



Kyndryl Resiliency Orchestration

Quick Install Guide

Version 8.4.6.0

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

©Copyright Kyndryl, Inc. 2003, 2023.

Printed December 2023.

Use, copy, and distribution of any Kyndryl software described in this publication need an applicable software license.

No part of this product or document may be reproduced, stored in a retrieval system, or transmitted, in any form by any means, electronic, mechanical, photocopy, recording, or otherwise, without the prior written authorization of Kyndryl and its licensors, if any.

TRADEMARK INFORMATION

Kyndryl and the Kyndryl logo are trademarks or registered trademarks of Kyndryl, Inc. in many jurisdictions worldwide. Other product and service names included herein may be trademarks of Kyndryl or other companies.

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



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
8.2.3	September 2021	All sections created
8.2.6	December 2021	RO Simple Architecture Diagram
		Installation Steps Diagram Updated
		JDK Support table added
		Tomcat Support table added
		Corrected MariaDB contents
		Note added in the section Installing Third-Party Dependencies for Site Controller
		Updated to Tomcat 9.0.54
		Updated to jdk1.8.0_311
8.2.7	January 2022	RHEL version 8.5 was added in the table under the section Prerequisites > Supported Versions of Different Components and platforms, Page 9
		Note deleted under section Prerequisites > Supported Versions of Different Components and platforms, Page 9
8.3.5	November 2022	Updated the section "Running the SecurityUserInjection.sh script on Page 29.Added a new section "Configuring the Catalina.sh file" on Page 32.RO-50332
		Included a Note in the section "Setting up Tomcat Environment – setenv.sh" on Page 26.RO-50332



Document Version	Revision Date	Sections Updated
		Updated the section with the latest Tomcat version in the section “Supported Versions of Different Components and Platforms” on Page 11 RO-50613
		Updated the section with the latest RHEL version in the “Supported Versions of Different Components and platforms” RO-50614
		Updated the section with the latest MariaDB version in the “Supported Versions of Different Components and platforms” RO-50612
8.3.8	February 2023	Updated Support matrix table page 11
8.3.9.0	March 2023	Support matrix updated RHEL 9.1, MariaDB 10.5.19, Tomcat 9.0.72
		Java version updated jdk1.8.0_362
		Added in properties file table: This concurrentRequestProcessCountMax property should be equal or greater than concurrentRequestProcessCount
8.3.11.0	May 2023	Updated jdk to 1.8.0_372
		Updated Architecture diagram with port details
		Updated MariaDB 10.5.20 Tomcat 9.0.73
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 – Prerequisites – Added a note.
8.4.1.0	July 2023	Tomcat 9.0.76 Maria DB 10.5.21 updated
8.4.2.0	August 2023	Open JDK:(Zulu 8.70.0.24-SA-linux64) (build 1.8.0_382-b05)
8.4.4.0	October 23	Tomcat 9.0.80 updated



Document Version	Revision Date	Sections Updated
8.4.5.0	November 23	Tomcat 9.0.82 updated OpenJDK Runtime Environment (build 1.8.0_392). Maria DB: 10.5.22
8.4.6.0	December 23	Support matrix updated RHEL 9.3 (Plow) Tomcat-9.0.83
		Added in support matrix RHEL 8.8, MariaDB 10.5.21, Tomcat 9.0.72



TABLE OF CONTENTS

Introduction	8
Limitations of this Document	8
How to Use this Guide	8
Deployment Architecture	10
Typical implementation of Resiliency Orchestration	11
Port Requirements	12
Prerequisites	12
Java versions used in the Kyndryl Resiliency Orchestration Software package	12
Supported Versions of O/S, D/B, and Web Server	13
Hardware Requirements	14
Software Requirements.....	16
Downloading the Kyndryl Resiliency Orchestration Software Package	16
Editing the Properties File	17
Subscribe System to Red Hat Subscription	23
Installing Essential Administration Utility Packages	23
Installing MariaDB	25
Downloading required packages.....	25
Installing MariaDB packages.....	26
Configuring MariaDB.....	26
Setting Up MariaDB Root Password.....	26
Installing Apache Tomcat Server	27
Post Install Configuration	28
Setting up Tomcat Environment – setenv.sh	28
Setting up Java Home and JRE Home variables.....	29
Installing Third-Party Dependencies	31
Running the SecurityUserInjection.sh script	31
Configuring the Tomcat server.xml file	32
Configuring the Catalina.sh file	34
Configuring the PanacesGUI web.xml file	35
Starting the Kyndryl Resiliency Orchestration Server.....	35
Logging into the Kyndryl Resiliency Orchestration Server.....	36
Allow-listing Commands or Kyndryl Resiliency Orchestration Server	37
Kyndryl Resiliency Site Controller Installation	40
Installing Red Hat Linux for Site Controller	40
Pre-requisites for Installing the Site Controller.....	40
Installing Third-Party Dependencies for Site Controller	40
Installing Site Controller on Red Hat Linux in Silent Mode	41
Post Install Configuration	43
Verify Site Controller Status.....	44
Installing Site Controller Server or Site Controller in MS Windows	44



Installation and Services	44
Pre-requisites for Installing the windows Site Controller.....	44
Installing Site Controller in Windows in Silent Mode.....	45
Post Installation Steps after you install the Site Controller in Windows.....	46
Recommended Security Steps	49



Introduction

This document provides a quick Step-by-Step procedure for installing, configuring, and verification of the Kyndryl Resiliency Orchestration Server and the Kyndryl Resiliency Site Controller on Red Hat Enterprise Linux.

Limitations of this Document

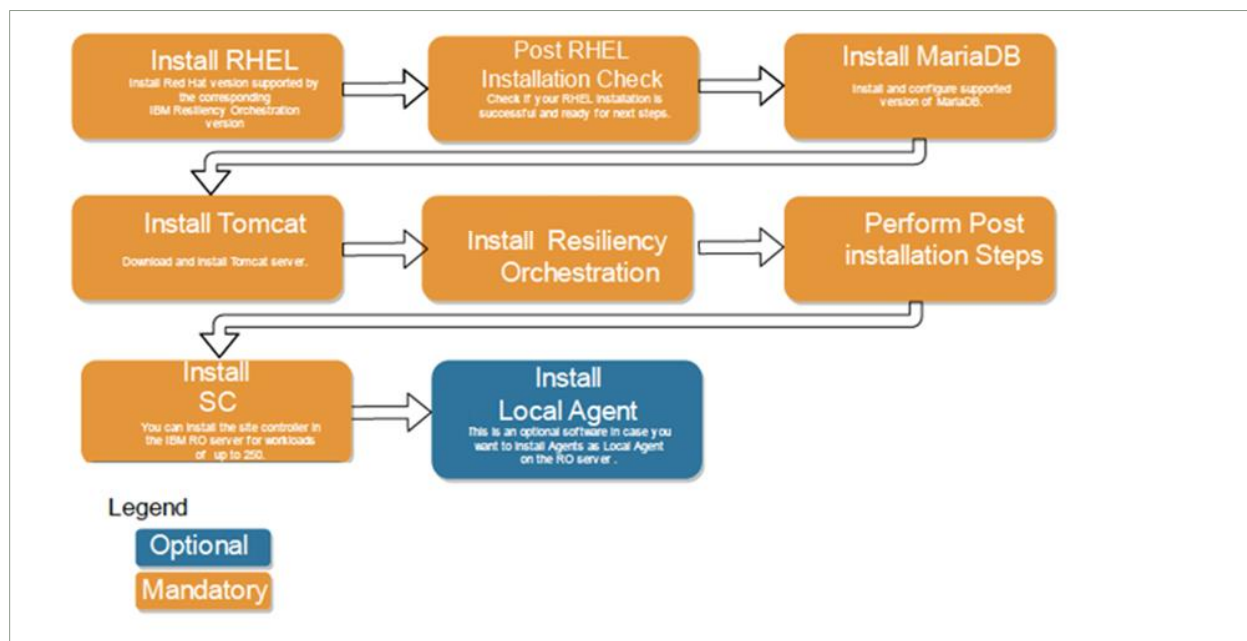
While this guide will quickly get you started with the installation process, it is not a substitute for the regular installation guide. It may not cover the following content but is not limited to:

