Kyndryl Resiliency Orchestration

Admin 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

TRADEMARK INFORMATION

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

kyndryl™

Revision History

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

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
8.1	June 2020	Handling Agent Plugins	70	8.1.x
		Configuring AD for AD Authenticate and Basic RO Authorize	89	
		Cancelling an Action in a running workflow	284	
		Agent Upgrade	354	
		Discovering MySQL Dataset	378	
8.1.1	Sep 2020	Mysqldump statement syntax	514	8.1.x
		Changing the Authentication/Authorization mode	19	
		Getting Started	21	
		FQDN Support	22	
		About Resiliency Orchestration	25	
		Importing CA Certificate	18	
		Configuring LDAP – Pre-packaged and custom roles	85, 86	
		Configuring AD for AD Authenticate and Authorize	88, 89	
		Configuring AD Groups	90 - 93	

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Event Duration	226	
		Event Search	235	
		Agent upgrade	355	
		Discovering components	359	
		Discovering datasets	365	
		Discovering protection schemes	371	
		Site Controller Mapping	419	
		vCenter Management Service	433	
		Resiliency Orchestration Server Fallback	509	
8.1.2	Dec 2020	FQDN support	22	8.1.x
		Special Characters in Passwords	22	
		Ansible Integration	43	
		Handling agent plugins	78	
		Organization Configuration	81	
		Enabling/disabling Users	92	
		Multiple User Credentials	364	
		Audit Logging	353	
		Modifying Component	383	
8.1.3	Mar 2021	Site Listing	359	8.1.3
		Site Controller Listing	441	
		Notifications	121	
		Special characters in Usernames	22	

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Start and Stop (Local and Remote) agent from Command line	440	
		Manage section Threadcount Property setting instruction	212	
		Monitor section Threadcount Property setting instruction	235	
8.2.0	Jun 2021	Support of Special characters in passwords used for Linux and Windows Operating Systems	20	8.2.x
		Special Characters in Usernames	21	
		Special Characters in Passwords	22	
		Remote Agent Migration tool	75	
		Registering Plugin for Optional Type Attribute	82	
		Role-Based Access Control	116	
		Creating a Custom Role when using RO for Authorization	116	
		Create/ Save as a Draft/Publish	161	
8.2.6		customize reports: CSV reports	344	
		Updated Agent Configuration > Agentless> Enabling PowerShell on Windows subsystem	65	8.2.x
		Removed the following command from the section- 'Enabling PowerShell on Windows subsystem', New-PSSession -ComputerName <ip> -Credential $C	66	8.2.x

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
8.2.6	Dec 2021	Discovering EMC SRDF Protection Scheme	428	8.2.x
		Agentless added Note nologin	65	
		IBM Resiliency Orchestration Server Recovery > Resiliency Orchestration Server Failover and IBM Resiliency Orchestration Server Fallback	541-542	
8.2.7	Jan 2022	Bullet point added under Note in section User Authentication and Authorization > Adding or Modifying User for Active Directory Authentication	18	8.2.x
		Notification: Email template Added “tls1.2”	132	
8.2.8		Note: updated Windows requires a Windows SC	449	
	Feb2022	Sub Section “RPO Calculation” created under the section “Compute current RTO and display the desired RTO and estimated RTO values”	50	8.2.x
8.2.9	March 2022	Updated section with a bullet to describe the character limitation in Wworkflow name: Workflow Configuration Limitations	165	8.2.x
		Added section Troubleshooting information for reports> Generating report after changing panaces/MariaDB password	359	
		Added a new section “Converting OpenSSH Private key to RSA	67	

