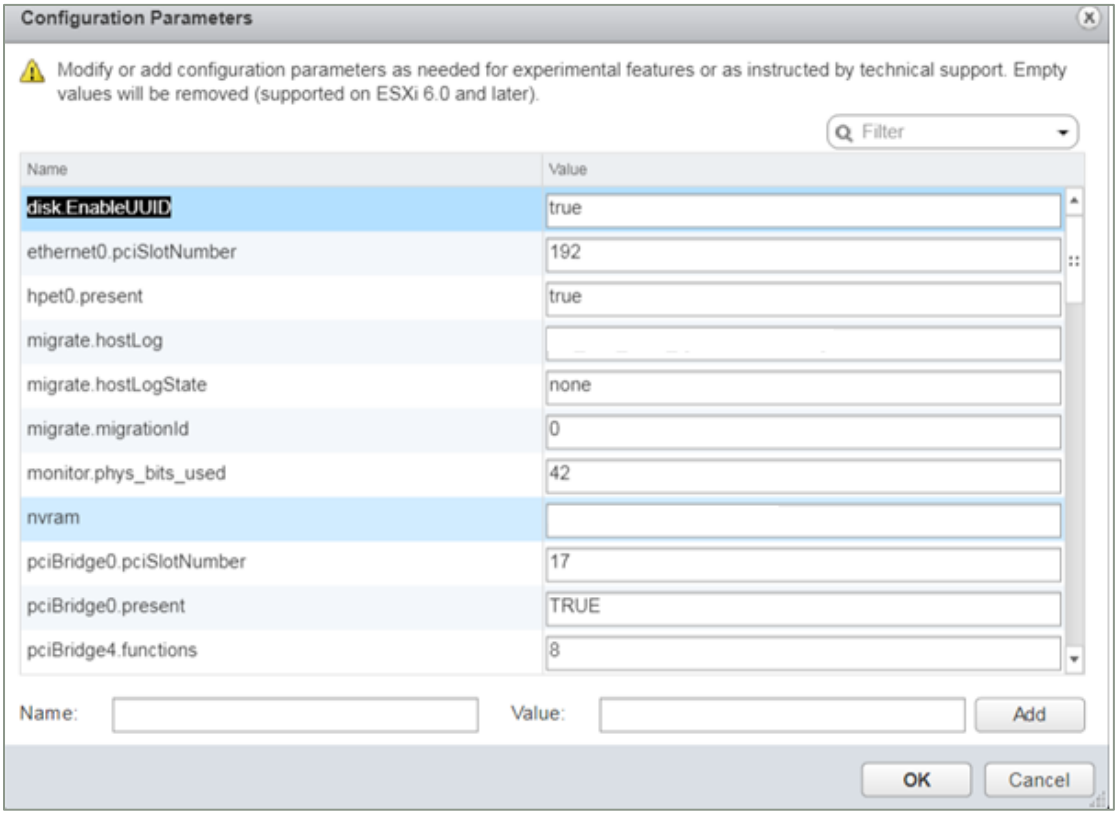


6. Power off the VM Created from vCen
7. Go to **Edit settings** of the VM. Navigate to VM Options > Advanced.

   Click on **EDIT CONFIGURATION...**

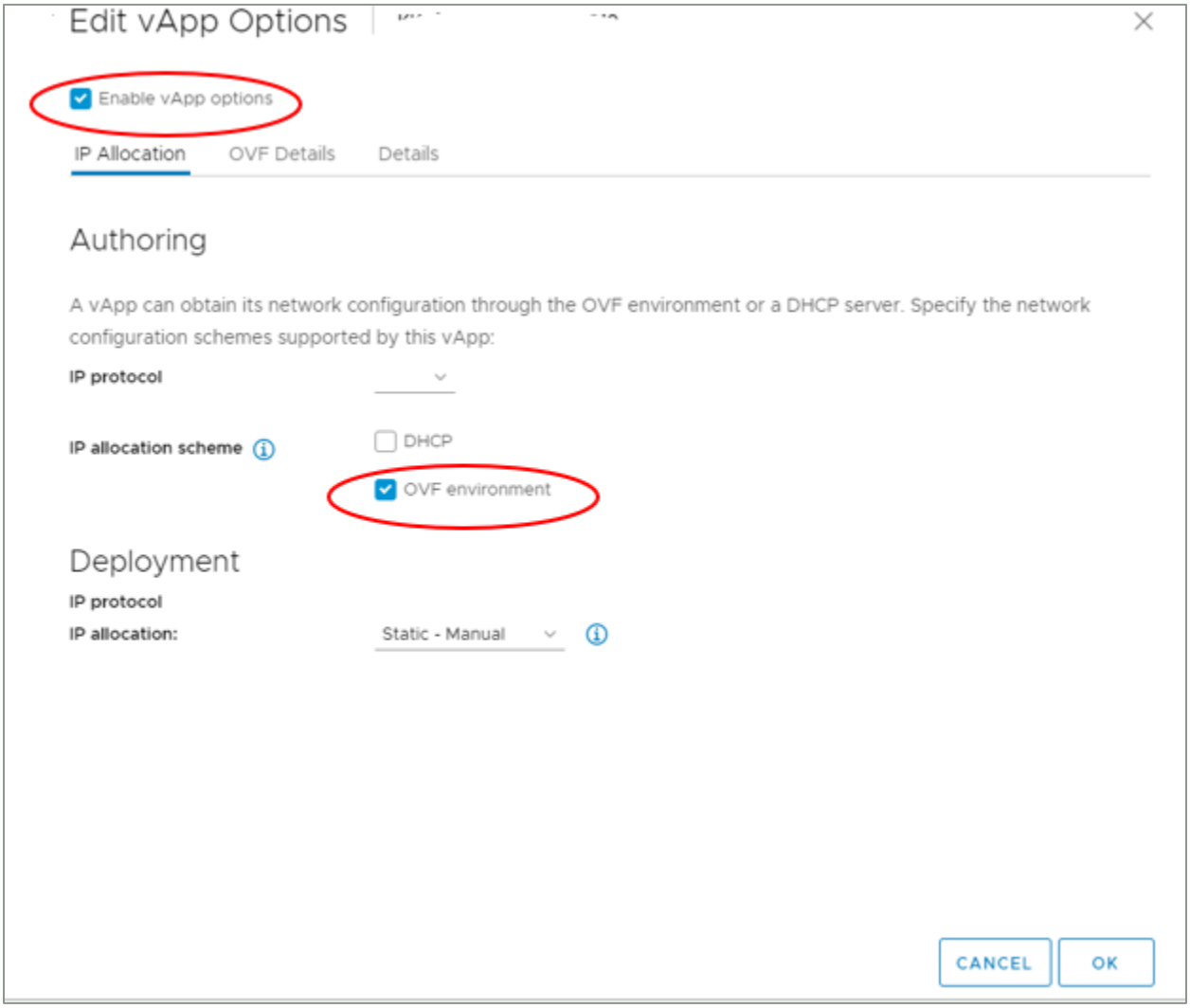


8. Add the Configuration parameters in the new windows by clicking on **Add** push button as à Name: "**disk.EnableUUID" Value: "true"** is shown below. Click on **OK**.

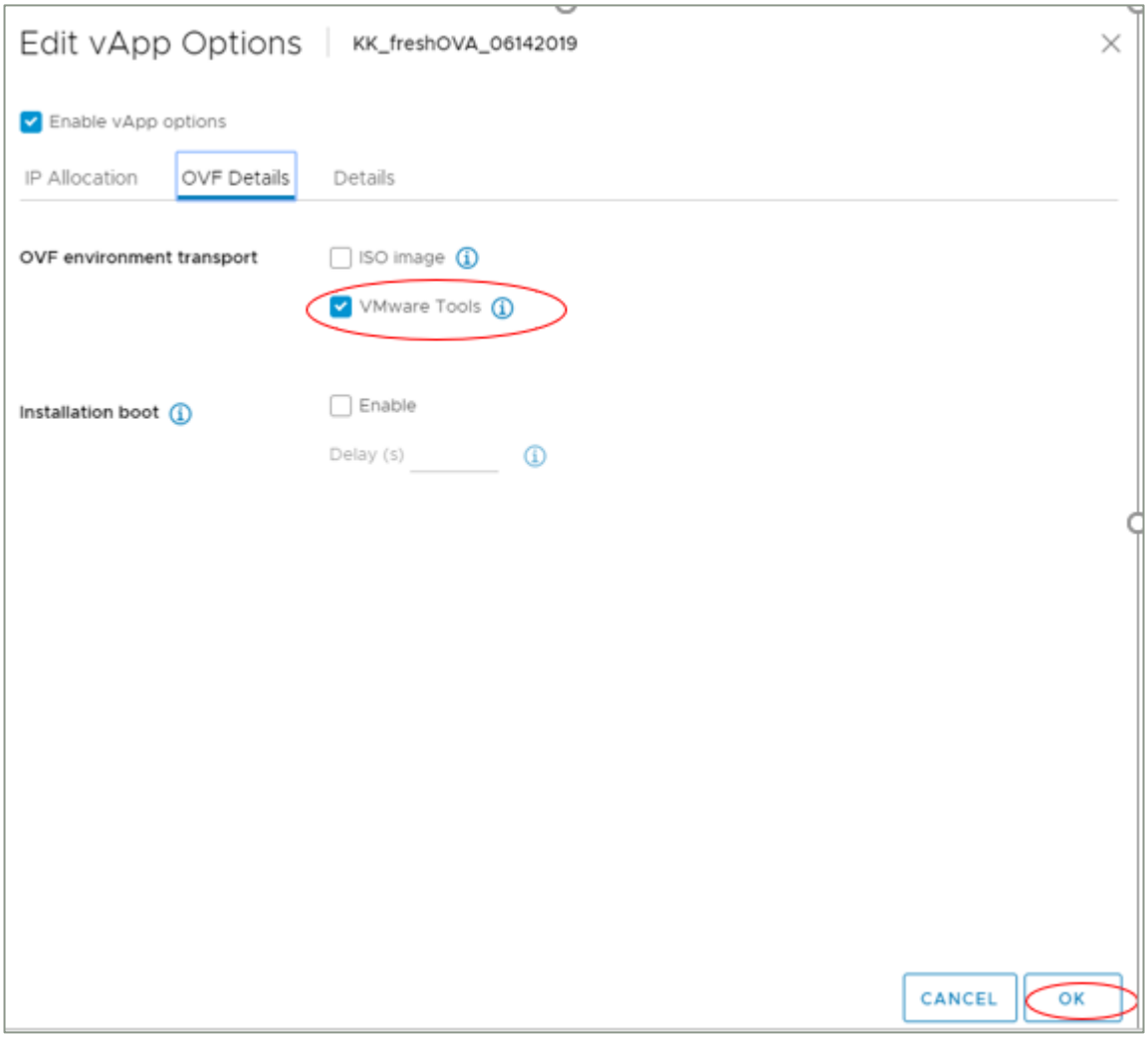


9. For the same VM, go to the "Configure" option in the vCenter and click on the "Edit" button.

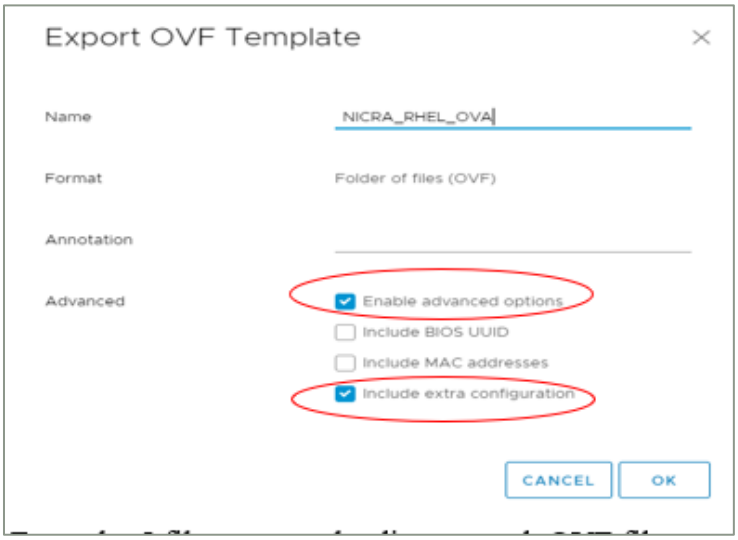
10. In the new window, select "Enable vApp Options" and "OVF environment". Allocation" tab.



11. In the same window, go to the OVF Details tab and select the check box for the "VMware Tools" option. Click the "OK" push button to close the window.



12. Export OVF from vCenter of the above-created VM. In the Advanced category select "Enable advanced options" and "Include extra configuration" and click OK.



13. From the 5 files exported, edit the exported.OVF file as described below and save it. This would include the Vapp parameters.

    Replace complete <ProductSection> above </VirtualSystem> as shown in figure below.

```
    <ProductSection>
      <Info>Information about the installed software</Info>
      <Category>IP</Category>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_ip">
        <Label>ovfenv_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_netmask">
        <Label>ovfenv_netmask</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_DMC_ip">
        <Label>ovfenv_DMC_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_hostname">
        <Label>ovfenv_hostname</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_gateway">
        <Label>ovfenv_gateway</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_port">
        <Label>ovfenv_port</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_dns_servers">
        <Label>ovfenv_dns_servers</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_ESXi_ip">
        <Label>ovfenv_ESXi_ip</Label>
        <Description/>
      </Property>
    </ProductSection>
  </VirtualSystem>
</Envelope>
```

By copying this content to the .ovf file:

14. Add the below section in the .ovf file for natip/fqdn

```
<Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_natip">
                <Label>ovfenv_natip</Label>
                <Description/>
        </Property>
```

Part-1

```
    <ProductSection>
      <Info>Information about the installed software</Info>
      <Category>IP</Category>
```

```
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_ip">
        <Label>ovfenv_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_netmask">
        <Label>ovfenv_netmask</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_DMC_ip">
        <Label>ovfenv_DMC_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_hostname">
        <Label>ovfenv_hostname</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_gateway">
        <Label>ovfenv_gateway</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_port">
        <Label>ovfenv_port</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_dns_servers">
        <Label>ovfenv_dns_servers</Label>
        <Description/>
      </Property>
```

```
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_ESXi_ip">
        <Label>ovfenv_ESXi_ip</Label>
        <Description/>
      </Property>
    </ProductSection>
```

Part-2

- Also, update the **NetworkSection** in the OVF file with VM Network details to enable the NICRA/SA deployment

```
  <NetworkSection>
    <Info>The list of logical networks</Info>
    <Network ovf:name="VM Network">
      <Description>The VM Network network</Description>
    </Network>
  </NetworkSection>
```

- Also, find and update in one of the <Item> sections for the **Connection** field as below with "VM Network"

```
<rasd:Connection>VM Network</rasd:Connection>
```

15. To update the vmdk size, copy all 5 exported files from the above step to some Linux VM and follow the below steps:

a) Run the command "ls -ltr" to find the vmdk sizes

Example output:

```
[root@localhost OVA_new]# ls -ltr NICRA_OVA_*.vmdk
-rw-r--r--. 1 root root     68096 Jul 23 06:42 OVA-2.vmdk
-rw-r--r--. 1 root root    220160 Jul 23 06:42 OVA-3.vmdk
-rw-r--r--. 1 root root 693826560 Jul 23 06:44 OVA-1.vmdk
```

b) Edit.OVF file and update the <References> tag with the ovf:size parameters captured above as shown in the below example with the corresponding VMDK.

From -

```
<References>
   <File ovf:id="file1" ovf:href="OVA-1.vmdk"/>
   <File ovf:id="file2" ovf:href="OVA-2.vmdk"/>
```

```
    <File ovf:id="file3" ovf:href="OVA-3.vmdk"/>
</References>
```

To – update ovf:size

```
<References>
    <File ovf:id="file1" ovf:href="OVA-1.vmdk"
    ovf:size="693826560"/>
    <File ovf:id="file2" ovf:href="OVA-2.vmdk" ovf:size="68096"/>
    <File ovf:id="file3" ovf:href="OVA-3.vmdk"
    ovf:size="220160"/>
    </References>
```

16. Since we have modified the content in the.OVF file in the above step, we need to update the shasum of the .OVF in the .mf(manifest) file as shown below in the same Linux VM.

    a) Run the command to find the modified shasum-> shasum -a 256 <.ovf file>

```
e.g. [root@localhost OVA_new]# shasum -a 256 OVA.ovf
7abc1212b2d1689377294a12bd55c235cd7ca767625356d9b5bb446530758711
OVA.ovf
```

    b) Check the shasum in the .mf for the OVF files., as it is different below in the manifest file generated.

```
[root@localhost freshOVA]# cat OVA.mf
SHA256(OVA-1.vmdk)=
b84f738318969f58459b8acfb5759b874393399b632e3c7dcfebd1a2509a22a2
SHA256(OVA-3.vmdk)=
dc702bd2f01223a017635d03926ab6ee446bf501b4572e3e995d2f9d67342f38
SHA256(OVA-2.vmdk)=
9616bf8fb2e93a1539dba3afabf02614696f872f550c4818fd1711e5de663947
SHA256(OVA.ovf)=
0f90b40a8c82dc3f22fe9e7c5ab166851a6d3726e31a7e4c96a407fd31bc21a8
```

    c) Replace the shasum of the .ovf file in the manifest file with the one calculated in step a.

```
[root@localhost freshOVA]# cat OVA.mf
SHA256(OVA-1.vmdk)=
b84f738318969f58459b8acfb5759b874393399b632e3c7dcfebd1a2509a22a2
```

```
SHA256(OVA-3.vmdk)=
dc702bd2f01223a017635d03926ab6ee446bf501b4572e3e995d2f9d67342f38

SHA256(OVA-2.vmdk)=
9616bf8fb2e93a1539dba3afabf02614696f872f550c4818fd1711e5de663947

SHA256(OVA.ovf)=
7abc1212b2d1689377294a12bd55c235cd7ca767625356d9b5bb446530758711
```

17. Create a file with the edited. ovf, .vmdk, .mf files to single OVA file format.
18. This OVA tar file is ready for NICRA deployment.

Note: Follow the same procedure to create Staging Appliance OVA also.

If the user wants to deploy the NICRA on 6.7 ESXi, the OVA needs to be created in 6.7 ESXi itself, to maintain the vmx version. The same applies to other versions of ESXi.

This chapter outlines the procedures for installing the Kyndryl Resiliency Orchestration Server OVA.

Kyndryl Resiliency Orchestration Server OVA software is delivered as the following file:

ResiliencyOrchestration_OVF10.ova: Kyndryl Resiliency Orchestration Virtual Appliance for VMware

18.2 Minimum System Requirements

The following are the minimum system requirements for Kyndryl Resiliency Orchestration Server.

- 2 vCPU
- 8 GB Memory
- 100 GB Hard Disk

18.3 Assumptions

It is assumed that the administrator who is installing and configuring Kyndryl Resiliency Orchestration Software is familiar with administering Cisco UCS Director Software including restarting UCS

Director services by accessing the UCS Director shell.

18.4 Installing Resiliency Orchestration Server Virtual Appliance for VMWare

18.4.1 Prerequisites

- You need administrator privileges to connect to VMware vSphere
- If you do not want to use DHCP, you need the following information: IP address, subnet mask, and default gateway.

18.5 Installation Procedure

1. Log in to vCenter using the VMware vSphere Client
2. In the Navigation pane, choose the Data Center for Kyndryl Resiliency Orchestration Server deployment.
3. Choose **File >Deploy OVF Template**.

   The Deploy OVF Template window appears.
4. In the Source pane, browse to the location where KyndrylRO_8.2.6.**ova is** located, choose the file, and click Open.
5. In the OVF Template Details pane, verify the details and click Next.
6. On the End User License Agreement page, read the license agreement, and click **Accept**.
7. In the Name and Location pane, enter the name for the VM and choose the Data Center where Kyndryl Resiliency Orchestration should be deployed
8. In the Host/Cluster pane, choose the required host, cluster, or resource pool, and click Next.
9. In the Datastore pane, choose the location to store Kyndryl Resiliency Orchestration VM files, and click Next.
10. In the Disk Format pane, choose one of the following radio buttons and click Next to create disks:
    - Thin Provisioned format—To allocate storage on demand as data is written to disk.
    - Thick Provisioned (Lazy Zeroed) format —To allocate storage immediately in thick format.
    - Thick Provisioned (Eager Zeroed) format —To allocate storage in thick format. It might take longer
12. In the Network Mapping pane, choose your network and click Next.
13. In the IP Address Allocation pane, leave the fields blank for DHCP, or enter the values for static IP

14. Click Next.
15. In the Ready to complete pane, verify the options selected, and click Finish.
16. Power on the VM once the upload is completed.

18.6 Creating NICRA/SA OVA Manually (RHEL 7.6)

Creating NICRA/SA OVA Manually (RHEL 7.6)

You can create the NICRA/SA Ova manually or automatically via a script.

- To create NICRA/OVA manually, refer to the topic Creating Nicra/SA OVA Manually.
- To create NICRA/OVA automatically with a script, refer to the topic Creating NICRA/SA OVA Using Automation Script.

Prerequisite:

You must have RHEL 7.6 OS (kernel 3.10.0-957) installed in a Virtual Machine.

Note: If RHEL7.6 OS Volume is under Linux-based LVM volumeGroup management, the LVM VolumeGroup name should be different from that of workload VM volumeGroup.

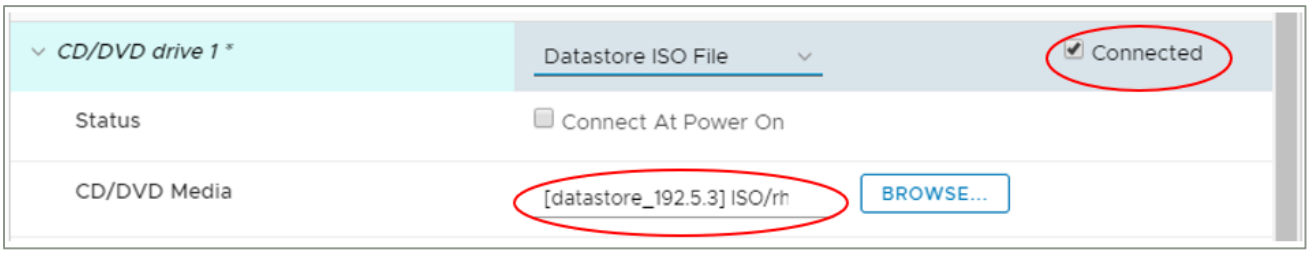
VM configuration required is as listed below:

- 8 vCPU
- 8 GB RAM,
- 16 GB VMDK disk for OS disk,
- 1 GB VMDK disk for Persistent Store (Kyndryl RBR requirement),
- 15 GB VMDK for Journal Disk (Kyndryl RBR requirement),
- 4 x SCSI controller and
- 1 temporary IP (to copy the NICRA bundle to VM)

- In case you would want to deploy the below created NICRA OVA in 6.7 ESXi, it is mandatory to generate NICRA OVA in 6.7 ESXi (To ensure the VM version is 14). The same condition applies to all ESXi versions.