- Kyndryl Resiliency Orchestration installation in graphical mode.
- Kyndryl Resiliency Site Controller installation in graphical mode.
- Setting up remote site controller.
- Agent Installation on various operating systems.
- Troubleshooting corner cases.
- Port forwarding.
- Secure connection-related information.
- Creating NICRA/SA OVA.

For more detailed information, please refer to the Kyndryl Resiliency Orchestration Installation Guide.

How to Use this Guide

The instructions given in this quick install guide pertain to the Kyndryl Resiliency Orchestration version and should be followed sequentially.



The following table lists the topics covered in this document in sequence.

S No.	Section Name	The intent of the section
1.	Prerequisites	This section covers the hardware and software requirements for the installation of Kyndryl resiliency orchestration.
2.	Installing Red Hat Enterprise Linux	This Section assists the user with installation and required settings for RHEL
3.	Post-install steps for Red Hat Enterprise Linux	This section covers the tasks you will need to perform after you have installed RHEL. This section ensures that your setup is ready for Maria DB and Tomcat Installations.
4.	Installing MariaDB	This section details topics that will guide you to download, install, and configure MariaDB supported by Kyndryl Resiliency Orchestration.
5.	Installing Apache Tomcat Server	This section covers steps to download and install a supported Tomcat supported by Kyndryl Resiliency Orchestration.
6.	Downloading the Kyndryl Resiliency Orchestration Software Package	This section covers various methods of downloading the Kyndryl Resiliency Orchestration software package.



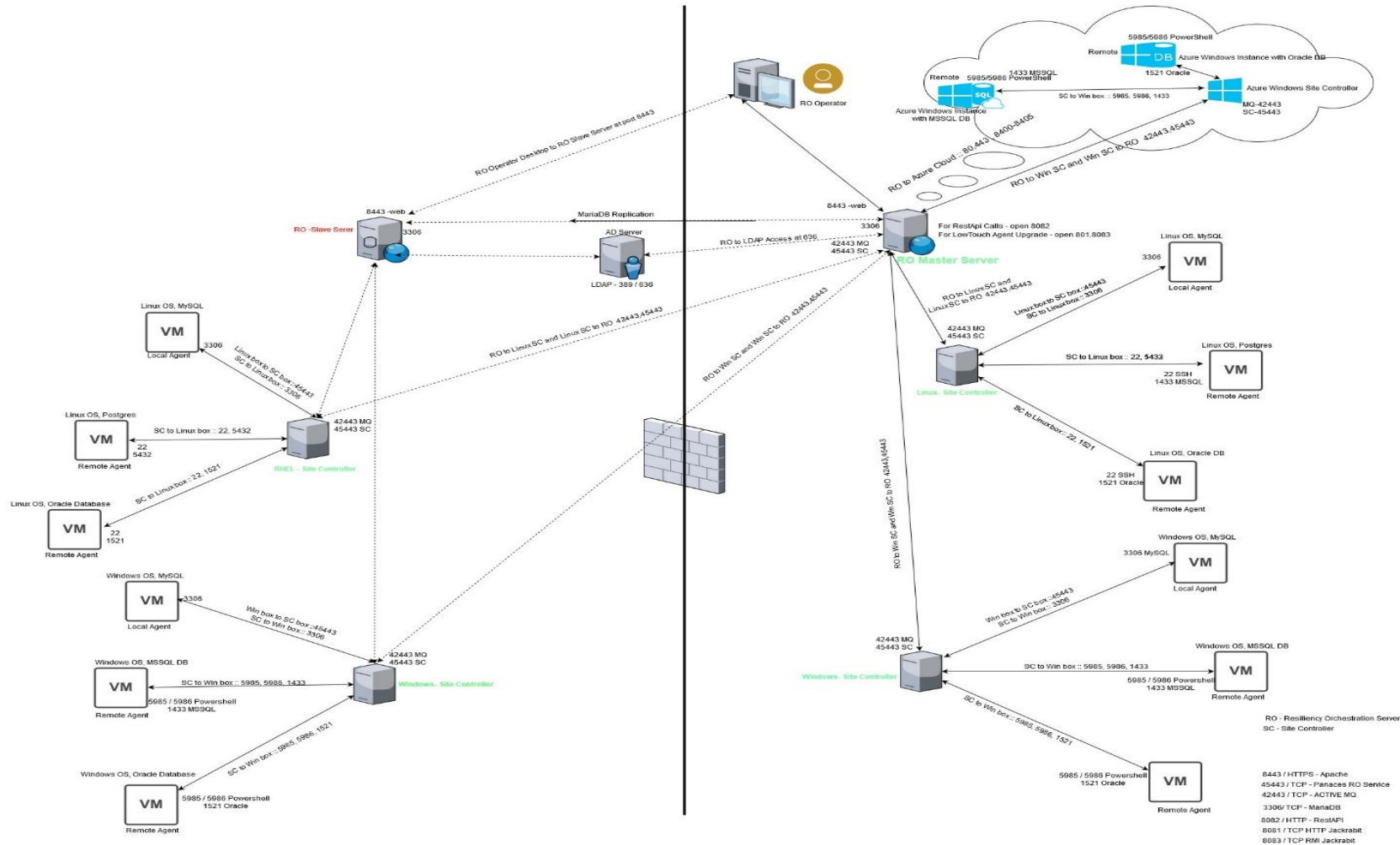
7.	Installing Kyndryl Resiliency Orchestration Server	This section covers the steps to install the Kyndryl Resiliency Orchestration server in silent mode.
8.	Post Install Configuration	Several final steps need to be completed after the Kyndryl Resiliency Orchestration Server has been installed. These are primarily to complete the configuration of the Tomcat server installed earlier.
9.	Kyndryl Resiliency Site Controller Installation	Covers the silent mode as well as the GUI mode of installation of the Site Controller.
10.	Post Install Configuration	Covers some of the tasks that need to be performed after installing the Site Controller.

Deployment Architecture

The following diagram depicts the typical deployment architecture.



Typical implementation of Resiliency Orchestration



**Note:**

- One RO Server can manage multiple Site Controllers; however, one Site Controller can be managed by only one RO Server
- One endpoint should be managed by only one Site Controller

Port Requirements**Mandatory ports for RO Server**

- Inbound 8443 is needed for GUI access depending on Tomcat configuration.
- Bidirectional ports 45443 and 42443 are needed for the connectivity of Site Controller(s). Port 42443 is needed for ActiveMQ.
- Inbound 45443 on-site controllers for Agents to connect.
- Bidirectional 3306 between the primary RO Server and its corresponding Standby RO Server.