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Private key” under Configuration> Agent Configuration> Agentless > Prerequisites.		
		Subsection “Multitenancy Integrated with AD” created under section “Multiple Organization Configuration”	85-86	
		Subsection “Manage Organizations” moved under “Multitenancy Integrated with AD”	87-91	
		Subsection “Manage Users” moved under “Multitenancy Integrated with AD”	91	
		Subsection “Multitenancy Integrated with RO/Basic Authentication Mode (Non-AD)” created under section “Multiple Organization Configuration”	92	
		Subsection “Configuring Basic Authentication Mode for Service Provider and Organizations” created under section “Multitenancy Integrated with RO/Basic Authentication Mode (Non-AD)”	93	
		Subsection “Manage Organizations” created under “Multitenancy Integrated with RO/Basic Authentication Mode (Non-AD)”	94-96	
		Subsection “Manage Users” created under “Multitenancy	97	

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Integrated with RO/Basic Authentication Mode (Non-AD)”		
		Configuration > Agent Configuration > Site Controller Deleted the following Sub-sections: Adding Site Controller to IBM Resiliency Orchestration Server Deleting Site Controller from IBM Resiliency Orchestration Server Reference JIRA: RO-39786		
8.2.9.1	April 2022	Replaced “Resiliency Orchestrationlogs.sh” with “drmlogs.sh” in the section “Fetching Log files using CLI tools”. Reference JIRA: RO-40691		8.2.9.x
		FQDN Support: added VM Protection with IBM Resiliency Block Replicator	27	
		Added section **Successful and failed events** under Validation> View Rules (Jira: RO-19619)	326	8.2.x
8.2.9.1	April 2022	Updated the section “Approving/Rejecting a workflow before execution”. Reference JIRA: RO-40881	363	8.2.x
8.2.9.1	April 2022	Updated the section “Creating a Custom Role when using RO for Authorization”	139	8.2.9.x

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Reference JIRA: RO-40750 and RO-40847		
8.2.9.2	May 2022	Updated the section “Server Memory Management” for default value and more than 100 groups. Reference JIRA: RO-42063	640	8.2.9.2
		Validation Manager	371	
8.2.9.2	May 2022	Added a note under the section ‘Generating report after changing panaces/MariaDB password’ Reference JIRA: RO-42117	417	8.2.x
8.2.9.2	May 2022	Added a Note in the section “Adding or Modifying User for Active Directory Authentication”. Reference JIRA: RO-35630	23	8.2.x
8.3.0	June 2022	Modified the note under the section ‘Generating report after changing panaces/MariaDB password’ Reference JIRA: RO-42117	417	8.3.x
		Updated Validation Manager section with • Creating Categories Listing Validation Rules	331	
		• Updated Configuration section with Multi-Node Solution supported configuration	62	
		Remote Agent Migration Tool	87	

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Created section Troubleshooting Agents	647	
		Section: Adding Site Controller, Added note to address RO-44338.	532	
8.3.1	July 2022	Added a new section “Deleting AD Users”. Reference JIRA: RO-43491	119	8.3.x
		Added a new Note on “Refresh Details” option for both Non-AD and AD roles. Reference JIRA: RO-41218	Page 100 and Page 109	8.3.x
		Added a new section on “Panaces DB Optimization Procedure”. Reference JIRA: RO-45373	Page 670	8.3.x
		Updated Remote Agent Migration Section	Page 87	8.3.x
8.3.2	August 2022	Added “Limitations” in section Manage > Continuity Workflows”	Page 267	8.3.x
8.3.2	August 2022	Updated “Validation Manager Added “Limitations” in section Manage > Continuity Workflows”” Section with the following section: Auto Import Validation Rules	Page 338	8.3.x
8.3.3	September	Steps updated under section “Resiliency Orchestration Server Failover” and created Sub section “Troubleshooting the Access Error”	Page 629	8.3.x
8.3.5	November 2022	Updated section by adding a note - “Discovering EMC SRDF Protection Scheme” under	Page 504	8.3.x