Note:

- For NICRA/SA OVA upgrade, refer to the topic **Upgrading NICRA/Staging Appliance** in **VM Protection with Kyndryl Resiliency Block Replicator** user guide.
- In the VM "Edit Settings" for CD/DVD Media, make sure to select the same .iso image used for RHEL OS installation. Select the "connected" option checkbox for the CD/DVD drive as shown in the below snapshot. It will be used for LSB installation later.



Steps

1. Copy the Kyndryl Resiliency Block Replicator-NICRA.tar available in passport advantage to /opt directory in the VM created. This NICRA bundle contains:

   d) NICRA rpm - Latest RPM

   e) NicraSetup script - which installs rpm and runs prerequisites required.

   f) Firstboot script - Enables for deployment.

2. Untar the NICRA bundle, to extract the files required for OVA creation.

3. Make a note of the network interface in your VM by running the command "ifconfig -a".

```
[root@localhost ~]# ifconfig -a
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 192.168.5.84  netmask 255.255.255.255  broadcast 192.168.5.84
inet6 fe80::d7fe:e545:70e6:b62c  prefixlen 64  scopeid 0x20<link>
ether 00:50:56:a8:ed:d9  txqueuelen 1000  (Ethernet)
```

```
RX packets 83838  bytes 663793721 (633.0 MiB)
RX errors 0  dropped 20  overruns 0  frame 0
TX packets 85109  bytes 664728852 (633.9 MiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

If the network interface is not ens161 in your deployed VM, use the below sed command to replace it with the one (ens192) which is present in your VM. This will update the first boot.sh script with your network interface.

For example, to update ens192 in the firstboot.sh ☐ sed -i 's/ens161/ens192/g' firstboot.sh

3.1. Boot option is not mentioned.

Here we have two optiions available, Right CLick on VM > Edit Setting > VM Options > Boot Options

- EFI (Recomended)

- BIOS

We have to set BIOS as the boot option.

3.2. Removal of ipv6

Kindly disable ipv6. Only allow IPv4.

Disable ipv6 setting:

https://www.thegeekdiary.com/centos-rhel-7-how-to-disable-ipv6/

1. Edit /etc/default/grub and add ipv6.disable=1 in line GRUB_CMDLINE_LINUX, e.g.:

cat /etc/default/grub

GRUB_CMDLINE_LINUX="ipv6.disable=1 crashkernel=auto rhgb quiet"

2. Regenerate a GRUB configuration file and overwrite existing one:

grub2-mkconfig -o /boot/grub2/grub.cfg

3. Restart system and verify no line “inet6” in “ip addr show” command output.

shutdown -r now

kyndryl

3.3. Following Installation pakages are mandatory,

1.gdb

#yum install gdb

2.crash utility

#yum install crash

3.kernel-modules-extra-4.18.0-305.el8.x86_64

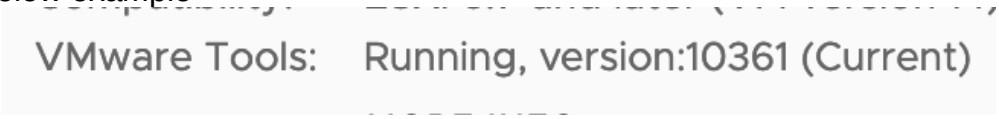
#yum install kernel-modules-extra-4.18.0-305.el8.x86_64

3.4. vmtoolsd - should be set with sbin i.e /usr/sbin/vmtoolsd

Note: With the latest vmtools it is found that vmtools is present inside /usr/bin/vmtoolsd

1.So to make the above change first we have to uninstall the latest vmtools.
2.Install the vm tools from VMwareTools-10.3.10-*

Example VMwareTools-10.3.10-12406962.tar.gz
3. Reboot
4. Check this command - "which vmtoolsd"
5. Now from the vCenter, upgrade the vmtools to current version. Something like below example



1.6 Remove unwanted packages as listed below

- yum remove gnome*
- yum remove qemu*
- yum remove libvirt *

4. Run the NicraSetup script.

For example -> ./NicraSetup.sh 2>&1 | tee NicraSetup_out

5. Remove the temporary IP configured and make it zeros as shown below in the network file.

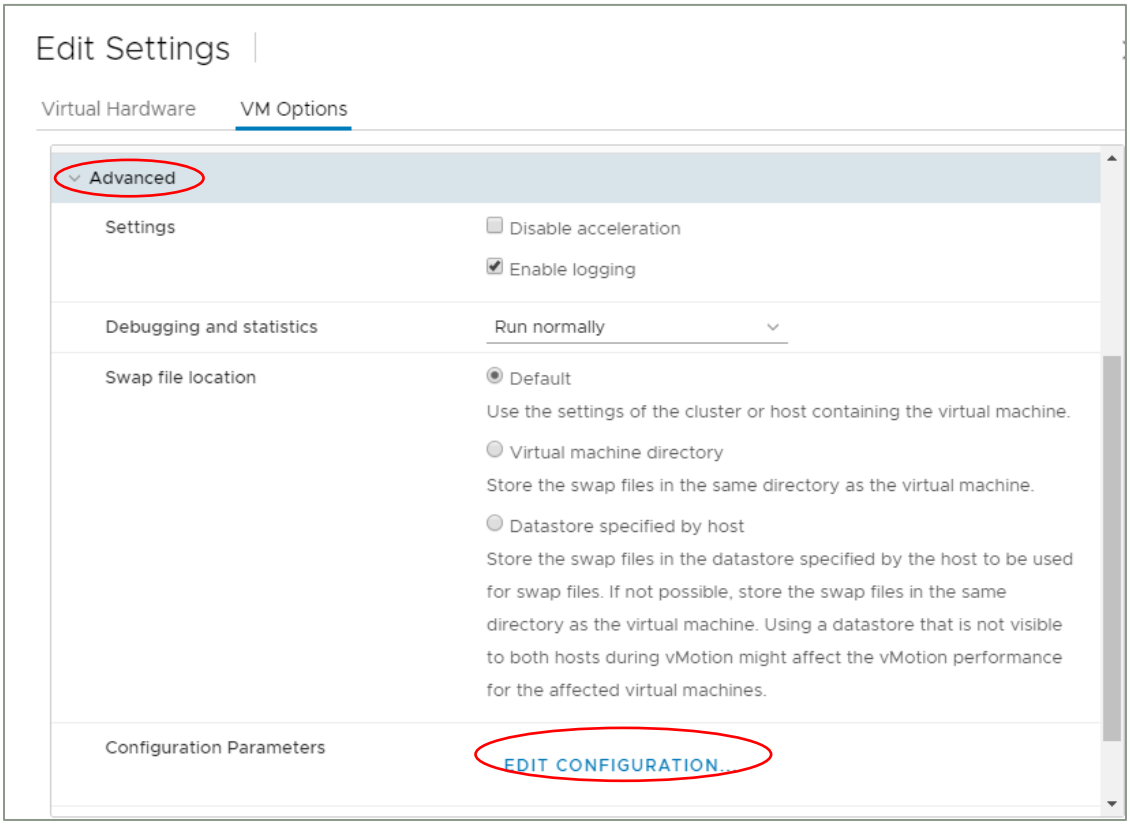
```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens161
#UUID=ed8a0030-98d7-4afe-80a9-96a8878ec101
DEVICE=ens161
ONBOOT=yes
IPADDR=0.0.0.0
PREFIX=0
GATEWAY=0.0.0.0
DNS1=0.0.0.0
~
```

6. Power off the VM Created from vCenter.

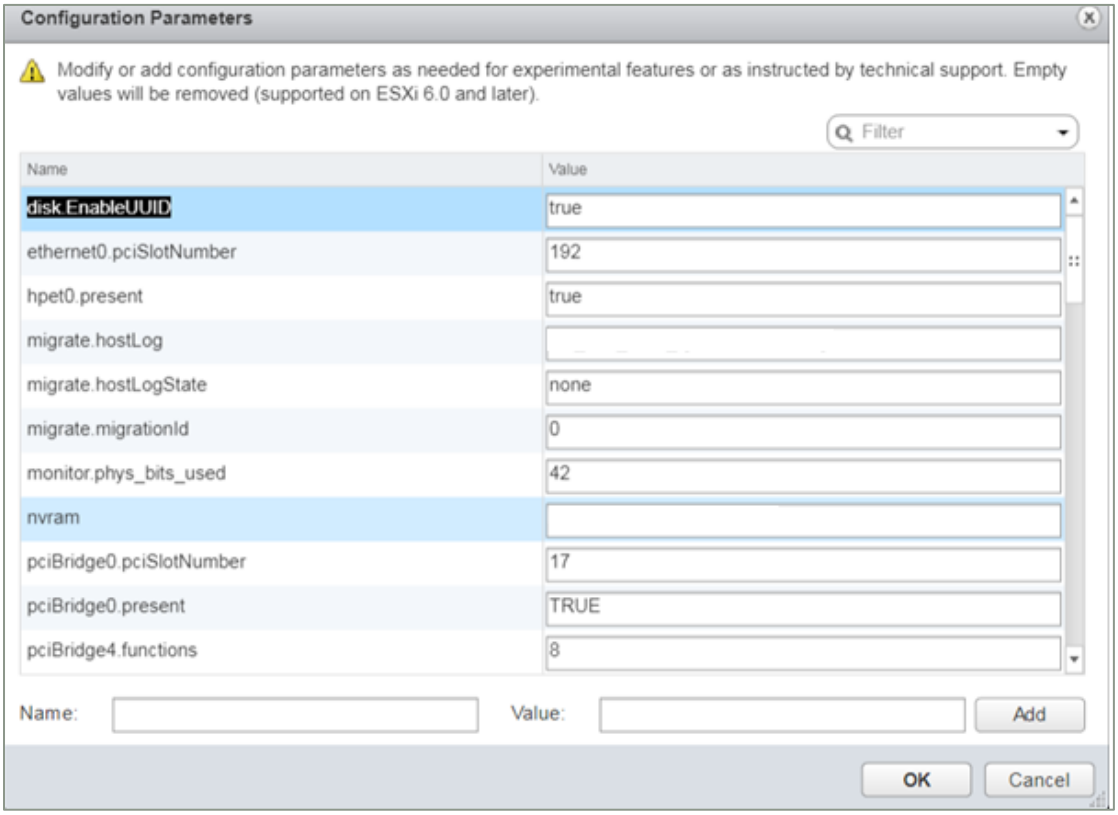
7. Disconnect the .iso mounted as mentioned in the Prerequisites section. Set CD/DVD drive to "Client Device".

8. Go to **Edit settings** of the VM. Navigate to VM Options > Advanced.

Click on **EDIT CONFIGURATION…**

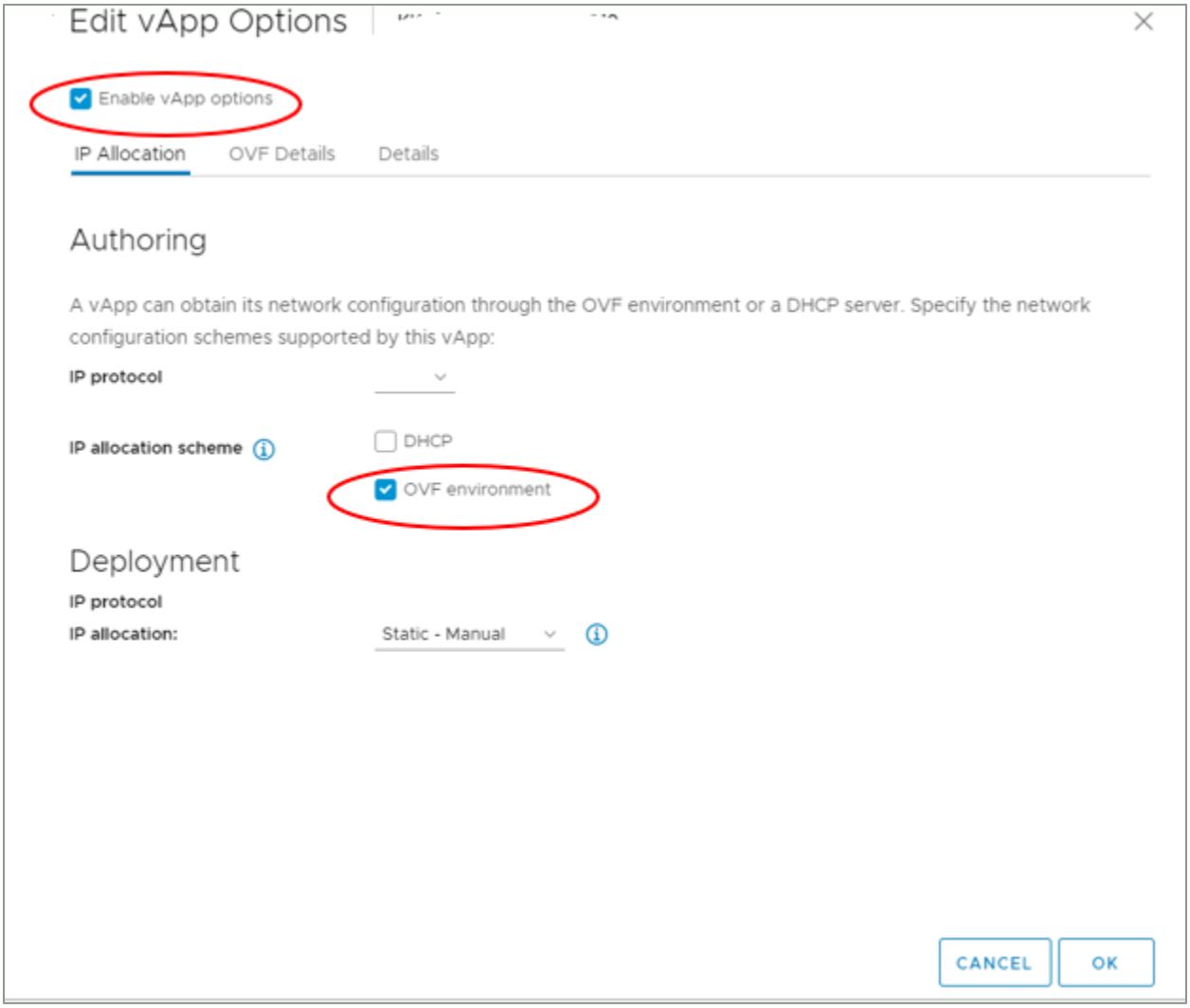


9. Add the Configuration parameters in the new windows by clicking on **Add** push button as à Name: "**disk.EnableUUID" Value: "true"** is shown below. Click on **OK**.

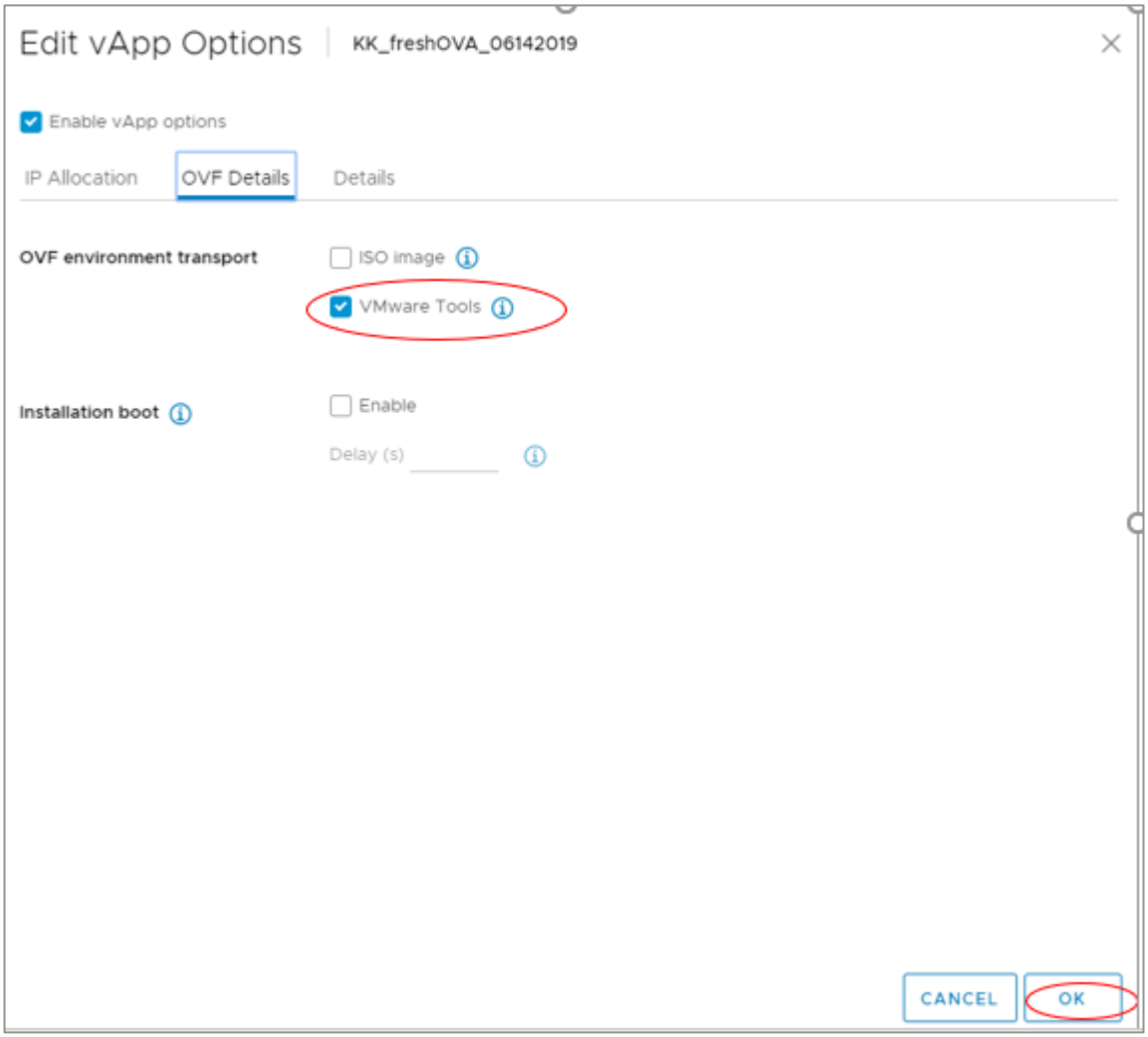


10. For the same VM, go to the "Configure" option in the vCenter and click on the "Edit" button.

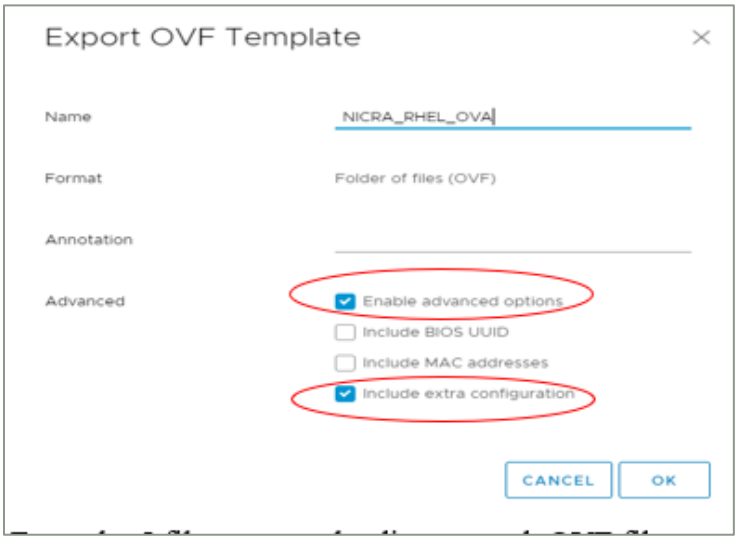
11. In the new window, select "Enable vApp Options" and "OVF environment". Allocation" tab.



12. In the same window, go to the OVF Details tab and select the check box for the "VMware Tools" option. Click the "OK" push button to close the window.



13. Export OVF from vCenter of the above-created VM. In the Advanced category select "Enable advanced options" and "Include extra configuration" and click OK.



14. From the 5 files exported, edit the exported.OVF file as described below and save it. This would include the Vapp parameters.

    Replace complete <ProductSection> above </VirtualSystem> as shown in figure below.