Mandatory ports for Site Controller

- Bidirectional 42443 and 45443 are needed for the connectivity of agents from each endpoint. Port 42443 is needed for ActiveMQ.
- Ports for an endpoint.
- Technology-specific ports are needed for remote management.

Prerequisites

The Kyndryl Resiliency Orchestration Server requires the following Hardware and Software prerequisites in a production environment.

Note:

- For a more detailed prerequisite, interoperability, and compatible OS, DB, web server, and JAVA version, refer to the **Kyndryl Resiliency Orchestration Installation Guide**.
- 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.

Java versions used in the Kyndryl Resiliency Orchestration Software package



Java Version	OS Version	Remarks
OpenJDK Runtime Environment (build 1.8.0_392).	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

Supported Versions of O/S, D/B, and Web Server

Server and Components	O/S Platform	D/B Platform	Web Server
	RHEL 9.3 (Plow)	Maria DB: 10.5.22	Tomcat 9.0.83
Kyndryl Resiliency Orchestration Server	RHEL 9.2 (Plow)	Maria DB: 10.5.22	Tomcat 9.0.82
	RHEL 9.2 (Plow)	Maria DB: 10.5.21	Tomcat 9.0.80
	RHEL 9.2 (Plow)	Maria DB: 10.5.21	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 8.8	MariaDB 10.5.21	Tomcat 9.0.72
	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



Server and Components	O/S Platform	D/B Platform	Web Server
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, Windows 2019, Windows 2022	Not applicable	Not applicable
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

Hardware Requirements

You will need the following hardware based on the number of endpoints needed.

Production Endpoints	Kyndryl Resiliency Orchestration Server (with cohosted Site Controller)	Additional Linux Site Controllers	Windows Site Controllers
		Additional Linux Site Controllers and Windows Site Controllers might be needed to manage endpoints.	
	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 Endpoints	CPU: 6 Core RAM 16GB	Not Required	CPU: 2 Core RAM: 16GB



Production Endpoints	Kyndryl Resiliency Orchestration Server (with cohosted Site Controller)	Additional Linux Site Controllers	Windows Site Controllers
	Disk: 150GB Total, 50GB for Binaries/Logs, 50GB for MariaDB and 50GB for Site Controller		Disk: 50GB Total
50 to 100 Endpoints	CPU: 6 Core RAM 24GB Disk: 250GB Total, 100GB for Binaries/Logs, 50GB for MariaDB and 100GB for Site Controller	Not Required	CPU: 2 Core RAM: 16GB Disk: 100GB Total
100 to 250 Endpoints	CPU: 8 Core RAM 40GB Disk: 350GB Total, 150GB for Binaries/Logs, 50GB for MariaDB and 150GB for Site Controller	Not required	CPU: 4 Core RAM: 32GB Disk: 200GB Total
250 to 500 Endpoints	CPU: 12 Core RAM 48GB Disk: 500GB Total, 250GB for Binaries/Logs, 100GB for MariaDB and 150GB for Site Controller	CPU: 4 Core RAM: 32GB Disk: 200GB Total	CPU: 4 Core RAM: 48GB Disk: 350GB Total
500 to 1000 Endpoints	CPU: 12 Core RAM 64GB Disk: 600GB Total, 350GB for Binaries/Logs, 100GB for MariaDB and 150GB for Site Controller	CPU: 4 Core RAM: 72GB Disk: 500GB Total	CPU: 6 Core RAM: 96GB Disk: 700GB Total
1000 to 2000 Endpoints	CPU: 12 Core RAM 64GB Disk: 850GB Total, 500GB for Binaries/Logs, 200GB for MariaDB and 150GB for Site Controller	2 x [CPU: 6 Core RAM: 96GB Disk: 700GB Total]	2 x [CPU: 6 Core RAM: 96GB Disk: 700GB Total]



Production Endpoints	Kyndryl Resiliency Orchestration Server (with cohosted Site Controller)	Additional Linux Site Controllers	Windows Site Controllers
2000 to 3000 Endpoints	CPU: 16 Core RAM 96GB Disk: 1TB Total, 650GB for Binaries/Logs, 200GB for MariaDB and 150GB for Site Controller	3 x [CPU: 6 Core RAM: 96GB Disk: 700GB Total]	3 x [CPU: 6 Core RAM: 96GB Disk: 700GB Total]

Software Requirements

You will need the following compatible software to install the Kyndryl Resiliency Orchestration Server.

- Compatible RHEL
- Compatible Java
- Compatible Tomcat
- Compatible MariaDB

Note: For installation and Post-installation steps refer to the Kyndryl RO Installation guide.

Downloading the Kyndryl Resiliency Orchestration Software Package

The Kyndryl Resiliency Orchestration Server package can be downloaded from the Kyndryl Passport Advantage site or Fix Central using the Customer's login credentials.

- **Passport Advantage link:**

<https://www-01.ibm.com/software/passportadvantage/>

The Passport Advantage provides customers with secure access to software downloads for each release.

- **Fix Central link:**

<https://www-945.ibm.com/support/fixcentral/>

Fix Central provides fixes and updates for your licensed software.

In case you are a Kyndryl Employee then download the package from the Kyndryl Internal DSW Downloads site at <https://w3-03.ibm.com/software/xl/download/ticket.wss>



This guide assumes that you will be downloaded from the Kyndryl Internal DSW Downloads site from your Kyndryl Laptop connected to W3.

1. Open the <https://w3-03.ibm.com/software/xl/download/ticket.wss> in your Kyndryl Laptop browser.
2. Accept the Agreement.
3. In the Search box type “Kyndryl Resiliency Orchestration” and click the search link.
4. In the list of results, click Kyndryl Resiliency Orchestration Electronic V Multiplatform English assembly.
5. Select Kyndryl Resiliency Orchestration Server V for RHEL English.
6. Scroll down and then click the **Download now** button.

Note: Once the download completes, you will have the package with the filename `Kyndryl_Resiliency_Orchestration_Srvr.tar.gz` in your Download folder.

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 files and property files are available in `/opt/Server` and that the logged-in user has sudo permissions equivalent to root.

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

```
cd /opt/Server
sudo vi PanacesServerInstaller.properties
```

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

PanacesServerInstaller.properties file

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

1. There are 2 additional properties added for Fully Qualified Domain Name (FQDN) selection – `FQDN_SELECTION` and `LOCAL_HOST_SERVER`.
2. `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, or else the installation will fail.



Table 1: Keywords in the PanacesServerInstaller.properties file

Keyword	Description
INSTALLER_UI	<p>Set to "silent" to install without any user interaction.</p> <p>Set to "console" to install with password on demand.</p> <p>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 the Post installation steps.</p>
MODIFY_SYSTEM_FILES=1	<p>It modifies system files, i.e. /etc/hosts, /etc/sysconfig/selinux, /etc/sysctl.conf</p> <p>The below-listed changes will be done</p> <p>"IP/Hostname localhost Hostname" in /etc/hosts file</p> <p>"net.ipv4.tcp_retries2 = 4" in /etc/sysctl.conf file</p> <p>"SELINUX=permissive" in /etc/sysconfig/selinux file</p>
USER_INSTALL_DIR	<p>Enter the path for the directory to install the Kyndryl Resiliency Orchestration Server software. (default path is /opt/panaces/)</p>
ON_DEMAND_PASSWORD	<p>Set to "Yes" if INSTALLER_UI is set to "console."</p> <p>Set to "No" if INSTALLER_UI is set to "silent."</p> <p>Note:</p> <ul style="list-style-type: none"> • 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 SANОВI_USER_PASSWORD in the property file. • In case this Keyword is set to "Yes," <ul style="list-style-type: none"> • Passwords for DATABASE_PASSWORD, SUPPORT_USER_PASSWORD, and SANОВI_USER_PASSWORD will be



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



Keyword	Description
	used, such as in Cyber Recovery using the AWS Vault solution.
DATABASE_TYPE=MARIADB	Database type values are MARIADB or AWS_RDS_MARIADB 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 the AWS RDS MariaDB instance will be used, such as in Cyber Recovery using the AWS Vault solution
Next 3 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.