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		"Discovering Protection Scheme" RO-48715		
		Added a new section "Metadata Replication using Automated Script". Reference JIRA: RO-50767	Page 638	8.3.x
8.3.6	December 2022	Port 46443 details added in section Configuration > Agent Configuration > Agentless > Prerequisites > Additional Settings on PFR Subsystem	Page 87	8.3.x
8.3.7	January 2023	Added "High availability Switchover/Switchback/Failover Using automated Scripts" under the section "High Availability of Kyndryl Resiliency Orchestration Server -> Resiliency Orchestration Server Fallback -> Metadata replication Using Automated script"	Page 641	8.3.x
		Updated Discovering MSSQL Dataset section	Page 473	8.3.x
		Added section 'Offline Purge Utility for Workflow Executions' under 'Kyndryl Resiliency Orchestration Logs > Operational History'	Page 600	8.3.x
		Jackrabbit related information (**Agent upgrade in non-secure mode(http)** and **Agent upgrade in secure mode(https)** sections in the Discovery section.		
8.3.7	February 2023	Updated Agent Configuration section with Known Limitations	Page 86	8.3.x

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
8.3.10	April 2023	Updated Agent Configuration with Troubleshooting section	81	8.3.x
8.3.10	April 2023	• Removed sub-section 'ADC Profile' from the section 'Agent Types are'. • Removed text ADC Profile from list under section Configuring Kyndryl Resiliency Orchestration	574, 74	8.3.x
8.3.11.0	May 2023	Added 13 screenshots for discovery AD2C updates	multiple	8.3.x
		Added AIX Validation Rules, Linux Validation Rules, Oracle Validation Rules, MSSQL Validation Rules, Windows Validation Rules sections under ‘Validation Manager > View Rules’	388-390	8.3.x
8.4.0.0	June 2023	Deleted section1. Using Resiliency Orchestration GUI Quick Start		
		Deleted section2. Agent Configuration Enabling WMI on Windows Subsystem (High level)		
		Using the new debugging capability for Dry run		
		Deleted section 3. Agentless Migration (SC mapping before Edit)		
		Deleted section 4. Organization Configuration Multiple Organization support		
		Deleted section 5. Multiple organization configuration Linking Directory Server Details to Subscriber		

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Deleted section 6. AD Groups to Kyndryl Resiliency Orchestration Roles		
		Deleted section 7. Create Users for Organizations using GUI		
		Cred migration script to extend to support management service creds		
		Removed "Configure SQS Mapping" button from listing page		
		Edit management service page -> test cred		
8.4.1.0	July 2023	Pagination added with 100 entires per page with screenshots under User management → configuration management → Events		
		In high availability SO/SB/FO section step c added to backup sitecontroller .cfg and update DR IP with the PR IP.		
8.4.2.0	August 2023	chapter 3 Discovery subsystem deleted now not applicable 20 pages Before ansible integration		
		Chapter 3 User Management User Screenshot Delete AD user		
		chapter 8. Configuration User management setting users		
		Chapter 17 Validation Manager Spectrum protect delete IBM		
		Chapter 18 Report viewing reports updated		
		Chapter 19 Discovery Sites deleted older inserted link. Credentials deleted Multiple User Credentials page 441 to 450		
		Chapter 20 Agent types are		

kyndryl™

Document Version	Revision Date	Sections Updated	Pages Updated	Supported Product Version
		Chapter 22 Admins screenshot updates mulitple		
		Chapter 23 Licensing introduction to Upload license deleted 594 to 597 deleted		
		User Management→ Vault configuration new steps added for XML Selective element to change required config parameters from open text to masked		
8.4.3.0	September 2023	Updated Screenshots in User management section		
		Updated section user management as per the changed UI		
		updated the RO Logs -> operational history -> Purge Log Now table.	852	
8.4.4.0	October 2023	Multiple sections revised with updated screenshots		
8.4.5.0	November 2023	Discovery-> Site-> Credential-> SSH credential		
8.4.6.0	December 2023	User Management ->SMTP password ->Note added (it will be blank to avoid plain password visibility vulnerability) Introduction -> List of protocols used by CRO Agent -> **Note:** Every end point will either have Local Agents or Remote Agents but cannot have both. RPO timestamp added to the Dashboard Active directory-> replaced screenshots as per new work flow		

Contents

Introduction

Kyndryl Resiliency Orchestration is an industry-leading software product for Business Continuity that addresses Disaster Recovery (DR) challenges. Kyndryl Resiliency Orchestration automates DR workflows by interoperating with several industry-leading Databases, Replication software, and Cluster Products and provides comprehensive Disaster Recovery Solution Management.