```
    <ProductSection>
      <Info>Information about the installed software</Info>
      <Category>IP</Category>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_ip">
        <Label>ovfenv_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_netmask">
        <Label>ovfenv_netmask</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_DMC_ip">
        <Label>ovfenv_DMC_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_hostname">
        <Label>ovfenv_hostname</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_gateway">
        <Label>ovfenv_gateway</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_port">
        <Label>ovfenv_port</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_dns_servers">
        <Label>ovfenv_dns_servers</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string" ovf:key="ovfenv_ESXi_ip">
        <Label>ovfenv_ESXi_ip</Label>
        <Description/>
      </Property>
    </ProductSection>
  </VirtualSystem>
</Envelope>
```

By copying this content to the .ovf file:

Part-1

```
    <ProductSection>
      <Info>Information about the installed software</Info>
      <Category>IP</Category>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_ip">
        <Label>ovfenv_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_netmask">
```

```
        <Label>ovfenv_netmask</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_DMC_ip">
        <Label>ovfenv_DMC_ip</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_hostname">
        <Label>ovfenv_hostname</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_gateway">
        <Label>ovfenv_gateway</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_port">
        <Label>ovfenv_port</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_dns_servers">
        <Label>ovfenv_dns_servers</Label>
        <Description/>
      </Property>
      <Property ovf:userConfigurable="true" ovf:type="string"
ovf:key="ovfenv_ESXi_ip">
        <Label>ovfenv_ESXi_ip</Label>
        <Description/>
      </Property>
    </ProductSection>
```

Part-2

- Also, update the **NetworkSection** in the OVF file with VM Network details to enable the NICRA/SA deployment

```
<NetworkSection>
  <Info>The list of logical networks</Info>
  <Network ovf:name="VM Network">
    <Description>The VM Network network</Description>
  </Network>
</NetworkSection>
```

- Also, find and update in one of the <Item> sections for the **Connection** field as below with "VM Network"

```
<rasd:Connection>VM Network</rasd:Connection>
```

15. To update the vmdk size, copy all 5 exported files from the above step to some Linux VM and follow the below steps -

b) Run the command "ls -ltr" to find the vmdk sizes

Example output:

```
[root@localhost OVA_new]# ls -ltr NICRA_OVA_*.vmdk
-rw-r--r--. 1 root root     68096 Jul 23 06:42 OVA-2.vmdk
-rw-r--r--. 1 root root    220160 Jul 23 06:42 OVA-3.vmdk
-rw-r--r--. 1 root root 693826560 Jul 23 06:44 OVA-1.vmdk
```

b) Edit .OVF file and update the <References> tag with the ovf:size parameters captured above as shown in the below example with the corresponding VMDK.

From -

```
<References>
   <File ovf:id="file1" ovf:href="OVA-1.vmdk"/>
   <File ovf:id="file2" ovf:href="OVA-2.vmdk"/>
   <File ovf:id="file3" ovf:href="OVA-3.vmdk"/>
</References>
```

To – update ovf:size

```
<References>
```

```
<File ovf:id="file1" ovf:href="OVA-1.vmdk"
ovf:size="693826560"/>

<File ovf:id="file2" ovf:href="OVA-2.vmdk" ovf:size="68096"/>

<File ovf:id="file3" ovf:href="OVA-3.vmdk"
ovf:size="220160"/>

</References>
```

16. Since we have modified the content in the .OVF file in the above step, we need to update the shasum of the .OVF in the .mf(manifest) file as shown below in the same Linux VM.

    a) Run the command to find the modified shasum-> shasum -a 256 <.ovf file>

    ```
    e.g. [root@localhost OVA_new]# shasum -a 256 OVA.ovf

    7abc1212b2d1689377294a12bd55c235cd7ca767625356d9b5bb446530758711
    OVA.ovf
    ```

    b) Check the shasum in the .mf for the OVF files., as it is different below in the manifest file generated.

    ```
    [root@localhost freshOVA]# cat OVA.mf

    SHA256(OVA-1.vmdk)=
    b84f738318969f58459b8acfb5759b874393399b632e3c7dcfebd1a2509a22a2

    SHA256(OVA-3.vmdk)=
    dc702bd2f01223a017635d03926ab6ee446bf501b4572e3e995d2f9d67342f38

    SHA256(OVA-2.vmdk)=
    9616bf8fb2e93a1539dba3afabf02614696f872f550c4818fd1711e5de663947

    SHA256(OVA.ovf)=
    0f90b40a8c82dc3f22fe9e7c5ab166851a6d3726e31a7e4c96a407fd31bc21a8
    ```

    c) Replace the shasum of the .ovf file in the manifest file with the one calculated in step a.

    ```
    [root@localhost freshOVA]# cat OVA.mf

    SHA256(OVA-1.vmdk)=
    b84f738318969f58459b8acfb5759b874393399b632e3c7dcfebd1a2509a22a2

    SHA256(OVA-3.vmdk)=
    dc702bd2f01223a017635d03926ab6ee446bf501b4572e3e995d2f9d67342f38

    SHA256(OVA-2.vmdk)=
    9616bf8fb2e93a1539dba3afabf02614696f872f550c4818fd1711e5de663947

    SHA256(OVA.ovf)=
    7abc1212b2d1689377294a12bd55c235cd7ca767625356d9b5bb446530758711
    ```

17. Create a file with the edited. ovf, .vmdk, .mf files to single OVA file format.
18. This OVA tar file is ready for NICRA deployment.

Note: Follow the same procedure to create Staging Appliance OVA also.

If the user wants to deploy the NICRA on 6.7 ESXi, the OVA needs to be created in 6.7 ESXi itself, to maintain the vmx version. The same applies to other versions of ESXi.

18.7 Post OVA deployment

Please find below the steps which we need to follow post OVA deployment –

1. Post OVA deployment Nicra shows multiple IPs, VMDK Discovery will fail due to multiple IP issues, so need to flush IP other than Nicra which we used during OVA deployment, use the below command to flush another IP-

```
Ip addr flush <network device name>
```

2. Need to disable SE Linux if it is set as enforced.

3. Go to /etc/selinux/config and modify it as disable.

Note: Above changes are specific to RHEL 8.4 NICRA only

18.8 Creating NICRA/SA OVA Using Automation Script

Steps

1. Copy and extract the latest "Kyndryl_Resiliency_Block_Replicator_x.x.x.tar" on Linux or Windows machines.

2. Follow the instructions given in the document "CREATE_NICRA_OVA_README_x.pdf" to create the OVA using an automation script.

   Note: This document is available as a part of the RBR bundle.

kyndryl

19 Installing DMC on Windows Server

Prerequisite:

DMC Sizing:

Manager for replication running Microsoft Windows Server Edition 2019, 2016, deployed in a Windows VM, 1 per VMware vCenter for versions ESXi 6.5,6.7or 7.0 with the configuration as

- Eight vCPU (for initial 200 VM protection), 300 GB for OS disk, 16 GB RAM
- One static IP for DMC
- NET Framework 3.5 installed is a prerequisite

Steps

1. Download the DMC zip file from Passport Advantage to the Windows machine.
2. Mount DMC .iso file and open.
3. Double-click on the setup.exe file to install. This will initiate InstallShield Wizard for build installation.
4. Check the box for both Data Mobility Console and Collector Database. Then click **Next**.
5. The database will also be installed (Microsoft SQL Server 2012 Express SP4).
6. After the installation is complete.
7. Go to C:\Program Files (x86)\IBM\Data Mobility Console.
8. Run dmc.exe to launch the DMC CLI console and then connect to the localhost for further operations.

Summary of RBR Solution deployment:

i. if there are no windows VMs to be protected, there is no need for Windows SC.

ii. if there are Windows VMs involved then Windows SC needs to be deployed.

iii. As deployment optimization, this can be deployed on the same Windows Server where DMC is deployed.

20 Installing Resiliency Orchestration Site Dashboard

Kyndryl Resiliency Orchestration Site Dashboard is the licensed feature. You can install it in GUI mode only. It is supported only in the Linux platform, to be installed on Resiliency Orchestration Server.

20.1 Prerequisites

The following are the prerequisites for installing the Resiliency Orchestration site dashboard:

- Kyndryl Resiliency Orchestration Server should be already installed in the machine, else the installer will display an error and quit.
- The Google map API key has to be generated to use google maps. Refer to https://developers.google.com/maps/premium/prelaunch-checklist for details.

20.2 GUI Mode Installation of Resiliency Orchestration Site Dashboard

You need to perform the following steps to install the site dashboard:

1. Download the Site Dashboard binaries from the Kyndryl Passport Advantage site.
2. Kyndryl Resiliency Orchestration Site Dashboard can be installed only if you log in as a root user. Run the following command in the Site Dashboard folder.

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

   Note

   If server hardening has been performed, you need to mention sudo before the above command.

3. After executing the command, Kyndryl Resiliency Orchestration Site Dashboard installation starts with the **Kyndryl Resiliency Orchestration Site Dashboard Introduction** window is displayed as shown in the following figure:

4. After displaying the **Kyndryl Resiliency Orchestration Site Dashboard Introduction** screen, the Kyndryl Resiliency Orchestration **Software License Agreement** window is displayed as shown in the following figure:

kyndryl

> **Note**
>
> Click the Cancel button to quit the installation.

5. Click **Next**. The **Choose Tomcat home Folder** window is displayed as shown in the following figure:

6. Click **Choose...** to browse and select the location of Tomcat.
7. Click **Next**. The **Kyndryl Resiliency Orchestration IP Address** window is displayed as shown in the following figure:
8. Enter the IP address of the current machine.
9. Click **Next**. The **Kyndryl Resiliency Orchestration Google Apis Key** window is displayed as shown in the following figure:
10. Click **Next**. The **Kyndryl Resiliency Orchestration Pre-Installation Summary** screen is displayed as shown in the following figure:

> **Note**
>
> Read through the preinstallation summary to verify the inputs provided. If you want to change the inputs, click Previous and modify.

11. Click **Install**. The **Kyndryl Resiliency Orchestration Installing Site Dashboard** window is displayed.
12. After the installation is complete, the **Kyndryl Resiliency Orchestration Installation Completed** window is displayed indicating a successful installation.
13. Click **Done** to complete the installation process.

kyndryl

21 Installing the Resiliency Orchestration Agent Server in Silent Mode

The following section provides steps to install the software in silent mode on Windows, Linux, Solaris, HPUX, and AIX servers.

> **Note**
>
> In silent mode, uninstallation does not check if the services are running or not. You need to ensure that the stopped before uninstallation is in silent mode.

21.1 Installing Agent Server on Windows in the Silent Mode

Perform the following steps to install Kyndryl Resiliency Orchestration on the Windows system.

1. Log on to the Windows system.
2. Open an MS-DOS command prompt window.
3. Go to the directory that contains the installation file and launch the installation procedure by entering the following command:

```
install.exe -f <complete path of the .properties file with the properties file name>
```

For Example: `install.exe -f c:\\Progra~1\\panaces\\PanacesAgentsInstaller.properties`

> **Note**
>
> After completing the installation of Agents on Windows Server, no status is displayed. The user does not get information on whether the installation is successful or not.

21.2 Installing Agent Server on Solaris, Linux, HPUX, or AIX in the Silent Mode

1. Log on to Linux/Solaris/HPUX/AIX system.
2. Navigate to the directory that contains the installation file.
3. Launch the installation by entering the following command:

```
Sudo ./install.bin -f <complete path of the .properties file with the properties file name>
```

For example, enter the following command for agents:

```
Sudo ./install.bin -f /Agents/ PanacesAgentsInstaller.properties
```

kyndryl

You need to enter the following command for the server:

```
Sudo ./install.bin –f /Server/ PanacesServerInstaller.properties
```

> **Note**
>
> You have to manually start Kyndryl Resiliency Orchestration Server after installing the Kyndryl Resiliency Orchestration.

21.3 Vault Configuration

If you want to use Vault, make the following changes before starting Panaces service.

> **Note**
>
> Restart Panaces if Panaces is already started after the following changes.

1. Set parameter `IS_SERIALCALL_ENABLED=TRUE` in **<EAMSROOT>/installconfig/PanacesAgentGeneric.cfg**.

   By default, it is set as `FALSE`.

2. Make the changes for both the Agent and Resiliency Orchestration Services as

   PanacesAgentGeneric.cfg (Agent) and **panaces.properties** (Resiliency Orchestration Services).

3. Set parameter `sanovi.vault.agent.onstartup = TRUE` in **<EAMSROOT>/installconfig/panaces.properties**.

   By default, it is set as `FALSE`.

21.4 Post Upgrade Tasks

Since the mount TCL scripts are modified, the agents using the TCL scripts (HPXP solution) should also be upgraded along with the Resiliency Orchestration Server upgrade, or else the mount operations will fail.

After the successful upgrade of the server, the user should clear the browser cache for the GUI changes to take effect completely.

The comparison between previous roles and new role definitions in Basic User Management is given as follows:

The **OPERATOR** has **READ** privileges for all the pages including the Admin tab.

The **ADMINISTRATOR** can change their User Management information and cannot edit or view other users.

SUPER ADMINISTRATOR has all the privileges as in the previous releases.

NOTIFICATION MEMBER will not be allowed to login into the system.

SUPPORT USER will be able to modify his password on login.

The **support** user will be present and can function similarly to the Super admin except for user administration.

For customers who are upgrading, the new username is also reflected. The existing password will not be changed on the upgrade.

The **drmadmin** user will not be allowed to be deleted by other users with the **SUPER ADMINISTRATOR** role. Only newly created users with **SUPER ADMINISTRATOR** roles can be deleted.

The username field can accept up to 64 characters. The same will be reflected in the UI on the login page and create/edit user page.

If HA is available, perform the following tasks:

- Uninstall on Standby Resiliency Orchestration Server.
- Install on Standby Resiliency Orchestration Server. Do not refresh the schema/DB during installation. Do not start Resiliency Orchestration Services on Standby Server.
- Restart MariaDB Replication.
- Restore required custom workflows/scripts from the backup.
- Start the Kyndryl Resiliency Orchestration Server services.

21.5 Server Memory Management

Depending on the expected number of groups that will be supported by Kyndryl Resiliency Orchestration Software, Java's maximum heap memory limit parameter needs to be specified. It is defined in the variable named DRM_SERVER_JVM_MEM, which is located at starting lines of the Resiliency Orchestration startup script DRM Install root/bin/panaces. The default value of this variable is set to –Xmx2048m.

The following are the recommended values:

Configuration with more than 100 groups: -Xmx4096m is recommended.

21.6 Backup and Fallback Plan

21.6.1 Backup Plan

- Take the backup of the following files and directories:
- Run the enableEncryptionOnTables.sh script. Refer procedure to enableEncryptionOnTables.
- Kyndryl Server MariaDB Metadata

  sudo mysqldump -u root --databases panaces pfr -R --triggers > backupfilename.sql
- Kyndryl Server Installation directory $EAMSROOT
- The following system files:
  - sysctl.conf
  - any user-specific scripts and cron job entries
  - /etc/hosts
  - User files
- If Panaces Server is configured with Linux OS agent:
  - Agent Binaries
  - Custom / Field Specific scripts

21.6.2 Fallback Plan

At any time of the upgrade, if there are failures that cannot be corrected within the upgrade window, use the following plan to restore to the old Kyndryl server installation.

- Run the following command to drop the existing databases if they already exist:

```
sudo mysqladmin –u root drop panaces
sudo mysqladmin –u root drop pfr
```

- Restore the MariaDB Metadata from backup.