Keyword	Description	
	For example: /opt/panaces/installconfig/keystore/sanovi.key store	
REFRESH_EXISTING_SCHEMA	<p>When the Schema Refresh option is chosen, the old schema which is already available in the system will be refreshed.</p> <p>Set the option to 0: If the option is set to 0 the schema will not be refreshed.</p> <p>Set the option to 1: if the option is set to 1, schema will be refreshed/reset.</p> <p>Note: Option 0 is set by default and is the only option for upgrades.</p>	
STOP_IBM_RESILIENCY_ORCHESTRATION_AND_UNINSTALL	<p>Set the option to 1: If the option is set to 1, the installer will stop the running services and uninstall.</p> <p>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.</p>	
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 AD/ LDAP Server Note: Please provide the root domain instead of Ad server IP.
THIRD_PARTY_SERVER_DOMAIN	NA	The Server Domain is applicable only to AD. Note: we should not enter the domain for LDAP
DIRECTORY_USERNAME	NA	Enter the Username for reading the external system for AD/LDAP server.
DIRECTORY_PASSWORD	NA	Enter the Password for reading the external system for AD/ LDAP server.



Keyword	Description	
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.
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.	
panaces.acp.server.concurrentRequestProcessCount	This concurrentRequestProcessCountMax property should be equal to or greater than concurrentRequestProcessCount	
panaces.acp.server.concurrentRequestProcessCountMax		



Post-install steps for Red Hat Enterprise Linux

After you have installed RHEL OS, you will need to perform the following.

- [Verify network connectivity.](#)
- [Subscribe to Red Hat Subscription.](#)
- [Installing essential administrative utility packages](#)

Subscribe System to Red Hat Subscription

To subscribe the system to the Red Hat subscription, refer to the following links:

- Online registration: <https://access.redhat.com/solutions/253273>
- Offline registration: <https://access.redhat.com/solutions/3121571>

Installing Essential Administration Utility Packages

Install the following packages from the default Red Hat Repository.

1. # yum install -y net-tools.

```

root@osever:
[root@osever ~]# yum install -y net-tools
Updating Subscription Management repositories.
Red Hat Enterprise Linux 8 for x86_64 - AppStream (RPMs)                6.8 MB/s | 19 MB   00:02
Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)                5.7 MB/s | 20 MB   00:03
Last metadata expiration check: 0:00:06 ago on Tue 25 Aug 2020 02:22:25 PM IST.
Dependencies resolved.
=====
Package              Arch             Version           Repository           Size
-----
Installing:
net-tools            x86_64          2.0-0.51.20160912git.e18  rhel-8-for-x86_64-baseos-rpms 323 k
Transaction Summary
-----
Install 1 Package
Total download size: 323 k
Installed size: 1.0 M
Downloading Packages:
net-tools-2.0-0.51.20160912git.e18.x86_64.rpm                       232 kB/s | 323 kB   00:01
-----
Total                                                                    232 kB/s | 323 kB   00:01
warning: /var/cache/dnf/rhel-8-for-x86_64-baseos-rpms-51b3b76d5696246b/packages/net-tools-2.0-0.51.20160912git.e18.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY
Red Hat Enterprise Linux 8 for x86_64 - BaseOS (RPMs)                603 kB/s | 5.0 kB   00:00
Importing GPG key 0xP431051:
  Userid      : "Red Hat, Inc. (release key 2) <security@redhat.com>"
  Fingerprint: 567E 347A D004 4ADE 55BA 9ASF 199E 2F91 FD43 1D51
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0xD4082792:
  Userid      : "Red Hat, Inc. (auxiliary key) <security@redhat.com>"
  Fingerprint: 567E 347A D004 4ADE 55BA 9ASF 199E 2F91 FD43 1D51
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction:
Installing : net-tools-2.0-0.51.20160912git.e18.x86_64                1/1
Running scriptlet: net-tools-2.0-0.51.20160912git.e18.x86_64        1/1
Verifying   : net-tools-2.0-0.51.20160912git.e18.x86_64            1/1
Installed products updated.

Installed:
net-tools-2.0-0.51.20160912git.e18.x86_64

Complete!
[root@osever ~]#

```

This step installs commonly used network diagnostic utilities such as ifconfig, netstat, route, and others.

2. # yum install -y bind-utils



```

root@rosever-
[root@rosever ~]# yum install -y bind-utils
Updating Subscription Management repositories.
Last metadata expiration check: 0:11:22 ago on Tue 25 Aug 2020 02:54:02 PM IST.
Dependencies resolved.
-----
Package                Arch          Version           Repository         Size
-----
Installing:
bind-utils              x86_64        32:9.11.13-5.el8_2  rhel-8-for-x86_64-appstream-rpms 443 k
Installing dependencies:
bind-libs-lite          x86_64        32:9.11.13-5.el8_2  rhel-8-for-x86_64-appstream-rpms 1.2 M
bind-license            noarch        32:9.11.13-5.el8_2  rhel-8-for-x86_64-appstream-rpms 100 k
bind-libs               x86_64        32:9.11.13-5.el8_2  rhel-8-for-x86_64-appstream-rpms 171 k
python3-bind           noarch        32:9.11.13-5.el8_2  rhel-8-for-x86_64-appstream-rpms 148 k
-----
Transaction Summary
-----
Install 5 Packages

Total download size: 2.0 M
Installed size: 4.7 M
Downloading Packages:
(1/5): bind-license-32:9.11.13-5.el8_2.noarch.rpm   38 kB/s | 100 kB  00:01
(2/5): bind-utils-32:9.11.13-5.el8_2.x86_64.rpm   225 kB/s | 443 kB  00:01
(3/5): bind-libs-lite-32:9.11.13-5.el8_2.x86_64.rpm 524 kB/s | 1.2 MB  00:02
(4/5): bind-libs-32:9.11.13-5.el8_2.x86_64.rpm    168 kB/s | 171 kB  00:00
(5/5): python3-bind-32:9.11.13-5.el8_2.noarch.rpm  174 kB/s | 148 kB  00:00
-----
Total
-----
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction:
  Preparing                : 1/1
  Installing               : 1/5
  Installing               : 2/5
  Installing               : 3/5
  Installing               : 4/5
  Installing               : 5/5
Running scriptlet: bind-utils-32:9.11.13-5.el8_2.x86_64  1/5
Verifying                 : 1/5
Verifying                 : 2/5
Verifying                 : 3/5
Verifying                 : 4/5
Verifying                 : 5/5
Installed products updated.

Installed:
bind-utils-32:9.11.13-5.el8_2.x86_64      bind-libs-lite-32:9.11.13-5.el8_2.x86_64      bind-license-32:9.11.13-5.el8_2.noarch      bind-libs-32:9.11.13-5.el8_2.x86_64
python3-bind-32:9.11.13-5.el8_2.noarch

Complete!
[root@rosever ~]#

```

The above package provides utilities such as nslookup that are useful to query DNS servers.