Note

In this document, the following list of terms will be used interchangeably.

- The product name **Kyndryl Resiliency Orchestration** and **Resiliency Orchestration** will be used interchangeably.
- The company name **Kyndryl**, **Kyndryl Technologies Corporation**, **Kyndryl Technologies**, and **Kyndryl Technologies Private Limited** will be used interchangeably.

Preface

Purpose

This manual is your guide for the operation and maintenance of the product. The document gives a detailed description of:

- All menu commands, icons, and links are available in the product.
- The terminologies used.
- Procedures to create, modify and delete various entities.
- Procedure to maintain an interface with a variety of features to accomplish a particular task.

Thus, the manual helps you to use the product with ease and makes you familiar with Kyndryl Resiliency Orchestration.

User Authentication and Authorization

Kyndryl Resiliency Orchestration supports three modes of user authentication and authorization. To toggle between different modes, refer Changing the Authentication/Authorization mode.

1. **Kyndryl Resiliency Orchestration User Management (Basic RO):** Users are authenticated and authorized locally by the Kyndryl Resiliency Orchestration application. System authentication is a basic user management system.

   Note: Kyndryl Resiliency Orchestration User Management and Basic(RO) are used interchangeably in this document as well as in the application.

2. **Third-Party User Management (AD Authenticate and Authorize):** Users are authenticated as well as authorized by a Lightweight Directory Access Protocol (LDAPS) server that uses Kerberos for the Windows domain networks. It is used to assign roles and privileges. Users are then mapped to these assigned roles and privileges. For more information, refer to the topic Configuring AD for AD Authenticate and Authorize mode.

   Note: In case there is a duplicate entry in both Kyndryl Resiliency Orchestration DB and AD server, then the user is not allowed to log in. For a successful login with AD Authenticate and Authorize mode, you will need to create a new user with a different username.

3. **Hybrid Authentication and Authorization (AD Authenticate and Basic RO Authorize):** Users are always authenticated by Active Directory with LDAPS protocol; however, authorization is handled by the Kyndryl Resiliency Orchestration application. For more information, refer to the topic Configuring AD for AD Authenticate and Basic RO Authorize.

Note:

1. User role options include out-of-the-box roles and configured roles assigned to AD Groups. Active Directory Groups (AD Groups) are a collection of users defined in the AD Server.
2. You can save the CA certificate in either DER Encoded Binary X-509 format or Based-64 Encoded X-509 format.

Enabling SSL Security for Active Directory

Exporting Certificate from Active Directory server

You must export the certificate authority CA certificate from the Active Directory server to enable Secure Sockets Layer (SSL) security.

To export the CA certificate, perform the following steps.

1. Log on as a domain administrator on the Active Directory domain server.
2. Click **Start > Control Panel > Administrative Tools > Certificate Authority** to open the CA Microsoft Management Console (MMC) GUI.
3. Highlight the CA computer, and right-click to select CA **Properties**.
4. From the General menu, click **View Certificate**.
5. Select the **Details** view and click **Copy to File** in the lower-right corner of the window.
6. Use the Certificate Export wizard to save the CA certificate in a file.

Note: You can save the CA certificate in either DER Encoded Binary X-509 format or Based-64 Encoded X-509 format.