```
sudo mysql –u root < backupfilename.sql
```

- Restore the Kyndryl Server software installation directory.
- Start up Kyndryl Server Services.

22 Upgrading Resiliency Orchestration Agents

The upgrade of agents on customer servers may be done at any time after the Kyndryl Resiliency Orchestration Server software is upgraded.

22.1 Prerequisites

The following are prerequisites for upgrading Resiliency Orchestration Agents:

- All the agents need to be stopped before performing any agent upgrade process.
- Kill rsync.exe processes started by Panaces agents (PFR), if any.
- The user needs to add a permanent firewall rule to allow port 8081(jetty) and 8083(RMI)

> **Note**
>
> If the firewall is off, adding a permanent firewall rule is not required.

- The user needs chmod 744 permissions to upload binaries to the jackrabbit repository.

22.2 Resiliency Orchestration Agent Upgrade [Optional]

Refer to the respective agent upgrade chapters for upgrading the agents from the older version to the current version.

After the agent upgrade, all new workflows or the new actions that got defined in the field or bundled with current releases will work.

> **Note**
>
> Upgrading the agents will retain the existing workflow configuration files in the $EAMSROOT/work directory to maintain backward compatibility. If new workflows from the current version are loaded, they may not work with the existing workflow configuration files. A fresh copy of the configuration file must be copied from the *$EAMSROOT/scripts/repository/workflow-config* directory to the working directory and must be configured to be used by the workflow.

The following are the steps to upgrade the Resiliency Orchestration agent:

1. For each identified Functional Group, move the Group to maintenance mode.
2. Upgrade the agent software on all servers.

Refer online help for more information under the section Home > Discovery >Subsystem > Agent Upgrade > Agent Upgrade.

22.3 Upgrading Agents on Linux Server

22.3.1 Prerequisites before upgrading agents on Linux Server

1. Stop all the agents.
2. Make sure that you have free space of approximately 2.5 GB in /tmp directory, before executing the above command.

22.3.2 Limitations

- Agents should be upgraded first and then Kyndryl Resiliency File Replicator is upgraded, when Kyndryl Resiliency File Replicator is installed with agents.
- During the upgrade, use the old EAMSROOT as the installation path.

22.3.3 Upgrading Agents on Linux Server in GUI mode

Perform the following steps for upgrading the agents on Linux Server. The commands specified in the following points must be provided at the command prompt:

To upgrade the agents, perform the following steps:

1. Download the agent binaries from the Kyndryl Passport Advantage site.
2. Browse through Kyndryl Resiliency Orchestration software from the downloaded path and go to the folder Agent/Linux_DRMAgent_<release_version>.zip for 32-bit Linux Operating Systems or Agents/ Linux64_DRMAgent_<release_version>.zip for 64-bit Linux Operating Systems.
3. Go to the extracted folder and execute the following command: (Use whichever is applicable)

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

Note

Make sure that you have free space of approximately 2.5 GB in /tmp directory, before executing the above command.

In case /tmp directory does not have enough space, execute the below command so that installer will use the specified temporary directory.

Example-

Assuming you want to make /opt/temp as the temporary directory.

#export IATEMPDIR=/opt/temp

After exporting the IATEMPDIR environment variable, proceed with the installation.

The user should be root/administrator or have root/administrator privileges to install agents as the user should have access to the installation directory, /tmp directory, /etc/profile, etc.

4. After executing the command, the Kyndryl Resiliency Orchestration Agent installation starts with the following screen.
5. After displaying the Kyndryl Resiliency Orchestration Agent Installer screen, the Introduction window is displayed.

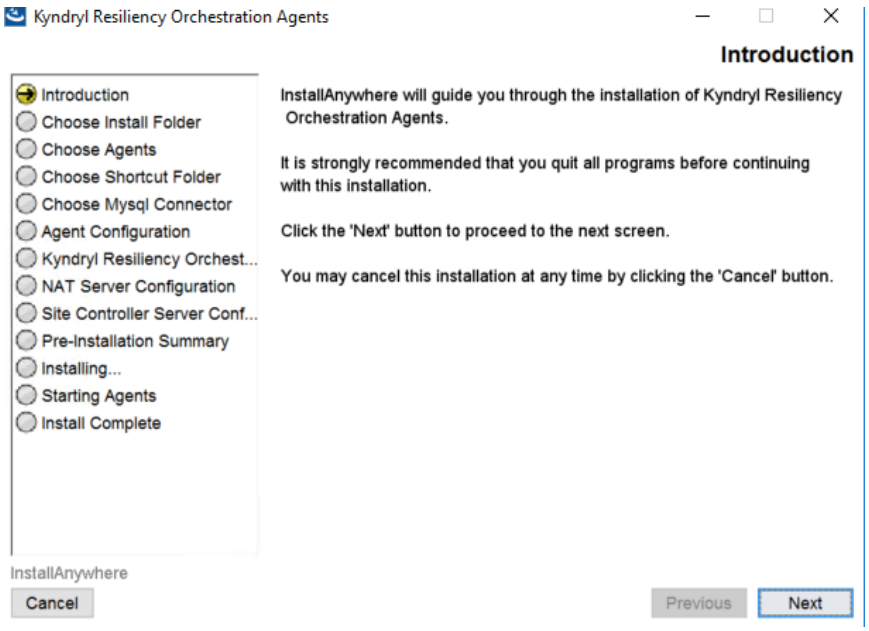


Figure 67: Upgrade Agents on Linux Server - Introduction

6. Go through the installation procedure and click **Next**. The **Choose Install Folder** window is displayed.

7. Select a path to install the software by clicking **Choose**. Alternatively, you can click **Restore Default Folder** to restore the default path. The default path is /**opt/panaces**. It is recommended that you use the default path. This needs to be the same as that of the previous agent installation.
8. Click **Next.** The **Choose Install Set** window is displayed. Select the **Upgrade** option and click **Next**
9. The **Choose Install Set** screen will be displayed only when the user selects the same install location as the current one.

Note:

Refer to the example figure which covers 6.3 to 7.1.

Please correlate to the current release to upgrade.

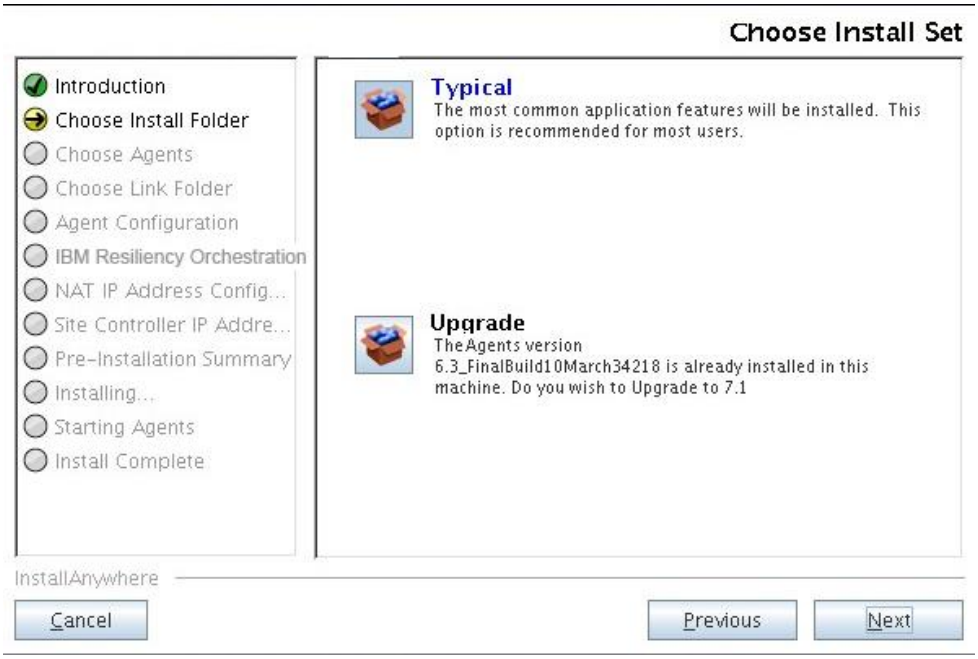


Figure 68: Upgrade Agents on Linux Server - Choose Install Set

10. The **Choose Agents - Linux** window is displayed.

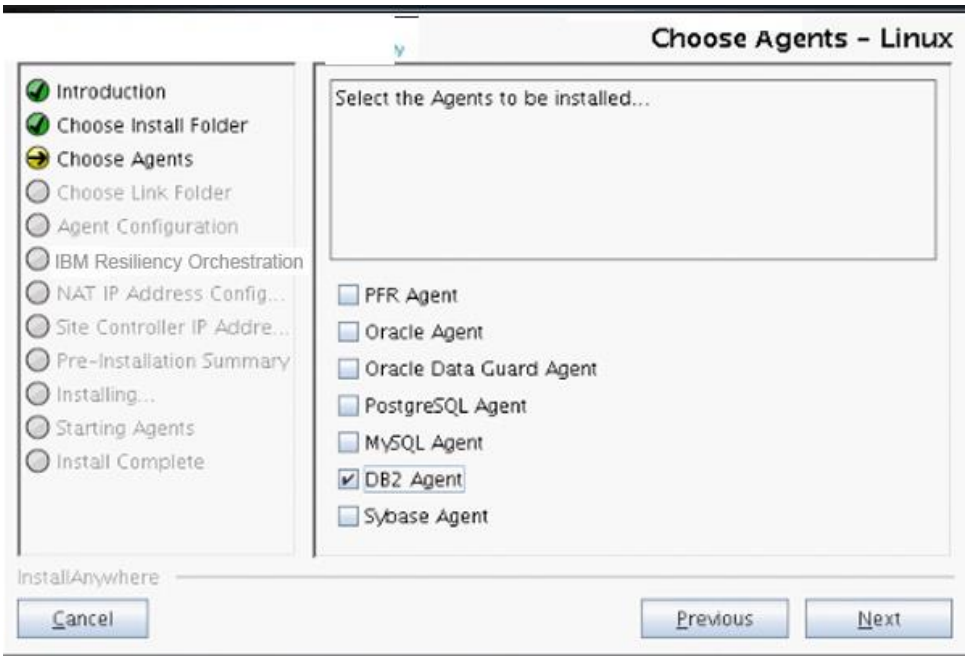


Figure 69: Upgrade Agents on Linux Server - Choose Agents - Linux

11. The list of agents available is displayed on the **Choose Agents - Linux** window. Select the checkbox next to the specific agent to install that agent. You can choose to install any or all of the agents.
12. Click **Next**. The **Choose Link Folder** window is displayed.

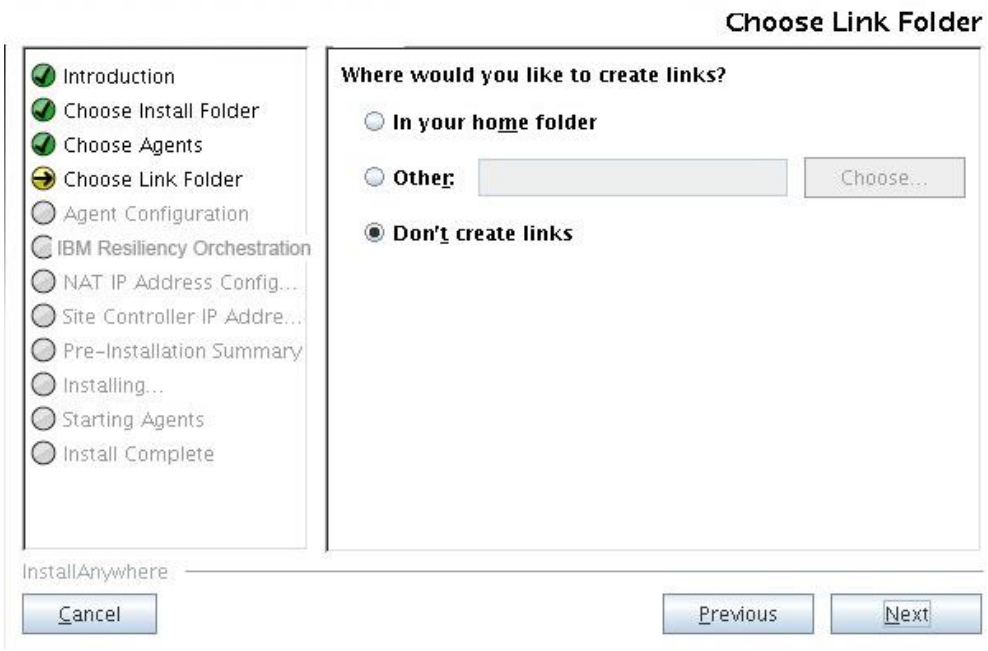


Figure 70: Upgrade Agents on Linux Server - Choose Link Folder

13. Choose a path for creating links in the **Choose Link Folder** window.
- Select **In your home folder** for creating a link in the home folder.
- Select **Other** to enter a specific path.
- Select **Don't create links** for not creating shortcut folders.

14. Click **Next.** The **Agent Configuration** window is displayed.

Figure 71: Upgrade Agents on Linux Server - Agent Configuration

15. Enter DB2 instance user login ID and click Next.

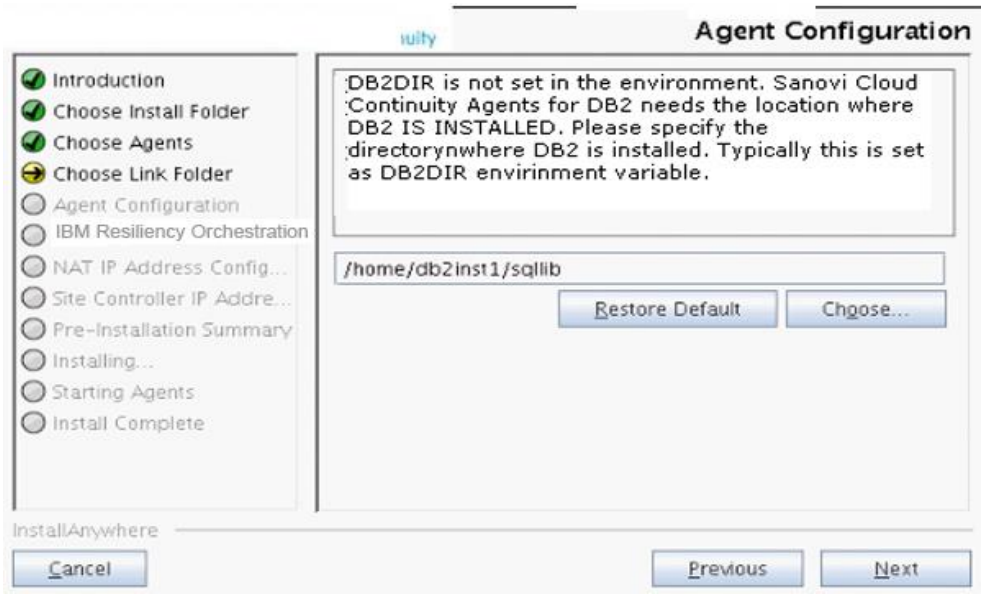


Figure 72: Upgrade Agents on Linux Server - Agent Configuration

16. Enter the DB2 file location. Click the **Choose** button to select the jar file location.
17. Click **Next**. The NAT IP Address Configuration window displays.

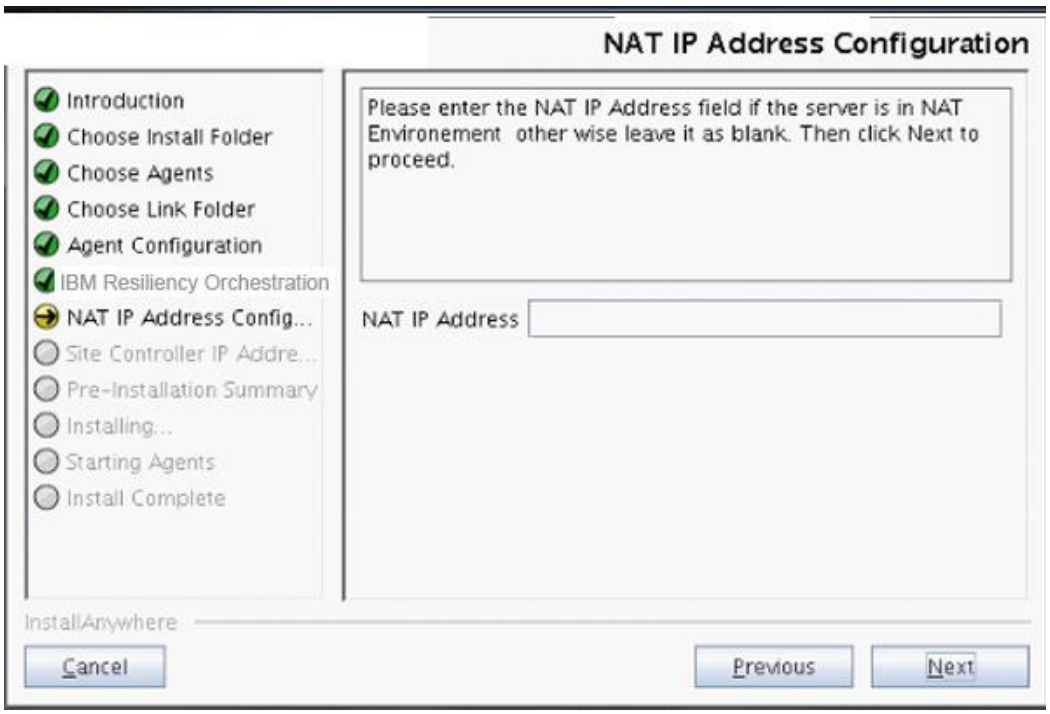


Figure 73: Upgrade Agents on Linux Server – NAT IP Address Configuration

18. Enter the **NAT IP Address** if applicable and click **Next**. The **Site Controller Configuration** window displays.

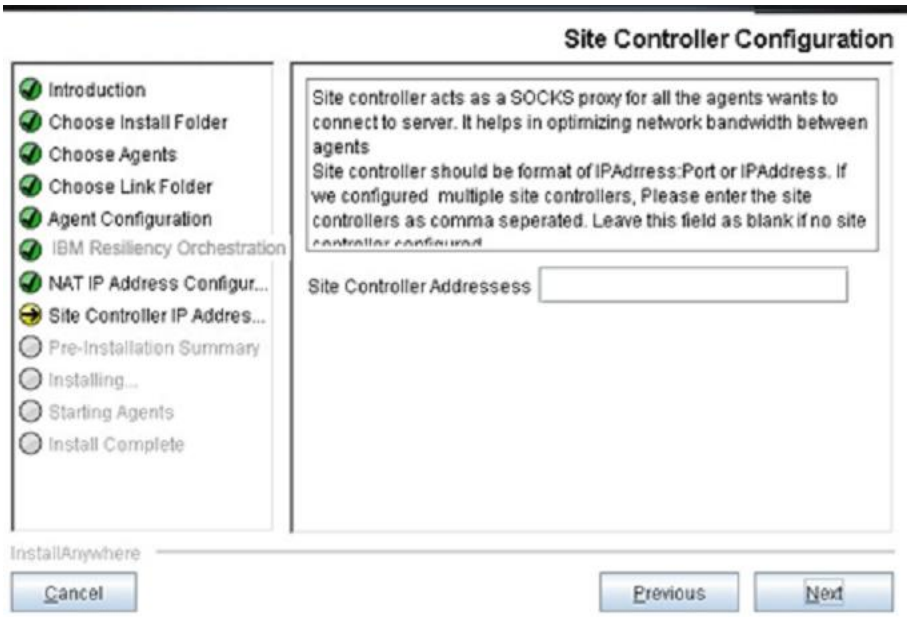


Figure 74: Upgrade Agents on Linux Server – Site Controller Configuration

19. Enter the **Site Controller IP Address/Name** as applicable and click **Next**. The **Pre-Installation Summary** window displays.

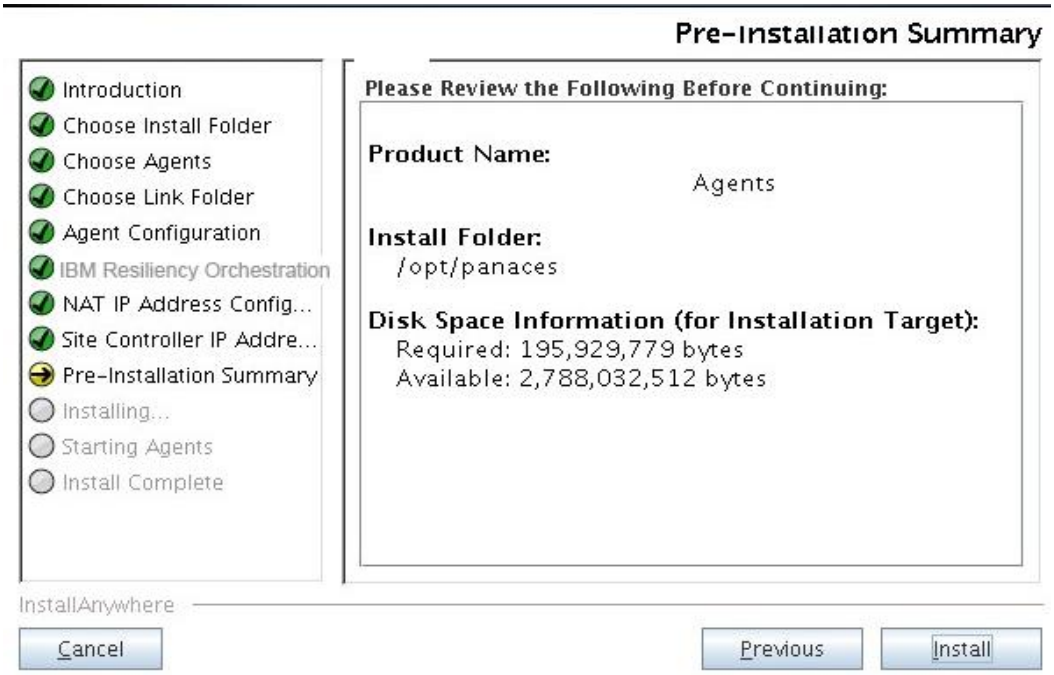


Figure 75: Upgrade Agents on Linux Server - Pre-Installation Summary

20. Go through the pre-installation summary to verify the inputs provided. If you want to change the inputs, click **Previous** and modify.
21. Click **Install**. The **Installing Kyndryl Resiliency Orchestration Agents** window is displayed.

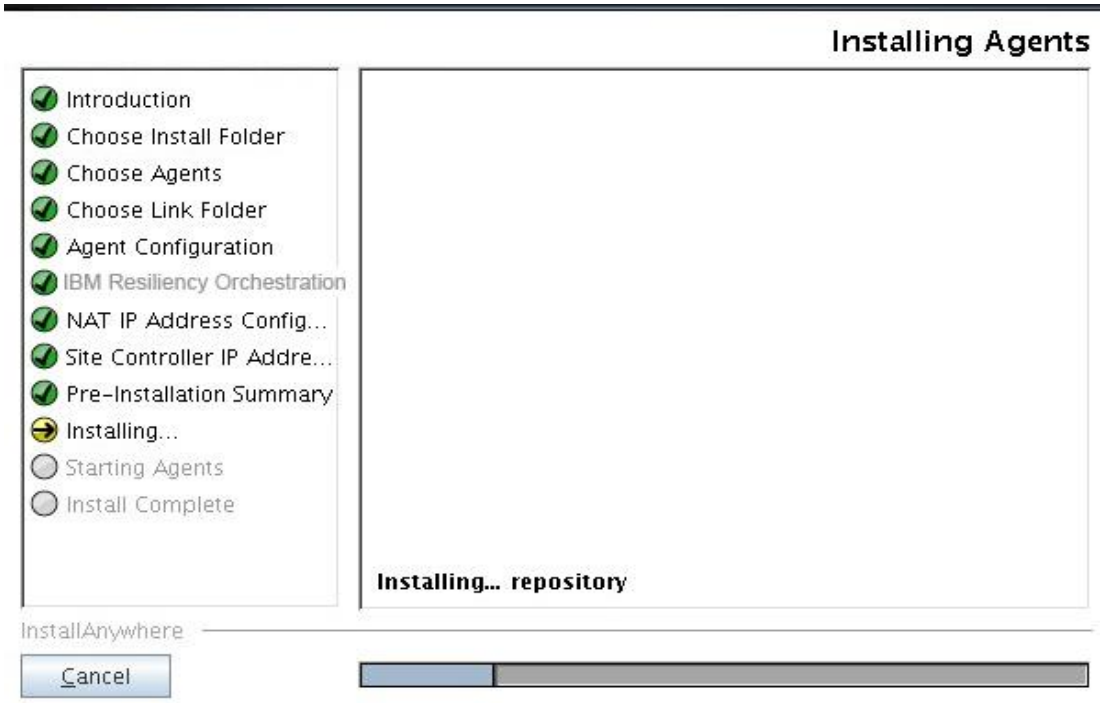


Figure 76: Upgrade Agents on Linux Server - Installing Kyndryl Resiliency Orchestration Agents

22. Once the installation is complete, the **Starting Agents** window is displayed.

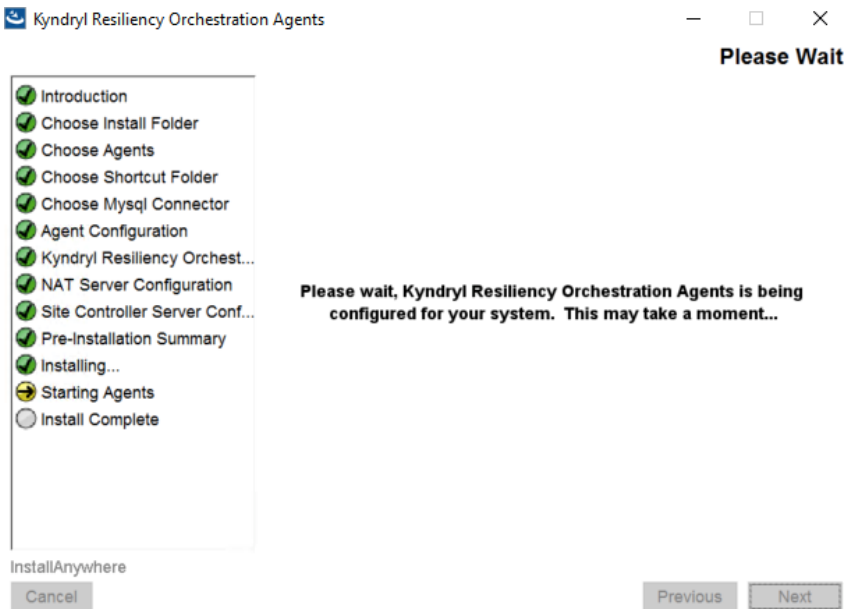


Figure 77: Upgrade Agents on Linux Server - Starting Agents

23. On the **Starting Agents** window, perform either of the following:

- Click **Yes** to start the agent services automatically.
- Click **No** to start the agent services manually.

> **Note**
>
> The best practice is not to change the default value displayed on the Starting Agents window.

24. Restart the agent machine, if the agents do not start after agent installation is complete.
25. Click **Next.** The **Upgrade Complete** window is displayed, indicating a successful upgrade.

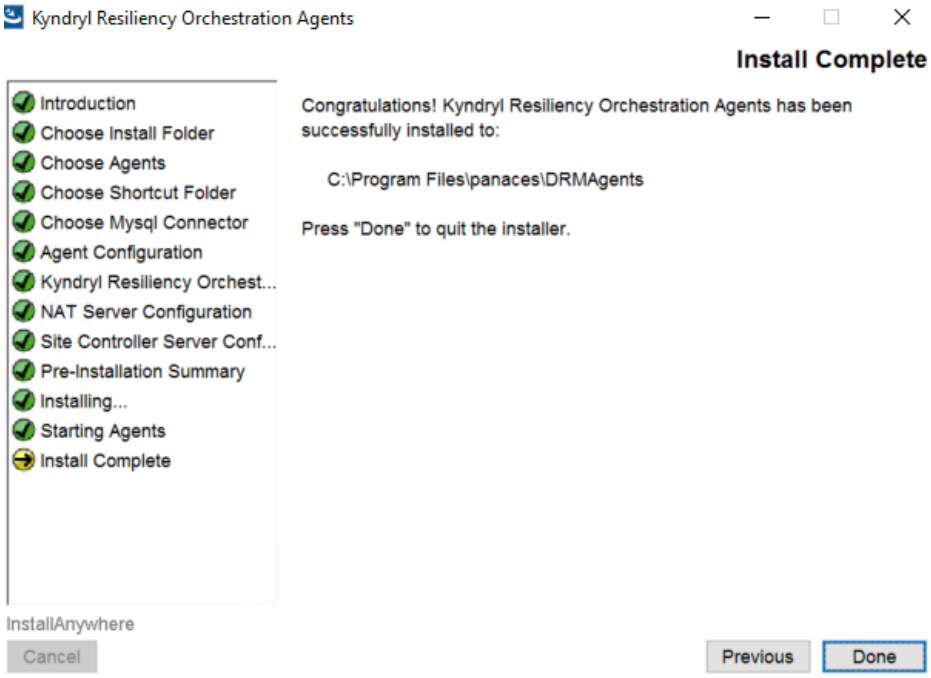


Figure 78: Upgrade Agents on Linux Server - Upgrade Complete

26. Click **Done** to complete the upgrade process.

23 Upgrading Resiliency Orchestration Agents Using Silent Mode Installation

23.1 Prerequisites before upgrading agents on AIX Server

Stop all the agents.

23.2 Limitations

- Agents should be upgraded first before Kyndryl Resiliency File Replicator is upgraded. in case Kyndryl Resiliency File Replicator is installed with agents.
- During the upgrade, use the old EAMSROOT as an installation path.

23.3 Editing Properties File

When you upgrade Kyndryl Resiliency Orchestration Agents in Silent mode, the upgrade program uses the **.properties** file for agents (PanacesAgentsInstaller.properties), to determine which upgrade options should be implemented.

Therefore, before you run the upgrade program in silent mode, you will need to edit the respective properties file to specify the upgrade options that you want to invoke during the Kyndryl Resiliency Orchestration Agents upgrade. Perform the following steps to edit the properties files.

1. Get the files from the Kyndryl Passport Advantage site and copy properties files by running the following command:

```
cp Agents/PanacesAgentsInstaller.properties  /tmp
```

2. Open the properties file by using the following command:

```
Agents(UNIX)

vi /tmp/PanacesAgentsInstaller.properties
```

3. Modify the respective properties file for the keywords shown in the following tables, to reflect your configuration.
4. For the panaces user, after updating the property file we have to add the query to start the server