3. # yum install -y wget

```

root@rosever-
[root@rosever ~]# yum install -y wget
Updating Subscription Management repositories.
Last metadata expiration check: 2:13:08 ago on Wed 26 Aug 2020 06:08:01 AM IST.
Dependencies resolved.
-----
Package                Arch          Version           Repository         Size
-----
Installing:
wget                   x86_64        1.19.5-8.el8_1.1  rhel-8-for-x86_64-appstream-rpms 735 k
-----
Transaction Summary
-----
Install 1 Package

Total download size: 735 k
Installed size: 2.9 M
Downloading Packages:
wget-1.19.5-8.el8_1.1.x86_64.rpm           524 kB/s | 735 kB  00:01
-----
Total
-----
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction:
  Preparing                : 1/1
  Installing               : 1/1
  Running scriptlet: wget-1.19.5-8.el8_1.1.x86_64  1/1
  Verifying                 : 1/1
Installed products updated.

Installed:
wget-1.19.5-8.el8_1.1.x86_64

Complete!
[root@rosever ~]#

```

The above package is a utility to browse and download files from the Internet using the command line. This will be used later to download the required packages.



4. # yum install -y unzip

```
root@rosever etc# yum install -y unzip
Updating Subscription Management repositories.
Last metadata expiration check: 0:00:43 ago on Wed 26 Aug 2020 08:27:32 PM IST.
Dependencies resolved.
-----
Package Arch Version Repository Size
-----
Installing:
unzip x86_64 6.0-43.el8 rhel-8-for-x86_64-baseos-rpms 195 k
-----
Transaction Summary
-----
Install 1 Package
Total download size: 195 k
Installed size: 414 k
Downloading Packages:
unzip-6.0-43.el8.x86_64.rpm 486 kB/s | 195 kB 00:00
-----
Total 483 kB/s | 195 kB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing :
Installing : unzip-6.0-43.el8.x86_64 1/1
Running scriptlet: unzip-6.0-43.el8.x86_64 1/1
Verifying : unzip-6.0-43.el8.x86_64 1/1
Installed products updated.
Installed:
unzip-6.0-43.el8.x86_64
Complete!
[root@rosever etc]#
```

The above step will install the unzip utility on your server. This is used later in the installation process.

Refer to The install guide for Configuring Firewall.

Installing MariaDB

The Kyndryl Resiliency Orchestration Server requires the installation of MariaDB. This package can be downloaded directly from the MariaDB site.

Example:

For MariaDB 10.5.8, you can navigate to the <https://downloads.mariadb.com/MariaDB/mariadb-10.5.8/yum/rhel8-amd64/rpms/> get the rpm packages required to install this.

Please download the following 3 packages from the above URL.

1. MariaDB-common-10.5.0-1.el8.x86_64.rpm
2. MariaDB-server-10.5.0-1.el8.x86_64.rpm
3. MariaDB-client-10.5.0-1.el8.x86_64.rpm

Downloading required packages

Use the wget utility to easily download these packages directly on the server.

Example:



For MariaDB 10.5, use the following commands:

```
# cd /tmp

# wget https://downloads.mariadb.com/MariaDB/mariadb-10.5.0/yum/rhel8-amd64/rpms/MariaDB-common-10.5.0-1.el8.x86_64.rpm

# wget https://downloads.mariadb.com/MariaDB/mariadb-10.5.0/yum/rhel8-amd64/rpms/MariaDB-server-10.5.0-1.el8.x86_64.rpm

# wget https://downloads.mariadb.com/MariaDB/mariadb-10.5.0/yum/rhel8-amd64/rpms/MariaDB-client-10.5.0-1.el8.x86_64.rpm
```

Installing MariaDB packages

This section covers procedures for installing the three packages downloaded in the previous topic.

Ensure you are in the /tmp directory and then execute the following

```
# yum localinstall MariaDB-*
```

You can now proceed to configure the MariaDB server as required by the Kyndryl Resiliency Orchestration Server covered in the next section.

Configuring MariaDB

You need to enable and start the MariaDB server before you configure it. For this, you will need to give the following commands as root.

1. To enable MariaDB, execute the following command.
systemctl enable mariadb
2. To start MariaDB, execute the following command.
systemctl start mariadb
3. To find the status of MariaDB, execute the following command.
systemctl status mariadb

Note: You should see the status as active (running).

Setting Up MariaDB Root Password



Once MariaDB is successfully started and running you can proceed with setting up the root password for MariaDB as needed. Execute the following commands in sequence.

```
1. # systemctl stop mariadb
2. # mysqld_safe --skip-grant-tables &
3. # mysql -u root
4. mysql> FLUSH PRIVILEGES;
5. mysql> exit
6. # mysql -u root
7. mysql>          SET          PASSWORD          FOR
   root@'localhost'=PASSWORD('password');
```

Note:

- Replace the 'password' with the actual password you would like to keep for the MariaDB root user.
- Now you will need to stop and restart the MariaDB server for the changes to get activated.

```
8. mysql> exit
9. # mysqladmin -u root -p shutdown
```

Note: You will now be prompted to enter the newly set root password. Please enter the password and hit enter.

10. Restart MariaDB using the standard systemctl command.
systemctl start mariadb
11. Login to the MariaDB server using the new password you just set.
mysql -u root -p
12. Enter the new password you set in Step 7 above.

Installing Apache Tomcat Server

The Kyndryl Resiliency Orchestration Server requires the installation of a compatible version of the Apache Tomcat Server. Follow the steps below to download and install the Tomcat server.

1. Change to /tmp directory.
2. Download the tomcat server .tar.gz file using wget command as below:

Example:

```
# wget https://archive.apache.org/dist/tomcat/tomcat-9/v9.0.48/bin/apache-tomcat-9.0.48.tar.gz.
```

3. Untar the archive into its directory under /opt/
tar -zxpvf apache-tomcat-<version>.tar.gz -C /opt/



Note: The above command will untar the package under /opt/apache-tomcat-<version>.

4. Edit the /etc/profile file as root and set the following variables, CATALINA_BASE and CATALINA_HOME as follows.

```
$CATALINA_HOME = /opt/apache-tomcat-<version>  
$CATALINA_BASE = /opt/apache-tomcat-<version>
```

5. Save and exit the file.
6. Logout and Login to the system again for the changes that have taken effect.
7. Confirm the changes by executing the following eco commands:

```
# echo $CATALINA_HOME  
# echo $CATALINA_BASE
```

Note: Do not try to start the Tomcat server at this time. There are some additional steps to successfully start the Tomcat Server which will be introduced in a later section of this manual. Please proceed to the next section.

Post Install Configuration

Several final steps need to be completed after the Kyndryl Resiliency Orchestration Server has been installed. These are primarily to complete the configuration of the Tomcat server that was installed earlier. These steps are below.

Setting up Tomcat Environment – setenv.sh

The Red Hat gets installed using a dual-stack TCP implementation. It has both TCP/IP v4 and TCP/IP v6 installed. When JDK is installed on such a system any process spawned by the JRE gets bound to the TCP/IP v6 address by default.