Importing CA Certificate to Kyndryl Resiliency Orchestration Server

Import the certificate authority (CA) certificate that you exported from the Active Directory server to Kyndryl Resiliency Orchestration Server to configure the Secure Socket Layer (SSL) security.

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

1. Run the following command to import the CA certificate

   ```
   keytool -import -keystore
   $EAMSROOT/jdk1.8.0_{version}/jre/lib/security/cacerts -alias 'ad-server-cert' -
   file /tmp/abc.cer
   ```

   Note: $EAMSROOT/ is the folder location where panaces is installed and {version} is the JDK version installed in the system.

2. Enter the following keystore password when prompted.

   Password: <Password[1]>

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

3. Confirm the import command by entering "Yes" on the console.
   Do you trust this certificate? [No]: Yes

Adding or Modifying User for Active Directory Authentication

Add or modify a new user in the Active Directory and then assign default roles to the users. Add the same default roles in Kyndryl Resiliency Orchestration at the time of installation and map it to the user.

Note:

- The "drmadmin" user must exist in the AD server with administrative privileges.

  Create the "drmadmin" user only in case it does not exist in the AD server.
- With AD authentication, if the user tries to log in to RO with three failed attempts, then the user will be locked from logging in. However, the AD user will not be locked in Windows Active Directory.
- To add, modify, or delete users in Active Directory, please refer to Microsoft Active Directory documentation.
- The user needs to be authenticated by any of the authentication modes to successfully log in to the application.
- In case a new custom role is added to a user with Active Directory authentication, the same custom role should be created in the Kyndryl Resiliency Orchestration application as well. The same privileges are assigned to the respective user in Active Directory.
- To remove privileges from a role in Active Directory, please refer to Microsoft Active Directory documentation. To remove privileges from a role in Kyndryl Resiliency Orchestration refer to the topic Editing a Custom User Role.
- To remove the role in Active Directory please refer to Microsoft Active Directory documentation. To remove the role in Kyndryl Resiliency Orchestration, refer to the topic Deleting a Custom User Role.
- Added the user to the Domain Users group and set it as a primary account. Then we can log in to RO.

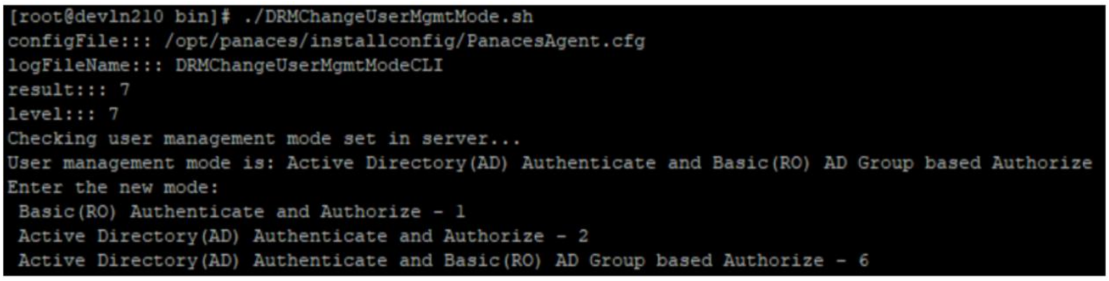
Changing the Authentication/Authorization mode

To change the authentication and authorization mode, run the script DRMChangeUserMgmtMode.sh.

Note - DRMChangeUserMgmtMode.sh script should not be used for multiple organization environments. Refer to section RO Installation for the alternate procedure for changing the mode.