```
GRANT SELECT,INSERT,UPDATE,DELETE,DROP,CREATE,EXECUTE,SHOW VIEW
ON panaces.* TO 'panaces'@'localhost' IDENTIFIED BY '<Password[1]>'
WITH GRANT OPTION;

flush privileges;
ALTER USER 'panaces'@'localhost' IDENTIFIED BY '<Password[1]>';
```

```
flush privileges;
```

[1]Connect with the Support/Delivery team to get the default passwords.

23.3.1 PanacesAgentsInstaller.properties file

The following table describes the keywords of the PanacesAgentsInstaller.properties file:

Table 24: Keywords of PanacesAgentsInstaller.properties File

Keyword	Description
INSTALLER_UI	Displays the mode of installation as "silent".
MSSQL_AGENT_WINDOWS_CHK Sanovi File replicator _AGENT_CHK SYBASE_AGENT_SOL_CHK SRS_AGENT_CHK ORACLE_AGENT_CHK ORACLE_DATA_GUARD_AGENT_CHK TRUE_COPY_AGENT_CHK SRDF_AGENT_CHK HPXP_AGENT_CHK DB2_AGENT_CHK POSTGRES_AGENT_CHK	Set to 1 to install the agent. Set to 0 to not install the agent.
USER_INPUT_RESULT_JAR_MSSQL	Enter the full path of the directory where the MSSQL Jar files have been installed. **For example:** On Windows, the location of the Jar files would be C:\Program Files\Microsoft SQL Server 2000 or 2005 Driver for JDBC\lib
USER_INPUT_ORACLE_HOME	Enter the full path of the directory where the Oracle is installed.
USER_INPUT_RESULT_JAR_ORA	Enter the full path of the directory where the Oracle Jar files have been installed. Usually, it is $ORACLE_HOME/jdbc/lib **Note**: Confirm that the path contains the following jar files:

Keyword	Description
	ojdbc<version>.jar orai18n.jar
USER_INPUT_RESULT_JLIB_ORA	Enter the full path of the directory where jar library files are located. Usually, it is $ORACLE_HOME/jlib **Note**: Confirm that the path contains the following jar files: oraclepki.jar osdt_cert.jar osdt_core.jar
USER_INPUT_RESULT_JAR_SYBASE	Enter the full path of the directory where the Sybase Jar files have been installed. For example: <sybase installation path>/jConnect-5_5/classes.
USER_INPUT_RESULT_SYBASE_LOGIN	Enter the Sybase Admin login ID.
USER_INPUT_RESULT_PRIMARY_PANACES_SERVER	Enter the IP address/Name of the primary server.
USER_INPUT_RESULT_SECONDARY_PANACES_SERVER	Enter the IP address/Name of the secondary server.
PANACES_AGENT_NODE_ADDRESS	Enter the IP address/Name of the Kyndryl Resiliency Orchestration Agent.
REG_PANACES_CLASSPATH	Displays the Kyndryl Resiliency Orchestration classpath. By default, the following classpath is displayed: lax.nl.env.PANACES_CLASSPATH
USER_INPUT_RESULT_DB2DIR	Enter DB2 installation path
USER_INPUT_RESULT_DB2_INSTANCEUSER	Enter DB2 instance username
USER_INSTALL_DIR	The full pathname for the directory in which you want to install the agent software.
AGENTS_START_YES	Set to 1 if you want to start the agents automatically after the Kyndryl Resiliency Orchestration installation.

Keyword	Description
	Set it to 0 if you want to start the agents manually. Refer to the Starting and Stopping of Agents in the respective *Installation of Agents* chapter in this guide for more information.
USER_INPUT_RESULT_POSTGRES_LOGIN	By default, "postgres" will be pre-filled as the login ID.
USER_INPUT_RESULT_NAT_SERVER	NAT IP Address/Name
USER_INPUT_RESULT_SITE_CONTROLLER_SERVER	Enter Site Controller IP address/Name.
CHOSEN_INSTALL_MODE	Enter Upgrade **Note**: This is used only during Upgrade

23.4 Upgrading Agents in Silent Mode on Windows

Perform the following steps to upgrade the Agents on Windows:

1. Log on to the Windows system.
2. Open an MS-DOS command prompt window.
3. Go to the directory that contains the installation file and launch the installation procedure by entering the following command:

```
install.exe -f <complete path of the .properties file with the properties file name>
```

For Example: install.exe -f c:\\Progra~1\\panaces\\PanacesAgentsInstaller.properties

Note

- After completing the installation of Agents on Windows Server, no status is displayed. The user does not get information on whether the installation is successful or not.
- For low-touch upgrade steps (Upgrade Assist feature), please refer to the topic Agent Upgrade in Kyndryl Resiliency Orchestration Admin Guide.

23.5 Upgrading Agents in Silent Mode on Solaris, Linux, HPUX, AIX Servers

1. Log on to Linux/Solaris/HPUX/AIX system.

2. Navigate to the directory that contains the installation file.
3. Launch the installation by entering the following command:

```
Sudo ./install.bin –f <complete path of the .properties file with
the properties file name>
```

For Example: For agents sudo ./install.bin –f /Agents/ PanacesAgentsInstaller.properties

24 Installing Third-party Software

Download the GPL dependent binaries from this link: *GPL Dependent Binaries* (https://sourceforge.net/projects/gnu-utils/files/binaries/).

You can use the procedures in this section to install the required third-party software that you can download from the GPL Dependent Binaries site.

For more information about the GPL licenses, see *GPL License Information*

Refer to the note about unzip utility at Unzip Note.

25.1 Red Hat Enterprise Linux (RHEL) Versions

25.1.1. RHEL 7.5/7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.4/8.5/8.6/9.0/9.1 (64-Bit)

1. Download the software from the GPL Dependent Binaries site.
1. Go to the ROOT folder for the Resiliency Orchestration application or its component.
2. Unzip the files by executing the following command

Example -

```
tar -xvzf rsync3.0.9-RHEL7-64bit.tar.gz
tar -xvzf tar1.23-RHEL7-64bit.tar.gz
```

25.2 Advanced Interactive eXecutive (AIX)

1. Download the software from the GPL Dependent Binaries site.
2. Go to the ROOT folder for the Resiliency Orchestration application or its component.
3. Unzip the files by executing the following command

Example -

```
gunzip rsync3.0.5-AIX.tar.gz
tar -xvf rsync3.0.5-AIX.tar.gz
gunzip tar1.14-AIX.tar.gz
tar -xvf tar1.14-AIX.tar.gz
```

25.3 HPUX 64-Bit Itanium

1. Download the software from the GPL Dependent Binaries site.
2. Go to the ROOT folder for the Resiliency Orchestration application or its component.

3. Unzip the files by executing the following command

Example -

```
gunzip rsync3.0.9-HPUX11.31-IA.tar.gz
tar -xvf rsync3.0.9-HPUX11.31-IA.tar
gunzip tar1.26-HPUX11.31-IA.tar.gz
tar -xvf tar1.26-HPUX11.31-IA.tar
```

25.4 HPUX 64-Bit Parisac

1. Download the software from the GPL Dependent Binaries site.
2. Go to the ROOT folder for the Resiliency Orchestration application or its component.
3. Unzip the files by executing the following command

Example -

```
gunzip rsync3.0.9-HPUX11i-PARISC.tar.gz
tar -xvf rsync3.0.9-HPUX11i-PARISC.tar
gunzip tar1.26-HPUX11i-PARISC.tar.gz
tar -xvf tar1.26-HPUX11i-PARISC.tar
```

25.5 Solaris_Sparc

1. Download the software from the GPL Dependent Binaries site.
2. Go to the ROOT folder for the Resiliency Orchestration application or its component.
3. Unzip the files by executing the following command

Example -

```
tar -xvzf rsync3.0.5-SOLARIS10-SPARC.tar.gz
tar -xvzf tar1.18-SOLARIS10-SPARC.tar.gz
```

25.6 Solaris_Intel

1. Download the software from the GPL Dependent Binaries site.
2. Go to the ROOT folder for the Resiliency Orchestration application or its component.
3. Unzip the files by executing the following command

Example -

```
tar -xvzf rsync3.0.5-SOLARIS10-x86.tar.gz
```

```
tar -xvzf tar1.26-SOLARIS10-x86.tar.gz
```

25.7 Installing LIBLDM Utility Tool

Perform the following steps to download and install the LIBLDM utility tool:

For Suse Linux:

1. Execute the below command to list all the extensions.

   ```
   SUSEConnect --list-extensions
   ```

   Note: To check whether the particular extension has been installed or not.

2. Connect to the internet, and download the RPM package to the local repository from https://opensuse.pkgs.org/15.3/opensuse-oss-x86_64/libldm-1_0-0-0.2.4-1.31.aarch64.rpm using the following command

   ```
   sudo wget
   ```

3. Execute the below command to connect to the suse repository.

   ```
   SUSEConnect -p PackageHub/15.3/x86_64
   ```

4. Execute the below command to install the package.

   ```
   zypper install libldm-1_0-0-0.2.4-1.31.aarch64.rpm
   ```

For RedHat Linux

1. Execute the below command to list all the extensions.

   ```
   yum update --list-extensions
   ```

   Note: This is to check whether the particular extension has been installed or not.

2. Connect to the internet, and download the RPM package to the local repository from

   https://opensuse.pkgs.org/15.3/opensuse-oss-x86_64/libldm-1_0-0-0.2.4-1.31.aarch64.rpm using the command:

   ```
   sudo wget
   ```

3. Execute the below command to connect to the suse repository.

   ```
   yum update -p PackageHub/15.3/x86_64
   ```

4. Execute the below command to install the package.

   ```
   yum install libldm-1_0-0-0.2.4-1.31.aarch64.rpm
   ```

Once the LIBLDM utility tool is downloaded and installed, ldmtool can be used to query and mount dynamic disks. To configure the LIBLDM tool, perform the following steps:

1. Execute the below command to get the disk group UUID:

   ```
   ldmtool scan
   ```

2. Execute the below command to find the volumes in a disk group:

   ```
   ldmtool show diskgroup <diskgroup UUID>
   ```

3. Use the below command to create the individual device mappers:

   ```
   ldmtool create volume <volume name>
   ```

4. Use the below command to create the device mappers for all the volumes in a disk group:

   ```
   ldmtool create volume diskgroup UUID
   ```

To create device mappers for all volumes, perform:

```
ldmtool create all
```

This command displays the /dev/mapper folder with volumes under LDM and can be accessible using:

```
mount -t ntfs /dev/mapper/LDM volume /mnt/mountpoint
```

For example:

```
mount-tntfs/dev/mapper/ldm_vol_jumpserver3-
   Dg0_Volume1/monitor/ldm_vol_jumpserver3/Dg0_Volume1
```

25 Uninstalling Resiliency Orchestration Agent Node

Perform the following steps to uninstall Kyndryl Resiliency Orchestration Agent Node.

1. Go to <$EAMSROOT>/UninstallerData folder.
2. Click **Uninstall Kyndryl Resiliency Orchestration Agent Node** folder. The **Uninstall Kyndryl Resiliency Orchestration Agent Node** window opens.
3. Click **Uninstall**.
4. The uninstallation process begins and lasts for a few seconds. When the process is complete, the following window is displayed.
5. Click **Done** to close this window.

kyndryl

26 Uninstalling Resiliency Orchestration Server

This chapter provides detailed information on uninstalling the Kyndryl Resiliency Orchestration products on your system.

> **Note**
>
> If you have used the Silent mode of installation, you can perform only the Silent mode of uninstallation. After the Silent mode of installation, the Graphical mode of uninstallation cannot be performed.

27.1 Uninstalling by using the Silent Mode

If the Kyndryl Resiliency Orchestration Server and/ or Agent is installed through Graphical mode, the uninstallation is possible through both Graphical and Silent mode by using the following command:

```
Uninstall_IBM_Resiliency_Orchestration -i silent
```

Uninstallation of Kyndryl Resiliency Orchestration Server can be performed from:

- GUI
- Command Prompt

27.2 Uninstalling by using the GUI

To uninstall Kyndryl Resiliency Orchestration Server from GUI, perform the following steps:

1. Go to $EAMSROOT/UninstallerData.
2. Click **Uninstall_Kyndryl_Resiliency_Orchestration.**
3. The **Introduction** screen is displayed, as shown in the following figure.
4. Click the **Uninstall** button to continue with Uninstallation. The **Uninstalling...** screen is displayed, as shown in the following figure.
5. Once the uninstaller removes all the features, the **Uninstall Complete** screen is displayed, as shown in the following figure.
6. Click **Done** to close the Uninstall Kyndryl Resiliency Orchestration Server window.

> **Note**
>
> The uninstallation of the Kyndryl Resiliency Orchestration Server does not delete the database.

You have to manually delete the databases by providing the following command at the command prompt:

```
#mysql -u root

mysql>drop database panaces;

mysql>drop database pfr;
```

27.3 Uninstalling by using the Command Prompt

To uninstall Kyndryl Resiliency Orchestration Server from the command prompt, perform the following steps:

```
# cd $EAMSROOT/UninstallerData

# ./Uninstall_IBM_Resiliency_Orchestration
```

This process will uninstall all binaries that have been installed while installing Kyndryl Resiliency Orchestration Server.

> **Note:**
>
> This process will not uninstall Tomcat binaries.

28 Uninstalling of Agents

28.1 Agents on Windows

Perform the following steps to uninstall all agents on your system.

1. Go to C:\Program Files\Panaces\ UninstallerData\ folder.
2. Click **Uninstall Agents** folder. The **Uninstall Agents** window opens.
3. Click **Uninstall**.
4. The uninstallation process begins and lasts for a few seconds. When the process is complete, the following window is displayed.

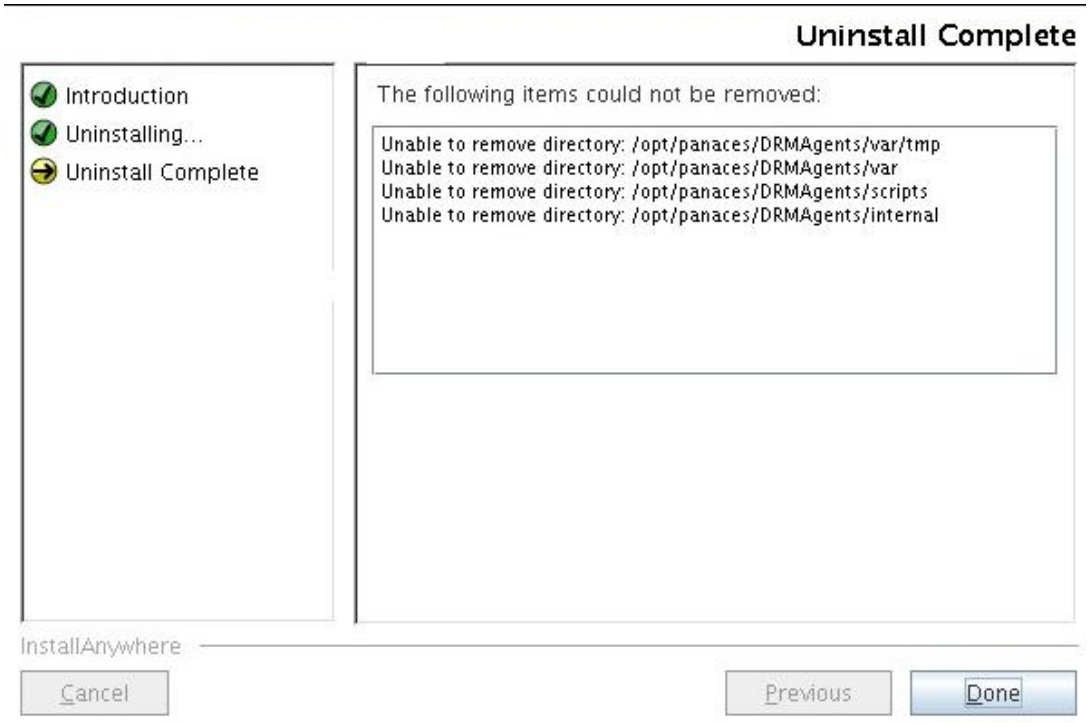


Figure 79: Uninstall the Complete screen

5. Click **Done** to close this window.

28.2 Agents on Solaris

Perform the following steps to uninstall all agents from your system.

To uninstall Solaris agent(s) from the command prompt, execute the following commands:

```
# cd $EAMSROOT/UninstallerData

# ./Uninstall_IBM_Resiliency_Orchestration_Agents
```

As part of uninstallation, the link names from the "/etc/rc3.d" directory should be manually removed.

28.3 Agents on Linux

Perform the following steps to uninstall all agents from your system.

To uninstall Linux agent(s) from the command prompt, perform the following steps:

```
# cd $EAMSROOT/UninstallerData

# ./Uninstall_IBM_Resiliency_Orchestration_Agents
```

As part of uninstallation, the link names from the "/etc/rc.d/rc3.d" directory should be manually removed.

28.4 Agents on HPUX

Perform the following steps to uninstall all agents from your system.

To uninstall HPUX agent(s) from the command prompt, perform the following steps:

```
# cd $EAMSROOT/UninstallerData

# ./Uninstall_IBM_Resiliency_Orchestration_Agents
```

As part of uninstallation, the link names from the "/etc/rc3.d" directory should be manually removed.

28.5 Agents on AIX

To uninstall AIX agent(s) from the command prompt, enter the following commands:

```
# cd $EAMSROOT/UninstallerData

# ./Uninstall_IBM_Resiliency_Orchestration_Agents
```

As part of uninstallation, the link names from the "/etc/rc.d/rc2.d" directory should be manually removed.

During uninstallation, the following directories will not be deleted, as they might be useful.

```
var/log
```

```
scripts/samples

panacesFileReplicator/filesets
```

If the above directories are not deleted, the uninstallation process will list the name of these directories. After reviewing its contents, the directories can be deleted as required.

kyndryl

29 Installing Resiliency Orchestration OS Command Processor

29.1 Prerequisites

Before installing the Kyndryl Sz/OS CP (Command Processor), you need to install the following components on your z/OS system:

z/OS ICSF: ICSF is a software element of z/OS. ICSF works with the hardware cryptographic features and the Security Server (RACF element) to provide secure, high-speed cryptographic services in the z/OS environment. ICSF provides application programming interfaces, which allow applications to request cryptographic services. ICSF is also a means for loading secure cryptographic features with master key values, allowing the hardware features to be used by applications. The cryptographic feature is secure, high-speed hardware that performs the actual cryptographic functions. Your processor hardware determines the cryptographic feature available to your applications.

> **Note**
>
> If z/OS ICSF is not installed, refer to the following manual: z/OS Cryptographic Services Integrated Cryptographic Service Facility System Programmer's Guide.

z/OS OpenSSH: OpenSSH provides secure encryption for both remote login and file transfer.

> **Note**
>
> If z/OS OpenSSH is not installed, refer to the following manual: z/OS Kyndryl Ported Tools for z/OS: OpenSSH User's Guide

29.2 Overview

The Kyndryl Sz/OS CP (Command Processor) enables the Kyndryl Resiliency Orchestration Manager workflows to communicate with z/OS systems. The communication is created by installing several modules in the OMVS subsystem that allow commands to be submitted through SSH communications and through OMVS to execute on your z/OS system. Responses to those commands are then captured and returned to the Resiliency Orchestration Manager Server for further workflow processing.

For example, the following figure displays the Resiliency Orchestration Manager workflow, where **Step A** checks if the job, JOB123 is executing, if it is, **Step B** submits JOB456, and **Step C** is ignored, otherwise if **Step A** is not executing, **Step B** is ignored and **Step C** is completed.

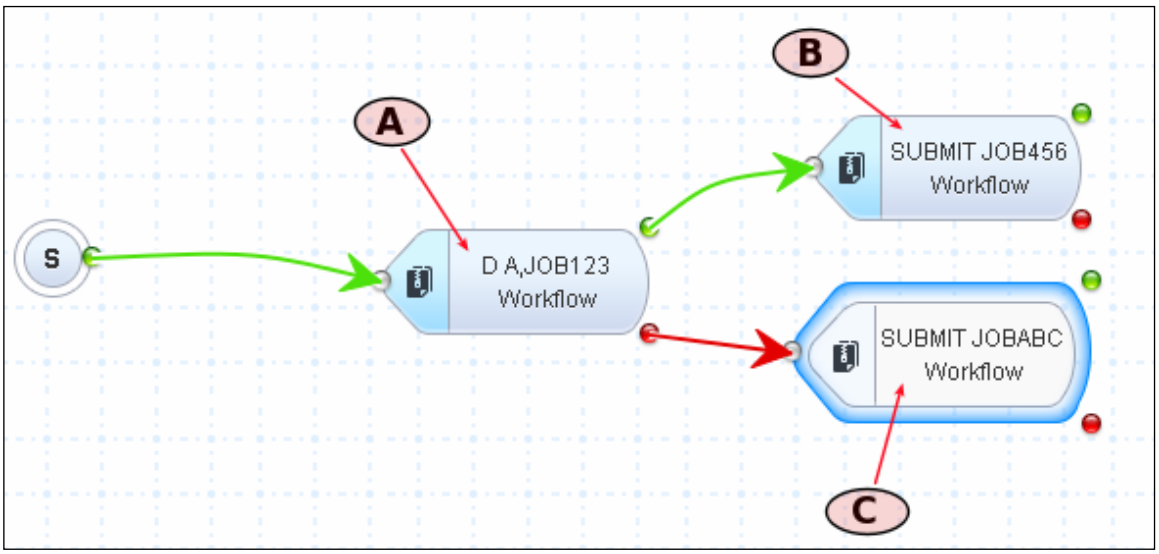


Figure 80: Resiliency Orchestration Workflow

29.3 Installing OS Command Processor

The Resiliency Orchestration OS Command Processor can be installed from a tar file. The name of the tar file is `sanovi-szcpvnnrnn.tar` where nn denotes the version and release number of the tar file.

> **Note**
>
> You need to install OS Command Processor into a directory named `/u/sanovi`.

The following tasks need to be performed to install the Resiliency Orchestration OS Command Processor from a tar file:

1. Extract the Installation File
2. Authorize APF for TCMD, ZCMD, GCMD, and XCMD
3. Define Userid SANOVI to RACF (or other security programs)

29.3.1 Extracting Installation File

The following are the steps to extract the installation file:

1. Specify the IP of your z/OS system, enable the download in binary mode, and FTP the SzCP tar file to your z/OS system, as shown in the following example:

```
ftp xxx.xxx.xxx.xxx  <- the IP of your z/OS system

bin      <- set binary mode
```

```
put /from/sanovi-szcpvnnrnn.tar /to/sanovi-szcpvnnrnn.tar
```

2. Create the `/u/sanovi` folder. If you have a previous version installed, copy it to the backup before proceeding, for example, `/u/sanovi-prev-version`.
3. Extract the `sanovi-szcpvnnrnn.tar` file. Specify `-xvf` to extract and display the untared files, and then specify the location `/xxxx` where the tar file is FTP'd in Step 1. The following example displays the snippet for installing `v01r00`:

```
tar -xvf /xxxx/sanovi-szcpv01r00.tar
```

4. Verify that the following files are extracted in the `/u/sanovi` folder:

/u/sanovi/TCMD, 12288 bytes, 24 tape blocks

/u/sanovi/ZCMD, 24576 bytes, 48 tape blocks

/u/sanovi/tcmd.sh, 64 bytes, 1 tape block

/u/sanovi/zcmd.sh, 64 bytes, 1 tape block

29.3.2 Authorizing APF for TCMD, ZCMD, GCMD, and XCMD

1. After the untar, the contents of the /u/sanovi folder are displayed as shown below:

```
gcmd.sh                          File rwxrwxrwx  fff--- --s- ----
 tcmd.sh                          File rwxr-xr-x  fff--- --s- ----
 xcmd.sh                          File rwxr-xr-x  fff--- --s- ----
 zcmd.sh                          File rwxr-xr-x  fff--- --s- ----
 GCMD                             File rwxrwxrwx  fff--- --s- ----
 TCMD                             File rwxr-xr-x  fff--- --s- ----
 XCMD                             File rwxr-xr-x  fff--- --s- ----
 ZCMD                             File rwxr-xr-x  fff--- --s- ----
```

Note

The contents of the `/u/sanovi` folder displayed from the ISPF `Data Set List Utility` or `Edit Entry Panel` are the same.

2. Set the APF Extended Attribute ON for TCMD and ZCMD. You can perform this through ISPF, for example using **MX (**Modify Extended Attributes):

```
MX       TCMD                File rwxr-xr-x  fff--- --s- ----
```

3. Enter "/" next to APF Authorized, as shown below

```
Modify z/OS UNIX File Extended Attributes
Command ===>

Pathname . : /u/sanovi/TCMD
Type . . . : File

Enter "/" to select option
/  Use Shared Address Space
/  APF Authorized
   Program Controlled
   Shared Library
```

4. After APF authorization is turned on for TCMD and ZCMD, verify that the extended attribute displays, as shown below:

```
Pathname. : /u/sanovi
EUID . . . : 0
Command Filename  Message Type Permission Audit  Ext  Fmat
-----------------------------------------------------------
                      Dir  rwxr-xr-x  fff---      ----
                      Dir  rwxr-xr-x  fff---      ----
gcmd.sh               File rwxrwxrwx  fff--- --s- ----
tcmd.sh               File rwxr-xr-x  fff--- --s- ----
xcmd.sh               File rwxr-xr-x  fff--- --s- ----
zcmd.sh               File rwxr-xr-x  fff--- --s- ----
GCMD                  File rwxrwxrwx  fff--- a-s- ----
TCMD                  File rwxr-xr-x  fff--- a-s- ----
XCMD                  File rwxr-xr-x  fff--- a-s- ----
ZCMD                  File rwxr-xr-x  fff--- a-s- -------
```

29.3.3 Defining Userid SANOVI to RACF/Other Security Program

Define a userid named SANOVI to RACF or equivalent security program. The SANOVI userid needs the following OPERPARM attributes set:

```
OPERPARM INFORMATION
--------------------
STORAGE= 00000
AUTH= MASTER
DOM= ALL
CMDSYS= *
```

29.4 Verifying Sz/OS CP (Command Processor) Install

1. After the install, verify the install by executing the SzCPIVP Workflow from Resiliency Orchestration. The following figure displays the SzCPIVP Workflow.

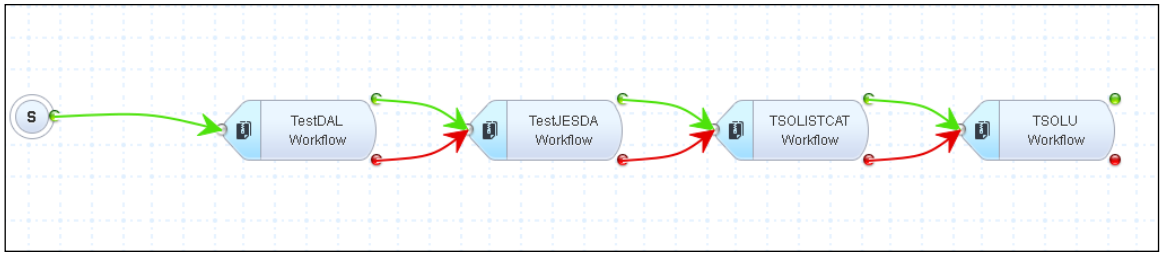


Figure 81: SzCPIVP

2. The workflow executes a few simple tests to confirm that your install was successful. The following tasks will be performed:

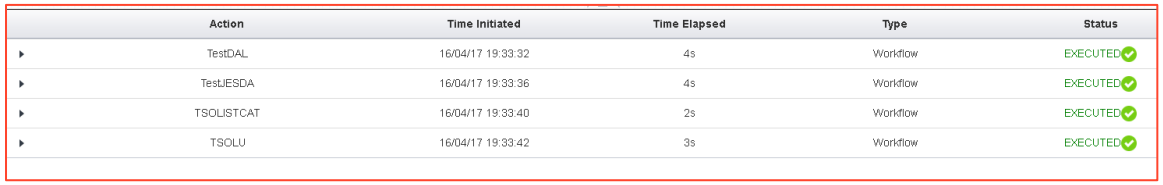
TESTDAL: The TESTDAL enters and returns the output from a z/OS command "D A,L".

TESTJESDA: The TESTJESDA enters and returns the output from a JES command "$DA".

TSOLISTCAT: The TSOLISTCAT enters and returns the output from a TSO LISTC command.

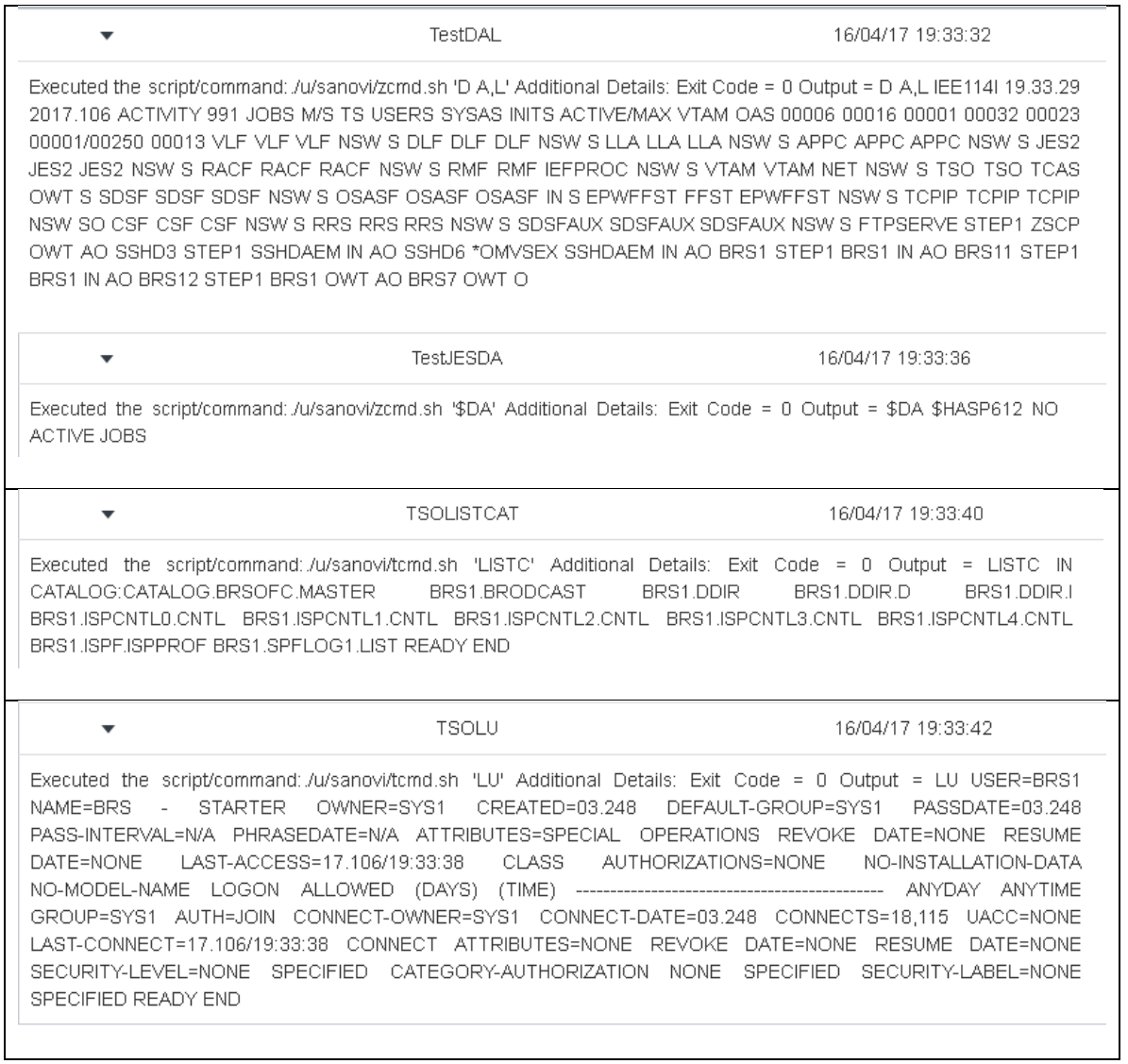
TSOLU: The TSOLU enters and returns the output from a TSO LU command.

3. After the workflow is executed, confirm that each step is successful. For example, successfully executed actions are displayed as shown below:



	Action	Time Initiated	Time Elapsed	Type	Status
▸	TestDAL	16/04/17 19:33:32	4s	Workflow	EXECUTED
▸	TestJESDA	16/04/17 19:33:36	4s	Workflow	EXECUTED
▸	TSOLISTCAT	16/04/17 19:33:40	2s	Workflow	EXECUTED
▸	TSOLU	16/04/17 19:33:42	3s	Workflow	EXECUTED

4. Click on the expand arrow to the left of each Action to verify that the correct output is returned. For example, your install is complete when the output is returned as shown in the following figure:



▾ TestDAL 16/04/17 19:33:32

Executed the script/command: /u/sanovi/zcmd.sh 'D A,L' Additional Details: Exit Code = 0 Output = D A,L IEE114I 19.33.29 2017.106 ACTIVITY 991 JOBS M/S TS USERS SYSAS INITS ACTIVE/MAX VTAM OAS 00006 00016 00001 00032 00023 00001/00250 00013 VLF VLF VLF NSW S DLF DLF DLF NSW S LLA LLA LLA NSW S APPC APPC APPC NSW S JES2 JES2 JES2 NSW S RACF RACF RACF NSW S RMF RMF IEFPROC NSW S VTAM VTAM NET NSW S TSO TSO TCAS OWT S SDSF SDSF SDSF NSW S OSASF OSASF OSASF IN S EPWFFST FFST EPWFFST NSW S TCPIP TCPIP TCPIP NSW SO CSF CSF CSF NSW S RRS RRS RRS NSW S SDSFAUX SDSFAUX SDSFAUX NSW S FTPSERVE STEP1 ZSCP OWT AO SSHD3 STEP1 SSHDAEM IN AO SSHD6 *OMVSEX SSHDAEM IN AO BRS1 STEP1 BRS1 IN AO BRS11 STEP1 BRS1 IN AO BRS12 STEP1 BRS1 OWT AO BRS7 OWT O

▾ TestJESDA 16/04/17 19:33:36

Executed the script/command: /u/sanovi/zcmd.sh '$DA' Additional Details: Exit Code = 0 Output = $DA $HASP612 NO ACTIVE JOBS

▾ TSOLISTCAT 16/04/17 19:33:40

Executed the script/command: /u/sanovi/tcmd.sh 'LISTC' Additional Details: Exit Code = 0 Output = LISTC IN CATALOG:CATALOG.BRSOFC.MASTER BRS1.BRODCAST BRS1.DDIR BRS1.DDIR.D BRS1.DDIR.I BRS1.ISPCNTL0.CNTL BRS1.ISPCNTL1.CNTL BRS1.ISPCNTL2.CNTL BRS1.ISPCNTL3.CNTL BRS1.ISPCNTL4.CNTL BRS1.ISPF.ISPPROF BRS1.SPFLOG1.LIST READY END

▾ TSOLU 16/04/17 19:33:42

Executed the script/command: /u/sanovi/tcmd.sh 'LU' Additional Details: Exit Code = 0 Output = LU USER=BRS1 NAME=BRS - STARTER OWNER=SYS1 CREATED=03.248 DEFAULT-GROUP=SYS1 PASSDATE=03.248 PASS-INTERVAL=N/A PHRASEDATE=N/A ATTRIBUTES=SPECIAL OPERATIONS REVOKE DATE=NONE RESUME DATE=NONE LAST-ACCESS=17.106/19:33:38 CLASS AUTHORIZATIONS=NONE NO-INSTALLATION-DATA NO-MODEL-NAME LOGON ALLOWED (DAYS) (TIME) ---------- ANYDAY ANYTIME GROUP=SYS1 AUTH=JOIN CONNECT-OWNER=SYS1 CONNECT-DATE=03.248 CONNECTS=18,115 UACC=NONE LAST-CONNECT=17.106/19:33:38 CONNECT ATTRIBUTES=NONE REVOKE DATE=NONE RESUME DATE=NONE SECURITY-LEVEL=NONE SPECIFIED CATEGORY-AUTHORIZATION NONE SPECIFIED SECURITY-LABEL=NONE SPECIFIED READY END

30 Migrating the Resiliency Orchestration Server

This section covers the information on migrating the Kyndryl Resiliency Orchestration Application Server to a New Server.

The system allows you to migrate to the new server and retain the Same IP as the old server or set up a new IP for the new server.

30.1 Migrating to new Server with Same IP

The folder /backup must have enough disk space for the original and new Kyndryl Resiliency Orchestration Server. In the below procedure, EAMSROOT is /opt/panaces, and TOMCAT_HOME is /opt/jboss-ews-2.0/ tomcat9.0.27. It also requires the same OS with the same MariaDB DB version level.

The below steps need to be followed to migrate Kyndryl Resiliency Orchestration Server to a new server with the same IP

1. Stop all the services in the current Kyndryl Resiliency Orchestration Server.

255. Run the `enableEncryptionOnTables.sh` script under $EAMSROOT/bin in the Kyndryl Resiliency Orchestration server

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

Check for the below table decryption confirmation message.
Executing the alter ddl statements.
Decrypted
```

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

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

For Example –

/opt/panaces/bin/enableEncryptionOnTables.sh "dec" <Password[1]>

[1]Connect with the Support/Delivery team to get the default passwords.

256. Take the mysql Schema

```
mysqldump -u root --databases panaces pfr --triggers --routines > /backup/panaces-pfr.sql
```

257. Take EAMSROOT, and TOMCAT Home folder backup

```
cd /opt
```

```
tar –cvzf  /backup/EAMSROOT.tar.gz  panaces
cd /opt/
tar –cvzf /backup/tomcat9.0.27.tar.gz   jboss-ews-2.0
```

5. Copy **/backup/panaces-pfr.sql /backup/EAMSROOT.tar.gz /backup/tomcat**9.0.27**.tar.gz /etc/security/limit.conf /etc/hosts /etc/my.cnf** to a common share location.
6. Note down hostname of original server, at prompt type hostname
7. Note down the port exceptions in firewall, use system-config-firewall or system-config-securitylevel
8. Shutdown the current Kyndryl Resiliency Orchestration Server using the poweroff command
9. Bring the New Kyndryl Resiliency Orchestration Server with the Same IP with the help of IT.
10. Login to the new Kyndryl Resiliency Orchestration Server using putty.
11. Copy all the files from the common share folder to /backup. Files to be copied are - panaces-pfr.sql EAMSROOT.tar.gz tomcat9.0.27.tar.gz limit.conf hosts my.cnf
12. Extract Kyndryl Resiliency Orchestration binaries

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

13. Extract Tomcat

```
cd /opt
tar –xvzf /backup/tomcat9.0.27.tar.gz
```

14. Update EAMSROOT

```
echo  “export  EAMSROOT=/opt/panaces” >> /etc/profile
```

15. Refer **/backup/limit.conf , /backup/hosts , /backup/my.cnf and update /etc/security/limit.conf /etc/hosts /etc/my.cnf** respectively
16. Set hostname same as noted one

```
hostname <original_server_hostname>
update same in /etc/sysconfig/network
```

17. Configure the exception ports as noted earlier using system-config-firewall or system-config-securitylevel
18. Restore the mysql schema

```
mysql  -u root < /backup/panaces-pfr.sql
```

19. Create required mysql users along with privileges

```
Mysql –u root

use mysql;

CREATE USER 'pfradmin'@'localhost' IDENTIFIED BY '<Password[1]>';

GRANT ALL PRIVILEGES ON *.* TO 'pfradmin'@'localhost' IDENTIFIED BY
'<Password[1]>' WITH GRANT OPTION;

CREATE USER 'panaces'@'localhost' IDENTIFIED BY '<Password[1]>';

GRANT ALL PRIVILEGES ON *.* TO 'panaces'@'localhost' IDENTIFIED BY
'<Password[1]>' WITH GRANT OPTION;

CREATE USER 'sanovireporter'@'localhost' IDENTIFIED BY
'<Password[1]>';

GRANT ALL PRIVILEGES ON *.* TO 'sanovireporter'@'localhost'
IDENTIFIED BY '<Password[1]>' WITH GRANT OPTION;


[1]Connect with the Support/Delivery team to get the default
passwords.
```

20. Verify the panaces, and pfr databases are available after they are restored in the new server.
21. Start Kyndryl Resiliency Orchestration Services:

```
/opt/panaces/bin/panaces start
```

22. Verify that the console log shows panaces services started successfully

```
tail –f  /opt/panaces/var/log/console.log
```

30.2 Migrating to a new Server with New IP

The folder /backup must have enough disk space for the original and new Kyndryl Resiliency Orchestration Server. In the below procedure, EAMSROOT is /opt/panaces, and TOMCAT_HOME is /opt/jboss-ews-2.0/tomcat9.0.27. It also requires the same OS with the same MariaDB DB version level.

The below steps need to be followed to migrate Kyndryl Resiliency Orchestration Server to a new server with new IP.

1. Stop all the services in the current Kyndryl Resiliency Orchestration Server.

258. Run the enableEncryptionOnTables.sh script. Refer procedure to enableEncryptionOnTables .

259. Take the mysql Schema dump

```
mysqldump -u root --databases panaces pfr --triggers --routines >
/backup/panaces-pfr.sql
```

260. Take EAMSROOT, and TOMCAT Home folder backup
    - `cd /opt`
    - `tar –cvzf /backup/EAMSROOT.tar.gz panaces`
    - `cd /opt/`
    - `tar –cvzf /backup/tomcat9.0.27.tar.gz jboss-ews-2.0`
261. Copy **/backup/panaces-pfr.sql** **/backup/EAMSROOT.tar.gz** **/backup/tomcat9.0.27.tar.gz** **/etc/security/limit.conf** **/etc/hosts** **/etc/my.cnf** to **/backup** of new Kyndryl Resiliency Orchestration Server using scp.
262. Note down the port exceptions in the firewall, use system-config-firewall or system-config-securitylevel
263. Log in to the new Kyndryl Resiliency Orchestration Server using putty
264. Extract Kyndryl Resiliency Orchestration binaries
    - `cd /opt`
    - `tar –xvzf /backup/ EAMSROOT.tar.gz`
265. Extract Tomcat
    - `cd /opt`
    - `tar –xvzf /backup/tomcat9.0.27.tar.gz`
    - `Update EAMSROOT`
    - `echo “export EAMSROOT=/opt/panaces” >> /etc/profile`
266. Refer **/backup/limit.conf , /backup/hosts , /backup/my.cnf** and **update /etc/security/limit.conf /etc/hosts /etc/my.cnf** respectively
267. Configure the exception ports as noted earlier using system-config-firewall or system-config-securitylevel
268. Restore the mysql schema

```
mysql -u root < /backup/panaces-pfr.sql
```

Troubleshooting Tip!!

During restore, if you come across this error

ERROR 1418 (HY000) at line 22616: This function has none of DETERMINISTIC, NO SQL, or READS SQL DATA in its declaration, and binary logging is enabled (you *might* want to use the less safe log_bin_trust_function_creators variable)"

Follow the below procedure to fix this issue -

1. Log in to maria DB
2. Set the value of a variable as shown below -

   set GLOBAL log_bin_trust_function_creators=1;

3. Add this entry in my.cnf –

   log_bin_trust_function_creators=1;

269. Verify the panaces, and pfr databases are available after they are restored in the new server.

270. Create required mysql users along with privileges

```
Mysql –u root

use mysql;

CREATE USER 'pfradmin'@'localhost' IDENTIFIED BY '<Password[1]>';

GRANT ALL PRIVILEGES ON *.* TO 'pfradmin'@'localhost' IDENTIFIED
BY '<Password[1]>' WITH GRANT OPTION;

CREATE USER 'panaces'@'localhost' IDENTIFIED BY '<Password[1]>';

GRANT ALL PRIVILEGES ON *.* TO 'panaces'@'localhost' IDENTIFIED
BY '<Password[1]>' WITH GRANT OPTION;

CREATE USER 'sanovireporter'@'localhost' IDENTIFIED BY
'<Password[1]>';

GRANT ALL PRIVILEGES ON *.* TO 'sanovireporter'@'localhost'
IDENTIFIED BY '<Password[1]>' WITH GRANT OPTION;

[1]Connect with the Support/Delivery team to get the default
passwords.
```

271. Update the following tables to be done for Agent Node and Vault Agent if we use:

```
Use panaces;
```

```
update component set
c_ipaddr='New_IBM_Resiliency_Orchestration_IP' where
c_name='AgentNode' and
c_ipaddr='OLD_IBM_Resiliency_Orchestration_IP';

update component set
c_display_ipaddr='New_IBM_Resiliency_Orchestration_IP' where
c_name='AgentNode' and
c_display_ipaddr='OLD_IBM_Resiliency_Orchestration_IP';

update agent_csa set ac_connectorIP =
'New_IBM_Resiliency_Orchestration_IP' where ac_connectorIP
='OLD_IBM_Resiliency_Orchestration_IP';

update agent_csa set
ac_anode_ip='New_IBM_Resiliency_Orchestration_IP' where
ac_anode_ip='OLD_IBM_Resiliency_Orchestration_IP';

update agent_csa set ac_displayIPaddress =
'New_IBM_Resiliency_Orchestration_IP' where ac_displayIPaddress
='OLD_IBM_Resiliency_Orchestration_IP';

update agent_csa set
ac_ipaddress='New_IBM_Resiliency_Orchestration_IP' where
ac_ipaddress='Old_IBM_Resiliency_Orchestration_IP;

update  component_OSServer
set  cos_mgmt_ipaddr='New_IBM_Resiliency_Orchestration_IP'
where  cos_mgmt_ipaddr='Old_IBM_Resiliency_Orchestration_IP';
```

272. Start Kyndryl Resiliency Orchestration Services:

```
/opt/panaces/bin/panaces start
```

273. Verify that the console log shows panaces services started successfully

Note: Modifying the IP is not supported and there are unknown risks involved if we do.