We will need to change this behavior to make Java bind to the TCP/IP v4 address.

To do this, edit the /opt/apache-tomcat-<version>/bin/setenv.sh and add the following line just after the export JAVA_HOME line.

```
JAVA_OPTS="$JAVA_OPTS -Djava.net.preferIPv4Stack=true -  
Djava.net.preferIPv4Addresses=true "
```



Note: If `apache-tomcat-<version>/bin/setenv.sh` is not available in the package, then create a new blank `.sh` file in `apache-tomcat-<version>/bin/` with the file name `setenv.sh` and add the command text as per the following example.

Example:

```
# environment setting file for tomcat

export JAVA_HOME=/opt/panaces/jdk1.8.0_372

JAVA_OPTS="$JAVA_OPTS -Djava.net.preferIPv4Stack=true -
Djava.net.preferIPv4Addresses=true "

export CATALINA_OPTS="-Djava.awt.headless=true -XX:+CMSClassUnloadingEnabled -
Xms2048m -Xmx2048m -XX:MetaspaceSize=256m -XX:MaxMetaspaceSize=256m -
XX:MinHeapFreeRatio=40 -XX:MaxHeapFreeRatio=70 -XX:NewRatio=8 -
XX:SurvivorRatio=32 -XX:+UseG1GC"
```

Note: Compatible JDK version is displayed.

Setting up Java Home and JRE Home variables

This section details the `/etc/profile` file update to set up the `JAVA_HOME` and `JRE_HOME` variables. This is an optional step as these are set up by the Kyndryl Resiliency Orchestration Server startup scripts automatically. However just to be sure and to make Java runtime available systemwide, it is recommended that you make the following change.

1. `# vi /etc/profile`
 2. Add two lines just above the `$CATALINA_HOME` line that we added earlier
- Example:**
- ```
JAVA_HOME=/opt/panaces/jdk1.8.0_372
JRE_HOME=/opt/panaces/jdk1.8.0_372
```
3. Now export these two variables as well by appending the two variables to the export line as follows.
  4. `export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL CATALINA_HOME CATALINA_BASE JAVA_HOME JRE_HOME`

Your final file with the relevant lines added should look like the example figure below.

```
JAVA_HOME=/opt/panaces/jdk1.8.0_251
JRE_HOME=/opt/panaces/jdk1.8.0_251
CATALINA_HOME=/opt/apache-tomcat-9.0.27
CATALINA_BASE=/opt/apache-tomcat-9.0.27

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL CATALINA HOME CATALINA BASE JAVA HOME JRE HOME
```

**Important!**

Do not change anything else in the profile file. Just make the changes highlighted in the screenshot above. For your quick reference, the lines are pasted in the below table as well.


Please use a compatible version of JDK. For a compatible version of JDK, please refer to the Kyndryl Resiliency Orchestration Installation document.

```
JAVA_HOME=/opt/panaces/jdk<version>
JRE_HOME=/opt/panaces/jdk<version>
CATALINA_HOME=/opt/apache-tomcat-<version>
CATALINA_BASE=/opt/apache-tomcat-<version>
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL
CATALINA_HOME CATALINA_BASE JAVA_HOME JRE_HOME
```

5. Save and exit this file.
6. Log out and log in to the server for the profile settings to become effective.
7. Check if you have the four variables available in the shell by executing the following command:

```
echo $JAVA_HOME
echo $JRE_HOME
echo $CATALINA_HOME
echo $CATALINA_BASE
```

You should see the following output on the screen

 root@roserver:/etc

```
[root@roserver etc]# echo $JAVA_HOME
/opt/panaces/jdk1.8.0_251
[root@roserver etc]# echo $JRE_HOME
/opt/panaces/jdk1.8.0_251
[root@roserver etc]# echo $CATALINA_HOME
/opt/apache-tomcat-9.0.27
[root@roserver etc]# echo $CATALINA_BASE
/opt/apache-tomcat-9.0.27
[root@roserver etc]# █
```



## Installing Third-Party Dependencies

The Kyndryl Resiliency Orchestration Server has some third-party dependencies. These need to be downloaded and installed before we start the server. These can be downloaded from the following URL: <https://sourceforge.net/projects/gnu-utils/files/binaries/>

You will need to download ThirdPartyJSLib.zip from the above location.

Once downloaded transfer both files to the /tmp directory on the server and unzip them. You can give the following command to unzip both files.

```
unzip ThirdPartyJSLib
```

After unzipping the files, we need to copy the unzipped files to specific locations. You can use the following commands to complete this.

```
cp -r /tmp/ThirdPartyJSLib/*.* /opt/apache-tomcat-
<version>/webapps/PanacesGUI/scripts/
```

```
cp -r /tmp/json-20180813.jar /opt/apache-tomcat-
<version>/webapps/PanacesGUI/WEB-INF/lib/
```

```
cp -r /tmp/json-20180813.jar /opt/panaces/lib/
```

```
cd /opt/apache-tomcat-<Version>/webapps/PanacesGUI/scripts/
```

```
chown tomcatuser.tomcatusergroup calendar_en.js calendar_ja.js calendar.js
calendar-setup.js dhtmlgoodies_calendar.js dhtmlgoodies_slider.js
dhtmlgoodies_tooltip_helper.js JsSimpleDateFormat.js wz_tooltip_ja.js
wz_tooltip.js wz_tooltip_new_ja.js wz_tooltip_new.js
```

```
chmod 770 calendar_en.js calendar_ja.js calendar.js calendar-setup.js
dhtmlgoodies_calendar.js dhtmlgoodies_slider.js
dhtmlgoodies_tooltip_helper.js JsSimpleDateFormat.js wz_tooltip_ja.js
wz_tooltip.js wz_tooltip_new_ja.js wz_tooltip_new.js
```

## Running the SecurityUserInjection.sh script

1. Execute the cat panaces\_env in the bin folder of panaces and check the Tomcat java path.
2. Open **SecurityUserInjection** script and modify the Tomcat and jdk path.
3. Run the following command to execute the *SecurityUserInjection.sh*:

```
/opt/panaces/bin/SecurityUserInjection.sh
```



This script sets up all necessary users, groups, and permissions needed to start the Kyndryl Resiliency Orchestration Server.

### Configuring the Tomcat server.xml file

There are a few changes that need to be done to the Tomcat server.xml file to publish the Panaces Application. These changes are listed below.

1. Navigate to the /opt/apache-tomcat-<version>/conf directory
2. Edit the server.xml file using your favorite editor
3. Find the following section in the file and comment on it

Change the following section from:

```
<Connector
port="8080"
protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" />
```

To:

```
<!--

 <Connector
port="8080"
protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" />

-->
```

The above .xml file stops the Tomcat server from working on the insecure HTTP protocol using Port 8080.





4. Add a new Connection executor section as follows

```
<Connector executor="tomcatThreadPool"
 port="8080" protocol="HTTP/1.1"
 connectionTimeout="20000"
 redirectPort="8443"
 compression="on"
 compressionMinSize="2048"
 nocompressionUserAgents="gozilla, traviata"
 compressableMimeType="text/html,text/xml,text/plain,te
xt/css,text/javascript,text/json,application/x-
javascript,application/javascript,application/json"
/>
```

The above change will enable the redirection of port 8080 to port 8443.