Steps:

1. Go to $EAMSROOT/bin/
2. Input the command `sudo ./DRMChangeUserMgmtMode.sh`.
   Enter the required new mode when prompted. The options available are as shown in the below screenshot.



```
[root@devln210 bin]# ./DRMChangeUserMgmtMode.sh
configFile::: /opt/panaces/installconfig/PanacesAgent.cfg
logFileName::: DRMChangeUserMgmtModeCLI
result::: 7
level::: 7
Checking user management mode set in server...
User management mode is: Active Directory(AD) Authenticate and Basic(RO) AD Group based Authorize
Enter the new mode:
 Basic(RO) Authenticate and Authorize - 1
 Active Directory(AD) Authenticate and Authorize - 2
 Active Directory(AD) Authenticate and Basic(RO) AD Group based Authorize - 6
```

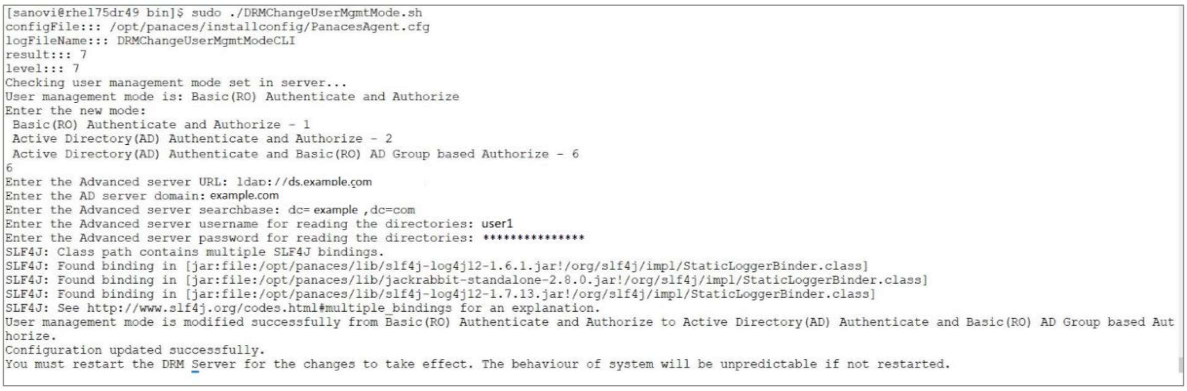
3. Select **Active Directory(AD) Authenticate and Basic(RO) AD Group based Authorize - 6** option for AD Group based authentication.

Note – If you have selected AD authentication and RO authorization (option 6), you will need to perform role assignments for AD Groups. For more information on role assignment to AD groups, refer AD Groups to Kyndryl Resiliency Orchestration Roles Mapping.

4. Enter the AD server username and password.
   Note - The password length supported by Kyndryl Resiliency Orchestration is 256 characters. Enter the password as per what is supported and configured in Windows Active Directory.
5. Restart the Kyndryl Resiliency Orchestration server services after running the script.

Note: In option 2, roles have to be assigned to individual users whereas in option 6, roles have to be assigned to AD groups.

Example:



```
[sanovi@rhel75dr49 bin]$ sudo ./DRMChangeUserMgmtMode.sh
configFile::: /opt/panaces/installconfig/PanacesAgent.cfg
logFileName::: DRMChangeUserMgmtModeCLI
result::: 7
level::: 7
Checking user management mode set in server...
User management mode is: Basic(RO) Authenticate and Authorize
Enter the new mode:
 Basic(RO) Authenticate and Authorize - 1
 Active Directory(AD) Authenticate and Authorize - 2
 Active Directory(AD) Authenticate and Basic(RO) AD Group based Authorize - 6
6
Enter the Advanced server URL: ldap://ds.example.com
Enter the AD server domain: example.com
Enter the Advanced server searchbase: dc= example ,dc=com
Enter the Advanced server username for reading the directories: user1
Enter the Advanced server password for reading the directories: ***************
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/opt/panaces/lib/slf4j-log4j12-1.6.1.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/panaces/lib/jackrabbit-standalone-2.8.0.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/panaces/lib/slf4j-log4j12-1.7.13.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
User management mode is modified successfully from Basic(RO) Authenticate and Authorize to Active Directory(AD) Authenticate and Basic(RO) AD Group based Aut
horize.
Configuration updated successfully.
You must restart the DRM Server for the changes to take effect. The behaviour of system will be unpredictable if not restarted.
```

Note: To successfully integrate Active Directory for Kyndryl Resiliency Orchestration, the user must provide the default Active Directory roles. This can be accomplished by any following methods.