30.3 Changing Resiliency Orchestration Server IP to New IP

The below steps are to be followed in case there is a change in the Resiliency Orchestration Server IP address from the allocated IP address.

1. Stop Remote Agents from Resiliency Orchestration UI and stop Site Controller services.

2. Stop all Local Agents pointing to Resiliency Orchestration Server.

3. Stop all the services in the Kyndryl Resiliency Orchestration Server.
4. Log in to MariaDB and execute the following command:

```
mysql –u root -p
```

kyndryl

5. Perform the following table changes:

> **Note**
>
> Replace “ “New_IBM_Resiliency_Orchestration_IP” and “OLD_IBM_Resiliency_Orchestration_IP” with the respective IPs.

a. `Use panaces;`

b.
```
update component set
c_ipaddr='New_IBM_Resiliency_Orchestration_IP' where
c_name='AgentNode' and
c_ipaddr='OLD_IBM_Resiliency_Orchestration_IP’;
```

c.
```
update component set
c_display_ipaddr='New_IBM_Resiliency_Orchestration_IP' where
c_name='AgentNode' and
c_display_ipaddr='OLD_IBM_Resiliency_Orchestration_IP';
```

d.
```
update agent_csa set ac_connectorIP =
'New_IBM_Resiliency_Orchestration_IP’ where ac_connectorIP
='OLD_IBM_Resiliency_Orchestration_IP’;
```

e.
```
update agent_csa set
ac_anode_ip='New_IBM_Resiliency_Orchestration_IP’ where
ac_anode_ip='OLD_IBM_Resiliency_Orchestration_IP';
```

f.
```
update agent_csa set ac_displayIPaddress =
'New_IBM_Resiliency_Orchestration_IP’ where ac_displayIPaddress
='OLD_IBM_Resiliency_Orchestration_IP';
```

g.
```
update agent_csa set
ac_ipaddress='New_IBM_Resiliency_Orchestration_IP' where
ac_ipaddress='Old_IBM_Resiliency_Orchestration_IP;
```

h.
```
update component_OSServer
set cos_mgmt_ipaddr='New_IBM_Resiliency_Orchestration_IP'
where cos_mgmt_ipaddr='Old_IBM_Resiliency_Orchestration_IP';
```

6. Update the following configuration properties to refer to the new RO server IP.

   - On RO:

kyndryl

```
$EAMSROOT/installconfig/PanacesAgentGeneric,
$EAMSROOT/bin/panaces_env
```

- On Site Controller:

```
$EAMSROOT/installconfig/PanacesAgentGeneric,
$EAMSROOT/installconfig/SiteController.cfg
```

- On Agents: `$EAMSROOT/installconfig/cfg`

```
PanacesAgentGeneric.cfg
```

7. Start the Resiliency Orchestration services.
8. Start the Site Controller services.
9. Start the Remote services and Local Agent services.

30.4 Migrating from one RHEL version to another RHEL version

Step 1 :- kill all process

Step 2 :- run this script for enabling Encyption on DB tables

./enableEncryptionOnTables.sh "dec" "<Password>"

Step 3 :- take mariadb backup for panacesPFR and user tables

Also make backup tar file of panaces directory

Step -4 :copy all the created DB backup and panaces tar file to new server

Step -5 : On the new Server follow the below steps

run getenforce

if not permissive change using command

setenforce permissive

Step - 6 :Restore DB backup files

mysql -u root -p<Password> < /panacesbackup.sql

mysql -u root -p<Password> mysql </userbackup.sql

Step :7-:log into maria db and use panaces database and execute the below queries

update component set c_ipaddr='<new ro ip address>' where c_name='AgentNode' and c_ipaddr='<old ro ip address>';

update component set c_display_ipaddr='<new ro ip address>' where c_name='AgentNode' and c_display_ipaddr='<old ro ip address>';

update agent_csa set ac_connectorIP='<new ro ip address>' where ac_connectorIP='<old ro ip address>';

update agent_csa set ac_anode_ip='<new ro ip address>' where ac_anode_ip='<old ro ip address>';

update agent_csa set ac_displayIPaddress='<new ro ip address>' where ac_displayIPaddress='<old ro ip address>';

update component_OSServer set cos_mgmt_ipaddr='<new ro ip address>' where cos_mgmt_ipaddr='<old ro ip address>';

Step -8 : untar Panaces.tar under cd /opt

Step -9: copy /tomcat/conf/server.xml (if updated server.xml with chipers are not present) to new server tomcat/conf

Step - 10: Upgrade with the latest version

kyndryl

31 Migrating remote agents from Agent Node (RO) to Site Controller

31.1 Prerequisites

1. Resiliency Orchestration and Site Controller should be ready. This means the Resiliency Orchestration Agent node and Site Controller local agent should be active and connected to the agent listing page.
2. Site Controller mapping and Site Controller as a component is registered. The site controller is required to be in ACTIVE status.
3. Make sure that the DB backup activity has been performed.

31.2 Procedure

1. Execute the following script:

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

Note:

This script moves the non Uniagents running in the Agent Node to the Site Controller but the Uniagents are not migrated.

kyndryl

32 Troubleshooting

The information about errors displayed while you are performing various tasks during the installation and configuration of the Kyndryl Resiliency Orchestration software and troubleshooting tips to resolve such errors is described in this section.

32.1 MariaDB Services Not Starting

The MariaDB services should start if Resiliency Orchestration is reinstalled in a different path. If MariaDB fails to start, you need to roll back the mariadb encryption, which is being performed as a part of the Resiliency Orchestration installation.

32.1.1 Resolution

The following steps need to be performed for a rollback of encryption of tables:

1. Run the following script in the /opt/panaces/bin folder.

   ```
   ./enableEncryptionOnTables.sh dec <DATABASE _PASSWORD>
   ```

2. Take a backup of mariadb, and run the following command to perform this task by assuming /opt/backup folder exists.

   ```
   sudo mysqldump --databases panaces pfr --routines --triggers
   > /opt/backup/metadata.sql
   ```

3. Stop mariadb services, and run the following command to perform this task.

   ```
   sudo service mysql stop
   or
   sudo /bin/systemctl stop mysql
   ```

4. Remove the following entries from the mariadb config file /etc/my.cnf:

   [mariadb]

   plugin-load-add = file_key_management.so
   file_key_management
   file_key_management_filename = /opt/panaces/installconfig/mariadbencryption /keys.txt
   innodb_default_encryption_key_id = 1
   ssl
   ssl-ca=/opt/panaces/installconfig/mariadbencryption/ca-cert.pem
   ssl-cert=/opt/panaces/installconfig/mariadbencryption /server-cert.pem

ssl-key=/opt/panaces/installconfig/mariadbencryption /server-key.pem

5. Start mariadb services, and run the following command to perform this task.

```
Sudo service mysql start
```

6. Restart the Resiliency Orchestration Server.

32.2 Resiliency Orchestration Start Fails with Error ActiveMQ Failed to Start

As part of the installation, the script **SecurityUserInjection.sh** will run correctly. In the event, this script fails to run correctly on starting the Resiliency Orchestration Server, the error message `ActiveMQ Failed to Start` is displayed.

32.2.1 Resolution

a. Kill the running Java ActiveMQ process by using the command: `kill -9 <pid>`

b. Run `$EAMSROOT/bin/SecurityUserInjection.sh`

c. Ensure this script has been completed without any errors displayed.

d. Start the Resiliency Orchestration.

32.3 Resiliency Orchestration application hangs

If the Resiliency Orchestration application hangs, refer to the panaces server log and site controller logs for reason(s) for failure.

The log files are located in the following location –

On the server where Resiliency Orchestration is installed, Resiliency Orchestration log file - /opt/panaces/var/log/PanacesServer.log

On the server where Site Controller is installed, Site Controller log file - /opt/panaces/var/log/SiteController.log

Text to be searched in the log file is - Class name not accepted:

The sample content of the log file is as below -

IOException occurred:: message->Class name not accepted: [C

kyndryl

32.3.1 Resolution

In the panaces.properties file, append the string that is coming after ":" in the error message, for example ",[C" in the key acp.object.deserialization.allow.list as shown in the below example –

```
#==============deserialization
allowist=======================
acp.object.deserialization.allow.list=[B,panaces.*,[Ljava.*,
java.util.*,[Ljava.lang.*,[I,[J,java.rmi.*,[Lpanaces.*,java.
lang.*,[[Ljava.*,[Ljava.math.*,[Z,java.net.*,java.io.*,[Lja
va.sql.*,java.security.*,sun.util.*,java.sql.*,java.math.*,[
C
```

32.4 Subsystem Discovery Failing for Oracle Solution

The product, by default, supports discovery and management for Oracle 12c, 18c, and 19c. Discovery may fail for Oracle 11g.

32.4.1 Resolution

For managing Oracle 11g or lower versions, replace 'ojdbc8.jar' with 'ojdbc6.jar' in the AGENT_CLASSPATH in the following files:

```
$EAMSROOT/bin/OracleAgent.sh

$EAMSROOT/bin/DataGuardAgent.sh
```

For Example:

```
AGENT_CLASSPATH=$ORA_CLIENT_HOME/ojdbc6.jar:$EAMSROOT/lib/DGAge
ntCSA.jar:$EAMSROOT/lib/jcifs-1.3.18.jar:$EAMSROOT/lib/j-
interopdeps.jar:$EAMSROOT/lib/j-
interop.jar:$EAMSROOT/lib/maverick-legacy-client-1.6.16-all.jar
```

32.5 Agent Not Starting on Windows Server

Scripts installed along with the installation start the Agents when the system is rebooted. Alternatively, you can start the agents manually, without rebooting the system. However, if the agents do not start by any of these methods, perform the following tasks:

Check the respective lax files for the agent's class path and java path entries. If these entries are incorrect, edit these files and restart the agents once the agent installation is complete.

Perform any of the following procedures depending on the agent selection:

Note

The default value of EAMSROOT is “C:\Program Files\panaces”. If you have installed Kyndryl Resiliency Orchestration at a different location, then the paths in the following lax files would be appropriately set by the installer program. Following is an example, with the assumption that Kyndryl Resiliency Orchestration has been installed at the default location.

32.5.1 Kyndryl Resiliency File Replicator Service

Open PFRService.lax file that has been installed in the Kyndryl Resiliency File Replicator Service installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= C:\Program Files\panaces\lib\commons-lang-
1.0.1.jar;C:\Program Files\panaces\lib\PADS.jar;C:\Program
Files\panaces\lib\log4j.jar;C:\Program
Files\panaces\lib\jacl.jar;C:\Program
Files\panaces\lib\tcljava.jar;C:\Program
Files\panaces\lib\PFR.jar:lax.jar
```

Edit the Kyndryl Resiliency File Replicator installation path in the `PFRConfiguration.cfg` file by following the steps given below:

1. Enter in the **$EAMSROOT /installconfig** folder.
2. Open the `PFRConfiguration.cfg` file. Provide the installation path of the Kyndryl Resiliency File Replicator in the `PFR_INSTALL_PATH` parameter.
3. Replace `C:\Program Files\panaces` with `C:\Progra~1\panaces`.

32.5.2 PFR Agent

Open PFRAgent.lax file that has been installed in PFR agent install path. Check if lax.class.path has the following classpath:

```
lax.class.path= C:\Program Files\panaces\lib\commons-lang-
1.0.1.jar;C:\Program Files\panaces\lib\PADS.jar;C:\Program
Files\panaces\lib\log4j.jar;C:\Program
Files\panaces\lib\tcljava.jar;C:\Program
Files\panaces\lib\jacl.jar;C:\Program
Files\panaces\lib\PFR.jar;C:\Program
Files\panaces\PFRAgentCSA.jar:lax.jar
```

kyndryl

32.5.3 MSSQL Agent For MSSQL 2005

Open MSSQLAgent.lax file that has been installed in MSSQL agent installation path with a text editor. Check if "LAX.CLASS.PATH" has the following class path:

```
lax.class.path= C:\Program Files\panaces\lib\commons-lang-
1.0.1.jar;C:\Program Files\panaces\lib\PADS.jar;C:\Program
Files\panaces\lib\log4j.jar;C:\Program
Files\panaces\lib\jacl.jar;C:\Program
Files\panaces\lib\tcljava.jar;C:\sqljdbc.jar;C:\Program
Files\panaces\MSSQLAgentCSA.jar:lax.jar
```

32.5.4 Windows OS Agent

Open WindowsOSAgent.lax file that has been installed in the Windows OS agent installation path with a text editor. Check if "LAX.CLASS.PATH" has the following class path:

```
lax.class.path= C:\Program Files\panaces\lib\commons-lang-
1.0.1.jar;C:\Program Files\panaces\lib\PADS.jar;C:\Program
Files\panaces\lib\log4j.jar; C:\Program
Files\panaces\lib\jacl.jar;C:\Program
Files\panaces\lib\tcljava.jar;C:\Program
Files\panaces\WindowsOSAgentCSA.jar; C:\Program
Files\panaces\lib\commons-dbcp-1.2.1.jar;C:\Program
Files\panaces\lib\commons-logging.jar;C:\Program
Files\panaces\lib\commons-pool-1.2.jar;C:\Program
Files\panaces\lib\quartz-all-1.5.2.jar:lax.jar
```

32.6 Agent Not Starting on Solaris Server

Before starting the agent services, check the respective lax files for the agent's class path and java path entries. If these entries are incorrect, edit these files and restart the agents once the agent installation is complete.

Perform any of the following procedures depending on the agent selection:

32.6.1 Sybase Agent

Open Sybase Agent.lax file that has been installed in the Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= /opt/panaces/lib/commons-lang-
1.0.1.jar:/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:/opt/
panaces/lib/jacl.jar:opt/panaces/lib/tcljava.jar:SybaseAgentCSA.jar:
```

kyndryl

```
opt/panaces/lib/SYBASE/ase_125/jConnect-
5_5/classes/jconn2.jar:/SYBASE/ase_125/jConnect-
5_5/classes/jTDS2.jar:lax.jar
```

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.6.2 Kyndryl Resiliency File Replicator Service

Open PFRService.lax file that has been installed in the Kyndryl Resiliency File Replicator Service installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= /opt/panaces/lib/commons-lang-
1.0.1.jar:/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:/opt/
panaces/lib/jacl.jar:opt/panaces/lib/tcljava.jar:/opt/panaces/lib/PF
R.jar:lax.jar
```

32.6.3 PFR Agent

Before starting the PFR Agent, open PFRAgent.lax file that has been installed in the Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= /opt/panaces/lib/commons-lang-
1.0.1.jar:/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:/opt/
panaces/lib/jacl.jar:opt/panaces/lib/tcljava.jar:/opt/panaces/lib/PF
RAgentCSA.jar:lax.jar
```

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.6.4 Solaris OS Agent

Open SolarisOSAgent.lax file that has been installed in Solaris OS Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= /opt/panaces/lib/commons-lang-
1.0.1.jar:/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:opt/p
anaces/lib/jacl.jar:opt/panaces/lib/tcljava.jar:opt/panaces/lib/Sola
risOSAgentCSA.jar:/opt/panaces/lib/commons-collections-
4.0.jar:/opt/panaces/lib/commons-dbcp-
1.2.1.jar:/opt/panaces/lib/commons-
logging.jar:/opt/panaces/lib/commons-pool-
1.2.jar:/opt/panaces/lib/quartz-all-1.5.2.jar:lax.jar
```

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

kyndryl

32.6.5 SRS Agent

Open **SrsAgent.lax** file that has been installed in Solaris OS Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path=/opt/panaces/lib/commons-lang-
1.0.1.jar:/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:/opt/
panaces/lib/tcljava.jar:/opt/panaces/lib/jacl.jar:.:/opt/panaces/Srs
AgentCSA.jar:lax.jar
```

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.7 Agent Not Starting on Linux Server

Before starting the agent services, check the respective lax files for the agent's class path and java path entries. If these entries are incorrect, edit these files and restart the agents once the agent installation is complete.

Perform any of the following procedures depending on the agent selection.

32.7.1 Kyndryl Resiliency File Replicator Service

Open PFRService.lax file that has been installed in the Kyndryl Resiliency File Replicator Service installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path=                    /opt/panaces/lib/commons-lang-
1.0.1.jar;/opt/panaces/l
ib/PADS.jar;/opt/panaces/lib/log4j.jar;/opt/panaces/lib/jacl.jar;opt
/panaces/lib/tcljava.jar;/opt/panaces/lib/PFR.jar:lax.jar
```

32.7.2 PFR Agent

Before starting the PFR Agent, open PFRAgent.lax file that has been installed in the Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path=                    /opt/panaces/lib/commons-lang-
1.0.1.jar;/opt/panaces/l
ib/PADS.jar;/opt/panaces/lib/log4j.jar;/opt/panaces/lib/jacl.jar;opt
/panaces/lib/tcljava.jar;/opt/panaces/lib/PFRAgentCSA.jar:lax.jar
```

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.7.3 Linux OS Agent

Open LinuxOSAgent.lax file that has been installed in the Linux OS Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

kyndryl

lax.class.path= /opt/panaces/lib/commons-lang-1.0.1.jar;/opt/panaces/lib/PADS.jar;/opt/panaces/lib/log4j.jar;/opt/panaces/lib/jacl.jar;opt/panaces/lib/tcljava.jar;opt/panaces/lib/LinuxOSAgentCSA.jar;/opt/panaces/lib/commons-collections-4.0.jar;/opt/panaces/lib/commons-dbcp-1.2.1.jar;/opt/panaces/lib/commons-logging.jar;/opt/panaces/lib/commons-pool-1.2.jar;/opt/panaces/lib/quartz-all-1.5.2.jar:lax.jar

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.8 Agent Not Starting on AIX Server

Before starting the agent services, check the respective lax files for the agent's class path and java path entries. If these entries are incorrect, edit these files and restart the agents once the agent installation is complete.

Perform any of the following procedures depending on the agent selection.

32.8.1 Kyndryl Resiliency File Replicator Service

Open PFRService.lax file that has been installed in the Kyndryl Resiliency File Replicator Service installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

lax.class.path= /opt/panaces/lib/commons-lang-1.0.1.jar:/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:/opt/panaces/lib/jacl.jar;opt/panaces/lib/tcljava.jar:/opt/panaces/lib/PFR.jar:lax.jar

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.8.2 PFR Agent

Before starting the PFR Agent, open PFRAgent.lax file that has been installed in the Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

lax.class.path=/opt/panaces/lib/commons-lang-1.0.1.jar:/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:/opt/panaces/lib/jacl.jar;opt/panaces/lib/tcljava.jar:/opt/panaces/lib/PFR.jar:/opt/panaces/lib/PFRAgentCSA.jar:lax.jar

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

kyndryl

32.8.3 AIX OS Agent

Before starting the AIX OS Agent, open the AIXOSAgent.lax file that has been installed in the Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

lax.class.path=/opt/panaces/lib/commons-lang-1.0.1.jar:

/opt/panaces/lib/PADS.jar:/opt/panaces/lib/log4j.jar:

/opt/panaces/lib/jacl.jar;/opt/panaces/lib/tcljava.jar:/opt/panaces/lib/commons-collections-4.0.jar:/opt/panaces/lib/commons-dbcp-1.2.1.jar:/opt/panaces/lib/commons-logging.jar:/opt/panaces/lib/quartz-all-1.5.2.jar:/opt/panaces/AIXOSAgentCSA.jar:lax.jar

Check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.9 Agent Not Starting on HPUX Server

Before starting the agent services, check the respective lax files for the agent's class path and java path entries. If these entries are incorrect, edit these files and restart the agents once the agent installation is complete.

Perform any of the following procedures depending on the agent selection:

32.9.1 Kyndryl Resiliency File Replicator Service

Open PFRService.lax file that has been installed in the Kyndryl Resiliency File Replicator Service installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= /opt/panaces/lib/commons-lang-
1.0.1.jar;/opt/panaces/lib/
PADS.jar;/opt/panaces/lib/log4j.jar;/opt/panaces/lib/jacl.jar;o
pt/panaces/lib/tcljava.jar;/opt/panaces/lib/PFR.jar:lax.jar
```

32.9.2 PFR Agent

Before starting the PFR Agent, open PFRAgent.lax file that has been installed in the Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= /opt/panaces/lib/commons-lang-
1.0.1.jar;/opt/panaces/lib
/PADS.jar;/opt/panaces/lib/log4j.jar;/opt/panaces/lib/jacl.jar;
opt/panaces/lib/tcljava.jar;/opt/panaces/lib/PFRAgentCSA.jar:la
x.jar
```

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.9.3 HPUX OS Agent

Open HPUXOSAgent.lax file that has been installed in the Linux OS Agent installation path with a text editor. Check if LAX.CLASS.PATH has the following class path:

```
lax.class.path= /opt/panaces/lib/commons-lang-
1.0.1.jar;/opt/panaces/lib/PAD
S.jar;/opt/panaces/lib/log4j.jar;/opt/panaces/lib/jacl.jar;opt/
panaces/lib/tcljava.jar;opt/panaces/lib/LinuxOSAgentCSA.jar;/op
t/panaces/lib/commons-collections-
4.0.jar;/opt/panaces/lib/commons-dbcp-
1.2.1.jar;/opt/panaces/lib/commons-
logging.jar;/opt/panaces/lib/commons-pool-
1.2.jar;/opt/panaces/lib/quartz-all-1.5.2.jar:lax.jar
```

Also, check for the java installation path displayed under LAX.NL.CURRENT.VM.