**Note:** Conditions for which this redirection works must be defined. These conditions are specified in the Applications web.xml file. The subsequent sections cover these conditions.

5. Add a new Connector port section as follows for secure access (HTTPS)

```
<Connector port="8443"

 protocol="org.apache.coyote.http11.Http11NioProtocol"
 maxThreads="150"
 SSLEnabled="true"
 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/css,text
/javascript
, text/json,application/x-
javascript,application/javascript,application/json"
 URIEncoding="UTF8"
```



```
xpoweredby="false"
ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA"
server="Web"/>
```

The above changes will publish the Panaces App and make it available on port 8443. Features like compression, UTF8, and security ciphers, etc are all defined here.

6. Save and exit the file.

## Configuring the Catalina.sh file

1. Navigate to the TOMCAT\_HOME/bin/catalina.sh file from the following directory path:

```
/opt/apache-tomcat-9.0.68/bin/catalina.sh
```

2. Locate the following line in the Catalina.sh file:

```
JAVA_OPTS="$JAVA_OPTS" -
Dorg.apache.catalina.security.SecurityListener.UMASK=`umask`"
```

3. Add the following property in the catalina.sh file after the above line:

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

**Note:** If this property is not added, then the following exception appears while loading to RO.

```
java.lang.NoClassDefFoundError: Could not initialize class
org.apache.taglibs.standard.util.XmlUtil.
```

4. Save and exit the file.



## Configuring the PanacesGUI web.xml file

1. Navigate to the `/opt/apache-tomcat-<version>/webapps/PanacesGUI/WEB-INF/` directory
2. Edit the `web.xml` file using your favorite editor
3. Find the following section in the file

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

4. Add the following lines after the lines in the above step.

```
<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>
```

These changes enable the rules for the automatic redirection from port 8080 (HTTP) to port 8443 (HTTPS). In effect, even if someone was able to type in the Panaces Server URL without specifying HTTPS, the Tomcat server would automatically redirect the request to the secure HTTPS port 8443.

5. Save and exit the file.

## Starting the Kyndryl Resiliency Orchestration Server

We are now at the last stage where the Kyndryl Resiliency Orchestration Server is ready to be started. Complete the following steps to start the server.

1. Reboot the server
2. After reboot, check if the MariaDB server is running. You can use the `systemctl status MariaDB` command to check the status.
3. Execute the following command:

```
/opt/panaces/bin/panaces start
```

You should see a similar output on the screen as shown below.



```
root@roserver:~
[root@roserver ~]# /opt/panaces/bin/panaces start
Starting Active MQ server...
Successfully Started Active MQ.
Starting Panaces server...
Successfully started.
Starting Tomcat server...
Successfully started.
Starting JackRabbit repository service...
Successfully started.
Starting Agent Node...
Agent type is local
Thu Aug 27 12:36:20 IST 2020 LinuxOSAgent started[].
[root@roserver ~]# █
```

## Logging into the Kyndryl Resiliency Orchestration Server

As a final step, try logging into the Kyndryl Resiliency Orchestration Server console. For this perform the following steps.

1. Start your Internet Browser.
2. Type the URL of the Kyndryl Resiliency Orchestration Server in the address bar.

**Example:** <https://192.168.15.30:8080/PanacesGUI/pages/Login>. You should automatically get redirected to the secure port 8443 and the URL should change to <https://192.168.15.30:8443/PanacesGUI/pages/Login>

For the first time when you open this site, you will also get a certificate warning, please accept the warning and proceed. This warning is because the installation uses a self-signed SSL certificate which flags this warning.

3. On the login page, log in using the default username and password as below.

Username: drmadmin

Password: <Password<sup>1</sup>>

<sup>1</sup>Connect with the Support/Delivery team to get the default passwords.

4. After logging in you should see the following screen.



If you can log in successfully then your installation is complete.

### Allow-listing Commands or Kyndryl Resiliency Orchestration Server

After the Kyndryl Resiliency Orchestration Server has been installed you should perform the following tasks to increase the security of the server.

1. Update the `/etc/sudoers` file with the below content

**Note:** Ensure to replace `/opt/panaces` with the absolute path of `$EAMSROOT`

```
User_Alias USERS = sanovi
```

```
Cmdnd_Alias NCMDs
```

```
=/usr/bin/ls,/usr/bin/cd,/opt/panaces/bin/AIXOSAgent.sh,/opt/panaces/bin/AS400Agent.sh,/opt/panaces/bin/AS400SAgentGeneric.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/IBMCSMPProtectionBulkUploadCLI.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/UniAgentCompo
```



```
nentInfo.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/drmtypes.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/initializeJackRabbitRepository.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
```

2. Change the directory by entering the following command:  
cd \$EAMSROOT
3. 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
```



In the next section, we will learn how to install the Kyndryl Resiliency Orchestration – Site Controller. Please follow the below steps to install the Site Controller.

## Kyndryl Resiliency Site Controller Installation

### Installing Red Hat Linux for Site Controller

For compatible versions of RHEL to that of the Site Controller, please refer to [Kyndryl Resiliency Site Controller \(Co-Hosted\)](#).

1. Install the Red Hat Server as per instructions given in the section [Installing Red Hat Enterprise Linux](#) in this document.
2. On the Software Selection Screen, select the “Server with GUI” option.
3. Complete the rest of the installation as mentioned in the section [Installing Red Hat Enterprise Linux](#) in this document.

### Pre-requisites for Installing the Site Controller

1. Ports are required to be open between the Site Controller and Kyndryl Resiliency Orchestration Server and Agents.

Port Number(s)	Description
42443 and 45443	<ul style="list-style-type: none"><li>• Kyndryl Resiliency Orchestration Server to Site Controller, open 45443 bi-directional and open and 42443 as uni-directional.</li><li>• Kyndryl Resiliency Orchestration Agents to Site Controller open ports as uni-directional.</li></ul>

### Installing Third-Party Dependencies for Site Controller

The Kyndryl Resiliency Site Controller has some third-party dependencies. These need to be downloaded and installed before we start the Site Controller. These can be downloaded from the following URL: <https://sourceforge.net/projects/gnu-utils/files/binaries/>

You will need to download the following two zip files from the above location.





- ThirdPartyJSLib.zip
- gnulib.zip

**Note:** Implementing steps mentioned in the above paragraph are not required from Kyndryl RO 8.2.6.

Once downloaded transfer both files to the /tmp directory on the server and unzip them. You can give the following command to unzip both files.

- # unzip ThirdPartyJSLib
- # unzip gnulib.zip

**Note:** You will need to copy the unzipped files to the specific locations in the Site Controller after the installation has been completed. This procedure will be covered in the later section.

### Installing Site Controller on Red Hat Linux in Silent Mode

The Site Controller installation can also be done in a Silent console-based manner. This is particularly useful when the installation must be done on headless servers or servers where the GUI is not available. You can also perform this type of installation remotely using just an SSH connection to the server.

To install the Site Controller in the Silent Console-based manner follow the steps outlined below.

1. Execute the earlier downloaded SiteController.bin with the following command:

```
./SiteController.bin -f PanacesAgentNodeInstaller.properties
```

2. The -f parameter above specifies the Parameter file that has the answers for the SiteController Installer. The Parameter file is explained below.

The Parameter file called PanacesAgentNodeInstaller.properties is a simple text file that has the information necessary to install the SiteController silently. The file is self-explanatory and has the following parameters.

Keyword	Description
INSTALLER_UI	Displays the mode of installation as “silent”.
MODIFY_SYSTEM_FILES=1	It modifies the following system files:



	/etc/hosts,/etc/sysconfig/selinux, /etc/sysctl.conf
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.

The actual Properties file used for this installation is reproduced below for your quick reference.

INSTALLER\_UI=silent

MODIFY\_SYSTEM\_FILES=1

USER\_INSTALL\_DIR=/opt/panaces/

USER\_INPUT\_RESULT\_PRIMARY\_PANACES\_SERVER=192.168.15.30

USER\_INPUT\_RESULT\_SECONDARY\_PANACES\_SERVER=192.168.15.30

PANACES\_AGENT\_NODE\_ADDRESS=192.168.15.133

AGENTNODE\_START\_YES=0

**NOTE: You will have to mention IP Address for both the following parameters**

**1. USER\_INPUT\_RESULT\_PRIMARY\_PANACES\_SERVER**

**2. USER\_INPUT\_RESULT\_SECONDARY\_PANACES\_SERVER**



**Note:** You can enter the two IP addresses for these servers. If you have only one RO Server then enter the same IP in both the parameters as shown above.

The installation should proceed as shown in the screenshots below.

1. Executing the SiteController.bin with the -f parameter to start the installation.

```
root@sitecontroller:~
[root@sitecontroller ~]# ./SiteController.bin -f PanacesAgentNodeInstaller.properties
```

2. The screenshot below shows the Silent Install proceeding with an Installation Complete message at the end.

```
root@sitecontroller:~
[root@sitecontroller ~]# ./SiteController.bin -f PanacesAgentNodeInstaller.properties
Preparing to install
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

Jar Path : /tmp/install.dir.1233/InstallerData/installer.zip
Jar Path : /tmp/install.dir.1233/InstallerData/installer.zip
DumpDebugInfo /opt/panaces/SanoviInstaller_debug.txt
EVAL BEGINNING
XMLScriptWriter: No Installation Objects were skipped
Retrying Installables deferred in pass 0
Deferral retries done because:
There were no deferrals in the last pass.

Installation Completed

(X) storing replay variable manager
8. final log file name=/opt/panaces/IBM_Resiliency_Orchestration_SiteController_Install_02_09_2021_11_19_09.log
[root@sitecontroller ~]#
```

## Post Install Configuration

1. Based on your site requirements you may wish to adjust the following 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.

2. Refer to the section [Installing Third-Party Dependencies for Site Controller](#) earlier and copy the libraries as per the following command.

```
cp -r /tmp/ThirdPartyJSLib/*.* /opt/panaces/lib
Change ownership of the libraries as follows.
chown panacesuser.panacesusergroup /opt/panaces/lib/json-20180813.jar
```



```
cd /opt/panaces/lib/
```

```
cd /opt/panaces/lib/
```

## Verify Site Controller Status

1. Execute the following command to check if the Site Controller is running successfully.

```
/opt/panaces/bin/SiteController.sh status
```

You should see the following output.

```
[root@sitecontroller ~]# /opt/panaces/bin/SiteController.sh status
Active MQ Is Running
Site Controller Is Running
[root@sitecontroller ~]#
```

If you see the above message, then you have successfully installed the Kyndryl Resiliency Site Controller.

You can explore the product and move on to more advanced topics and customizations as needed. Please refer to the various guides for the product available on the Kyndryl Passport Advantage site or contact your Kyndryl Resiliency Support / Sales representative for more details.

## Installing Site Controller Server or Site Controller in MS Windows

### Installation and Services

Perform installations and services in the following order:

4. Install the Kyndryl Resiliency Orchestration
5. Installation of Site Controller by using either the GUI mode or Silent mode
6. Configuring Agents to use PowerShell framework
7. Start Site Controller
8. Start Agent Node on Site Controller

### Pre-requisites for Installing the windows Site Controller

- Based on the features, download the GPL dependent binaries from this link [GPL dependent binaries](#) before the Site Controller installation



- The following ports are used in the communication protocol.

Port	Description
5985	For HTTP communication between the Agents and Windows-based Site Controller
5986	For HTTPS (secure) communication between the Agents and Windows-based Site Controller
42443/45443	For communication between the Windows-based Site Controller and the Kyndryl Resiliency Orchestration Server

### Installing Site Controller in Windows in Silent Mode

When installing the 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 Agents installation after which, you can run the installation program in silent mode.

Perform the following steps to edit the properties files.

- Edit the parameter and run the following command

```
Install.exe -f PanacesAgentNodeInstaller.properties -silent
```

- Modify the respective properties file for the keywords shown in the following tables, to reflect your configuration.

PanacesAgentNodeInstaller.properties file:

Keyword	Description
INSTALLER_UI	Displays the mode of installation as “silent”.



Keyword	Description
MODIFY_SYSTEM_FILES=1	Setting this property to 1 modifies the system files under the following system folder: C:\windows\system32\drivers\etc
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. Set this property to manual as there are some post-installation steps.

- Proceed to the Post-installation procedure. For instructions, see [Post Installation Steps after you install the Site Controller in Windows](#).

### Post Installation Steps after you install the Site Controller in Windows

- In the Site Controller installation folder, perform the following steps:
  - Go to the location: `$EAMSROOT/installconfig/` where `$EAMSROOT` is the location where the Site Controller is installed.
  - 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.

2. 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

3. Enter the path of the truststore in the same SiteController.cfg file.

For Example: panaces.acp.truststore=

**Notes:**

- This value of the ACP truststore will be the path where 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.

4. Post-installation, the site controller should start automatically.

In case it does not start, perform the following steps.

- 4.1. Check for special characters similar to "~ //RS" under the service property "**Path to executable.**"
- 4.2. Delete the first character and update it to "//RS" in the registry by following the steps below.
  - 4.2.1. Open registry editor.
  - 4.2.2. Edit --> find --> "ROActiveMQ" and "ROWindowsOSAgent\_"
  - 4.2.3. Find imagepath subkey and click on modify.
  - 4.2.4. Update the special character to "//RS" in the data value.
- 4.3. Enable the IBMROSiteController service, by following the steps below.
  - 4.3.1. Goto <install location>sitecontroller/bin.



- 4.3.2. Run SiteController.bat start on the command prompt.
- 4.3.3. Open registry editor.
- 4.3.4. Edit --> find --> "IBMROSiteController"
- 4.3.5. Find imagepath subkey and click on modify.
- 4.3.6. Update the special character to "//RS" in the data value.
- 4.3.7. Post update of imagepath data value, start the IBMROSiteController service by right-clicking and selecting the **Start** menu item.
- 4.4. Start IBMROWindowsOSAagent services by right-clicking and selecting the Start menu item.
5. 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>.
6. When the Site Controller has a NAT IP, and post-installation the Site Controller is in 'Unknown' state, follow the below steps –
  - 6.1.1. Stop the Site Controller services and the Agents running on the Site Controller.
  - 6.1.2. 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
```

- 6.1.3. 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>
```

Start the Site Controller services and Agents running on Site.





### **Recommended Security Steps**

To further enhance security and to change default passwords etc. for both the Kyndryl Resiliency Orchestration Server and the Site Controller installations, we recommend that you perform some additional steps. These steps are detailed in the Official Install Guide for Kyndryl Resiliency Orchestration Server, please refer to Section Configuring Resiliency Orchestration for Security.