32.10 Resiliency Orchestration HA Replication Monitoring

Issue - While monitoring the status of the HA replication using the RO UI, the user is getting an error unable to update the query.

Workaround – Perform these steps -

a. On the Primary RO server, at the mysql prompt, execute these commands (replace <Primary RO IP> with the actual primary RO server IP address) –

```
grant replication client on *.* to 'panaces'@'<Primary RO IP>';
grant replication client on *.* to 'panaces'@'localhost';

flush privileges;
```

b. Restart the RO services.

Monitor HA –

The admin can monitor the replication status manually on the backend using standard mysql commands as given below –

a. On the Primary RO server, log in to mysql and execute the command -

```
show mater staus;
```

b. On the Standby RO server, log in to mysql and execute the command -

```
show slave status\G;
```

32.11 Network Address Translation (NAT IP)

NAT is designed for IP address conservation. It allows private IP networks that use unregistered internal IP addresses to connect to the Internet.

Enter the IP addresses of the primary and secondary Kyndryl Resiliency Orchestration servers and the Kyndryl Resiliency Orchestration Agent Node Address. In a non-NAT environment, the NAT IP address should be left blank.

In a NAT environment, primary and secondary Resiliency Orchestration Server's public IP should be provided. Resiliency Orchestration Agent node address should be the public IP, and the NAT IP address should be the private IP of the server where you are installing.

> **Note**
>
> Manual Configuration of NAT IP is not provided during installation.

32.11.1 CFG file for NAT IP

Example Kyndryl Resiliency Orchestration CFG file for NAT IP

```
PANACES_MASTER_SERVER_ADDRESS=<Resiliency Orchestration IP>//priv IP
of Resiliency Orchestration

PANACES_SLAVE_SERVER_ADDRESS==<Resiliency Orchestration IP>//priv IP
of Resiliency Orchestration

PANACES_AGENT_NODE_ADDRESS==<Resiliency Orchestration IP>//priv IP of
Resiliency Orchestration

PANACES_AGENT_NODE_BIND_ADDRESS=           //leave empty
```

- Discover agent node using "PANACES_AGENT_NODE_ADDRESS"
- Discover PR & DR using their public IP

Example Local Agent CFG file for NAT IP

```
PANACES_MASTER_SERVER_ADDRESS==<Resiliency Orchestration IP> //public
IP of Resiliency Orchestration

PANACES_SLAVE_SERVER_ADDRESS==<Resiliency Orchestration IP>  //public
IP of Resiliency Orchestration

PANACES_AGENT_NODE_ADDRESS==<Resiliency Orchestration IP>   //public
IP of PR/DR (this server)
```

```
PANACES_AGENT_NODE_BIND_ADDRESS==<Resiliency Orchestration IP>
//private IP of PR/DR (this server)
```

Example PFR Configuration CFG file for NAT IP

```
PUBLIC IP: =<Resiliency Orchestration IP>//private IP of PR/DR
```

Site controller configuration for NAT IP in the local agent

```
In case the Site controller is configured with NAT_IP, you will need
to include the following property in the Local Agent
PanaceAgentGenric.cfg file.

"PANACES_SITE_CONTROLLER_NATIP_ADDRESS= <NAT_IP of the site
controller>"
```

32.12 Web Browser Displays Certificate Error

If the secure protocol is used to access the Kyndryl Resiliency Orchestration application and you have used the default certificate provided by Kyndryl, the web browser will display the certificate error. If you proceed further with this certificate, the web browser displays the certificate error. Sometimes, you may not be able to access the application. In this case, you need to obtain a certificate from a certifying authority and import the same into the Sanovi keystore.

32.13 Server Installation Fails with UnsatisfiedLinkError

While Installing the Kyndryl Resiliency Orchestration, the user may encounter the following UnsatisfiedLinkError:

IAResourceBundle: create resource bundle: en 'SWING' UI not supported by VM.
java.lang.UnsatisfiedLinkError:
/tmp/install.dir.30775/Linux/resource/jre/lib/i386/xawt/libmawt.so: libXext.so.6:
cannot open shared object file: No such file or directory at
java.lang.ClassLoader$NativeLibrary.load(Native Method)

This is due to the 32-bit rpm requirement from the Installer, required 32-bit rpms (libXext-1.1-3.el6.i686.rpm libX11-1.3-2.el6.i686.rpm libxcb-1.5-1.el6.i686.rpm libXau-1.0.5-1.el6.i686.rpm libXtst-1.0.99.2-3.el6.i686.rpm libXi-1.3-3.el6.i686.rpm) should be installed to continue installation.

32.14 Port Forwarding

32.14.1 Verify Firewall Status

The following are details to verify the Firewall status.

```
[sanovi@sbrphln02 lic]$ sudo systemctl status
firewalld.service
â firewalld.service - firewalld - dynamic firewall daemon
```

```
Loaded: loaded (/usr/lib/systemd/system/firewalld.service;
disabled; vendor preset: enabled)
Active: active (running) since Wed 2017-09-06 23:47:29 IST; 1
day 14h ago
Docs: man:firewalld(1)
Main PID: 29752 (firewalld)
CGroup: /system.slice/firewalld.service
ââ29752 /usr/bin/python -Es /usr/sbin/firewalld --nofork --
nopid
Sep 06 23:47:28 sbrphln02 systemd[1]: Starting firewalld -
dynamic firewall daemon...
Sep 06 23:47:29 sbrphln02 systemd[1]: Started firewalld -
dynamic firewall daemon.
[sanovi@sbrphln02 lic]$
```

32.14.2 Add Exception to Firewall

The following are details to add an exception to the firewall.

```
sudo firewall-cmd --zone=public --add-port=443/tcp --permanent

sudo firewall-cmd --zone=public --add-port=22/tcp --permanent

sudo firewall-cmd --zone=public --add-port=42443/tcp --permanent

sudo firewall-cmd --zone=public --add-port=45443/tcp --permanent

sudo firewall-cmd --zone=public --add-port=8083/tcp --permanent

sudo firewall-cmd --zone=public --add-port=8081/tcp –permanent

sudo firewall-cmd --zone=public --add-port=135/tcp --permanent
```

32.14.3 Open Ports

The following are details to list the ports, which are open to access.

```
[root@sbrphln02 httpd]# firewall-cmd --list-all
 public (active)
 target: default
 icmp-block-inversion: no
 interfaces: enp3s0f0
 sources:
 services: dhcpv6-client ssh
```

```
  ports: 42443/tcp 45443/tcp 443/tcp  22/tcp 8081/tcp 8083/tcp
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
[root@sbrphln02 httpd]#
```

32.15 Create Server Certificate and Server Private Key Reference

The following snippet shows the details for creating a server certificate and server private key reference:

```
openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
-keyout /opt/tomcatX/conf/ibm.key -out
/opt/tomcatX/conf/ibm.crt -subj "/O=IBM
Corporation/OU=PS/CN=<hostname.domainname.com>" -config
"/etc/pki/tls/openssl.cnf"
```

32.16 Analyze HTTPD Logs

The following are details to see httpd logs:

```
journalctl -xe

/bin/systemctl status  httpd.service    ( for checking the
status of httpd service )

Ref:

-- Unit user-0.slice has begun shutting down.

Sep 10 00:51:42 sbrphln02 sudo[10839]:   sanovi : TTY=pts/0 ;
PWD=/etc/httpd/conf.d ; USER=root ; COMMAND=/bin/bash

Sep 10 00:51:43 sbrphln02 dbus-daemon[840]: dbus[840]:
[system] Activating service name='org.freedesktop.problems'
(using servicehelper)

Sep 10 00:51:43 sbrphln02 dbus[840]: [system] Activating
service name='org.freedesktop.problems' (using servicehelper)

Sep 10 00:51:43 sbrphln02 dbus-daemon[840]: dbus[840]:
[system] Successfully activated service
'org.freedesktop.problems'
```

```
Sep 10 00:51:43 sbrphln02 dbus[840]: [system] Successfully
activated service 'org.freedesktop.problems'
[root@sbrphln02 ~]#
```

32.17 Install httpd, SSL Packages

32.17.1 Download/Mount the Operating System ISO

```
mailcap-2.1.41-2.el7.noarch.rpm
httpd-tools-2.4.6-31.el7.x86_64.rpm
httpd-2.4.6-31.el7.x86_64.rpm
mod_ssl-2.4.6-45.el7.centos.x86_64.rpm
```

32.17.2 Install the httpd, SSL Packages

```
rpm -ivh mailcap-2.1.41-2.el7.noarch.rpm httpd-2.4.6-
31.el7.x86_64.rpm httpd-tools-2.4.6-31.el7.x86_64.rpm
rpm -ivh mod_ssl-2.4.6-45.el7.centos.x86_64.rpm
```

32.18 Site Controller connection error

The Kyndryl Resiliency Orchestration UI displays site controller not connected error and does not resolve following a successful Site Controller restart. This error generally appears in certain instances which includes but are not limited to:

- The Site Controller was taken down intentionally.
- Kyndryl Resiliency Orchestration was upgraded.
- Related services were stopped.

The usual root cause for this error is that the server cache is not refreshed post the Site controller disconnection.

32.18.1 Resolution

Restart the Kyndryl Resiliency Orchestration application server. Please refer to the topic Starting and Stopping Kyndryl Resiliency Orchestration Server Services in the Kyndryl Resiliency Orchestration Admin Guide to restart the server.

32.19 Archiving the Resiliency Orchestration Anomaly Detection (ROAD) Raw Data

This utility is used to perform the following tasks.

- Archive the Resiliency Orchestration Anomaly Detection (ROAD) raw data database(raw_data) into an archive database(raw_data_archive) based on the retention criteria. Archiving is required to ensure that the ROAD application runs efficiently.
- Clean up the data in the archive database based on the retention criteria to maintain optimal disk space.

The following are the retention criteria available.

Note: The retention criteria can be applied for both archiving and cleanup procedures.

Retention Criteria	Description
Number of days of data to be retained	This criterion ensures that only those scanned VM snapshots which have a timestamp greater than or equal to the current timestamp – the number of days of data will be retained. If this is impacting all the VM snapshots, then the latest two snapshots will not be archived. **Example:** If there are VM snapshots every day and the current timestamp has the date of Dec 23rd, 2021 and the number of days of data is set as 10, then all the snapshots before Dec 13th, 2021 will be archived.
Number of jobs (per VM) to be retained	This criterion will apply after the above criteria 1 is executed. This criterion will ensure only the specified number of snapshots are retained. If the number of VM snapshots is less than this number of jobs set, then no action will be taken. **Example:** Based on criteria 1, if there are 10 snapshots for a VM present after Dec 13th, 2021 and if the number of jobs is set as 2, then only recent 2 VM snapshots will be retained, and others will be archived.

Prerequisite

You should have admin privileges to perform this procedure.

Steps:

1. Copy the *purge_util.tar.gz* to the ROAD Central/Management VM setup box and then un-tar the same to a folder.

   Note: The tar file is available in the Jforg repository.

2. Go to the un-tarred location and run *changePw.py* as below:

   ```
   python changePw.py
   Password: <Enter the root DB user password>
   ```

3. Run the below command to install the dependencies (only once).

   ```
   pip install -r requirements.txt
   ```

4. To get help on this purge, run the script with –the help option below.

   ```
   python purge_raw_util.py -help

   usage: purge_raw_util.py [-h] [--retention_days RETENTION_DAYS]
                            [--retention_jobs RETENTION_JOBS]
                            [--purge_db {RAW,RAW_ARCHIVE}]


   optional arguments:
   -h, --help            show this help message and exit
   --retention_days RETENTION_DAYS
                         number of days of data to be retained, the default
value
                         is 10
   --retention_jobs RETENTION_JOBS
                         number of scan jobs for a vm to be retained, default
                         value is 2
   --purge_db {RAW,RAW_ARCHIVE}
                         the database to be purged(RAW or RAW_ARCHIVE),
default
   ```

```
value is RAW
```

5. Configure the cron as required to the *purge_raw_util.py* as scheduled.
   Note: Please schedule the cron job to run at a non-peak hour, when there's no backup taken or the VM snapshot scan is not performed.

   For example:

```
0 0 * * * python purge_raw_util.py --retention_days 20 --
retention_jobs 5 --purge_db RAW
```

```
The above example will run every day at midnight.
```

Functional Details:

- To archive, the **raw_data**, pass the value *RAW* for the argument *purge_db* (default is *RAW* if not passed). This will archive the data from *raw_data* to *raw_data_archive* based on the retention criteria provided.
- To purge the **raw_data_archive**, pass the value *RAW_ARCHIVE* for the argument *purge_db* (default is *RAW* if not passed). This will purge the entries in *raw_data_archive* based on the retention criteria provided.

.

32.20 Removing Older Jars from Backup folder in production Server

After completing the Upgrade & Sanity tests in the Production server, the older log4J jars must be removed from the backup folder.

32.20.1 Resolution

After the log4J2 migration in the production server, remove the below listed log4J jar files from the backup folder:

- log4j-1.2.15.jar
- log4j-1.2.17.jar

- log4j.jar
- apache-log4j-extras-1.2.17.jar

33 Recommendations for Site Controller (SC) High Availability for Linux and Windows

33.1 Snapshot Based

Perform the following steps to set up and take the initial snapshot of the Site Controller:

1. Install Site Controller on a Virtual Machine (VM).
2. Start Installation of Site Controller.
3. Configure Site Controller on RO.
4. Map the Subsystems with Site Controller.
5. Shutdown Site Controller machine (it reduces the time taken for snapshots).
6. Take a snapshot of the Site Controller VM.
7. Start the Site Controller VM.
8. Start the Site Controller services.
9. Steps 5 to 8 must be repeated if any changes in the Site Controller VM and Site Controller are in a good state.

   Perform the following steps for Site Controller to revert to a Snapshot (the time when the Site Controller was in a good state):

   Note: If the Site Controller has any issues and wants to go back in time when it was working fine.

1. Login to VM Management console.
2. Identify the Site Controller VM and revert the VM to the latest good snapshot.
3. Start the Site Controller VM.
4. Start the Site Controller services.

33.2 Clone based

Perform the following steps to set up and take the initial snapshot of the Site Controller:

1. Install Site Controller on a Virtual Machine (VM).

2. Start Installation of Site Controller.
3. Configure Site Controller on RO.
4. Map the Subsystems with Site Controller.
5. Shut down the virtual machine (optional).
6. Clone the Site Controller VM.
7. Start the Site Controller VM.
8. Start the Site Controller services.
9. Steps 5 to 8 must be repeated if any changes to the Site Controller VM and Site Controller are in a good state, create a new clone and delete the older clone.

   Perform the following steps to start a cloned VM (latest cloned VM):

   Note: If the Site Controller has any issues and wants to go back in time when it was working fine.

1. Login to VM Management console.
2. Shut down the malfunctioning Site Controller VM.
3. Start the cloned Site Controller VM.
4. Start the Site Controller services.

Note: In case the snapshot is taken without shutdown, the VM will require a restart after reverting it to a snapshot.

34 License Information

34.1 GPL License Information

If you wish to access the source code for any of these packages, it is recommended that you visit the official download site of the package maintainer directly. A link to each download site appears in the table below. These links are provided "as-is" and will take you to sites that are not owned or controlled by Kyndryl. Kyndryl is not accountable for the contents of these sites and is not acting as a distributor of the code on such sites. Kyndryl in no way warrants that the code or other information on these sites is accurate, will function in a particular manner, or is non-infringing of a third party's intellectual property rights. Please contact the maintainers of the code for information on the licenses and documentation that accompany the source code distributed from their site.

Open source licenses such as GNU Public License (GPL) require that Kyndryl makes the source available on request by the client. For packages with such licenses, the client must either go to the official site of the source or download the information from this link: https://sourceforge.net/projects/gnu-utils/files/binaries/.

In addition to GPL, each of these packages includes its licensing information. It is essential to understand the terms and conditions of the licensing information of the individual tools.

35 Known limitation

35.1 Service getting stopped automatically

After successful installation of PFR, the Service is getting stopped automatically in the Windows server.

Workaround:

After installation, in the *$SFRROOT/SFR/installconfig/PFRConfiguration.cfg* file, the following parameter must have proper separator like "//".

SSL_KEYSTORE_FILE

In the prop file it must be mentioned as the file:

SSL_KEYSTORE_FILE= *$SFRROOT*//SFR//Installconfig//pfr.keystore

This known limitation is appearing because currently, this parameter is showing:
SSL_KEYSTORE_FILE = *$SFRROOT*\SFR/installconfig/pfr.keystore

35.2 Backup and Restore of Metadata

Using RO UI, you can back up the metadata on the same machine and restore it on the same machine. However, this metadata from one machine will not be useful on a different machine due to database restrictions.

Perform the following procedures for backup and restore of the metadata.

Backup and Restore of Metadata on the Same Machine

The following is the known limitation to backup and restore the metadata on the same machine:

Problem Statement: This error occurs after backing up the data and while restoring the metadata on the same machine due to a database error.

Error Message: During metadata restore, the following error appears:

```
1418 (HY000) at line 26302: This function has none of DETERMINISTIC,
NO SQL, or READS SQL DATA in its declaration, and binary logging is
enabled (you *might* want to use the less safe
log_bin_trust_function_creators variable)
```

Workaround:

1. Comment the binary log parameters from **/etc/my.cnf**.
2. Execute the following command:

```
sudo ./enableEncryptionOnTables.sh "dec" "<DB root user password>"
```

3. Execute the following command to restart MariaDB services.

```
sudo systemctl restart mysql
```

4. Restore the metadata now.

kyndryl

Backup and Restore of Metadata on a Different Machine

The following are the known limitations to backup and restore the metadata on any different machine such as HA or RO Standby server.

Issue 1: Metadata restore issue with the RO UI

Problem Statement: This error occurs during RO upgrade, migration, and HA. This error occurs after retrieving the metadata from the RO UI and while restoring the data manually from the same machine or a different machine.

The following error appears while retrieving the mysql data from the RO and trying to restore the metadata.

Error message:

```
Error 1005(HY000) at line 10993: can't create table 'panaces'.'action'
(errno: 140 "Wrong create options")
```

Workaround:

1. Execute the following command before retrieving mysql metadata backup from the RO and decrypt the db table.

   ```
   sudo ./enableEncryptionOnTables.sh "dec" "<DB root user password>"
   ```

2. Retrieve the data from RO, copy it to the destination RO, and restore the metadata.

Note: It is mandatory to decrypt the db table before retrieving metadata from the Admin RO UI. Else the error persists, and the metadata will not be useful unless it is taken after decrypting the tables.

Issue 2: Metadata restore issue on the Standby Server

Problem Statement: This error occurs while taking backup of any other machine such as a Standby server using RO UI.

An error occurs in the table, 'ext_client_config' while executing the insert query on the Standby server. This error occurs while applying the Primary database on the Standby server due to HASH encryption enabled on the table 'ext_client_config' with a unique key.

Error Message:

The following error message appears:

```
ERROR 1032 (HY000) at line 41: Can't find record in
'ext_client_config'
```

Workaround:

Perform the following steps manually to resolve the issue:

1. Alter the table, 'ext_client_config' to enable the keys, before inserting rows into the table.

```
/*!40000 ALTER TABLE `ext_client_config` ENABLE KEYS */;
```

2. Edit the Primary database records before applying on the Standby server, as per the following steps:

- From the Primary database, exclude the table **'ext_client_config'**.
- Include the **--ignore-table** flag in the database command and apply the changes on the Standby.
- From the **'ext_client_config'** table, edit the record and add a query to enable keys before insert the query.
- Apply the same changes on the Standby server.

35.3 Socket Read timeout error during synchronize file set

The Normal full copy is failing with Socket read time out exception error during synchronizing file set.

Problem Statement:

This error occurs due to a Socket Read timeout error during synchronize fileset operation. The synchronization task takes more time to finish the operation and the completion time is more than the specified time of 120 seconds.

Error Message:

```
Action execution failed. Inform on action completion is configured. The
workflow requires User Input.

Normal full copy operation failed for the group SFR_Rept_DMSApp_New
```

Workaround:

Ensure to not specify any time limit for such an operation because the Synchronize file set operation will complete depending on the file size.

Perform the following steps as a workaround:

1. Navigate to the Control Panel and select the **System** option.
2. In the System window, scroll to the bottom and click the **About** option.

3. In the About window, click the **Advanced System Settings** link at the bottom of the **Device Specifications** section.

4. In the **System Properties** window, click the **Advanced** tab, then click the **Environment Variables** button at the bottom of the tab.

5. Click **New** under **System**, Add `PANACES_SOCKET_TIMEOUT` as variable and "**0**" as value.

6. Click Save and apply.

7. To test whether the value got added properly, open cmd as administrator and execute the following command:

```
echo %PANACES_SOCKET_TIMEOUT%
```

35.4 MSSQL Local Agent dataset discovery process fails

The MSSQL Local Agent dataset discovery process fails.

Problem Statement:

The driver could not establish a secure connection to SQL Server by using Secure Sockets Layer (SSL) encryption and fails with the following error message.

Error Message:

"`SQL Server returned an incomplete response. The connection has been closed.`"

Workaround:

- Change the MSSQL JDBC jar from sqljdbc41.jar to mssql-jdbc-8.4.1.jre8.jar and ensure that the MSSQL Local Agent discovery on Windows 2019 is successful.
- Remove TLS1.1, TLS1.2, and SSL from java certs.

35.5 PasswordUpdater.sh script is non-functional

Currently, the passwordupdater.sh script is non-functional. So, Kyndryl recommends to perform the steps as mentioned in the section Changing Default Passwords (Recommended) to change the default passwords.

35.6 HA Configuration fails

The HA Configuration fails because of duplicate entries in the Panaces db in Master server.

Problem Statement:

The HA configuration fails displaying "error 1062" due to duplicate entries in the panaces.incident.log file.

Workaround:

As a workaround, add the following lines in the **my.cnf** file of the Slave server.

The replication is enabled.

```
slave-skip-errors=1062
skip-slave-start
```