- During the Kyndryl Resiliency Orchestration application installation, if you select **Advanced User Management System,** you will be prompted to enter comma-separated default roles configured in the Active Directory server.

- In case **Basic User Management System** was selected during installation, you will need to run the script DRMChangeUserMgmtMode.sh as shown in the steps above and add the comma-separated default ID roles configured in the Active Directory server.

List of protocols used by CRO

Sr. No.	Protocol	Industry Release version	Bank Use version	Existing version vulnerability is present or not	Vulnerability is exploited Yes/NO	Recommendation
1	TLS/SSL	TLS1.3	TLS1.2 or above	Present in TLS1.2	YES	Use latestTLS1.3
2	IMAP and POP	IMAP4rev2, IMAP5	IMAP4 and PO3	Present	YES	It should be disabled and enabled
3	SMB	SMB3.1.1	Not allowed	Present	YES	Use the version SMBv3.1.1
4	telnet		Not allowed	Present	YES	Replaced by SSH
5	ARP	ARPv2 with SEND	ARPv2	Present	YES	Use ARPv2 with SEND

Getting Started

Perform the following steps to start working with Kyndryl Resiliency Orchestration.

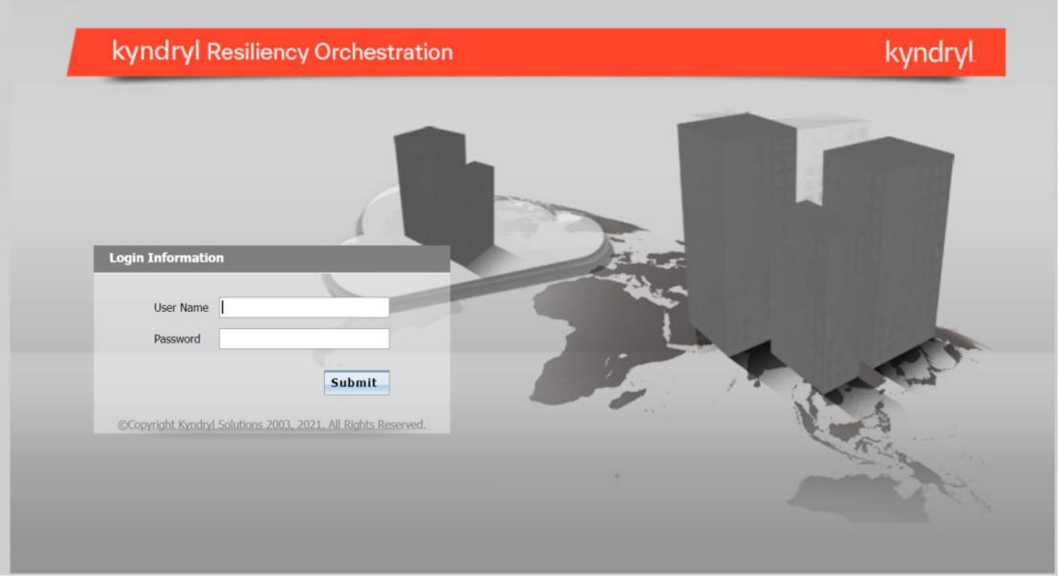
Logging in

1. Enter the following URL on the Internet Explorer browser for secure mode, use:

   https://<ip-address or name of the Kyndryl Resiliency Orchestration Server>:8443/PanacesGUI

   You can use either the IP address or the name (which could be a hostname or a Fully Qualified Domain Name (FQDN)) for launching the Resiliency Orchestration User Interface (UI).

   The following login screen is displayed in case only System Authentication mode is configured prompting the user for Username and Password.


kyndryl Resiliency Orchestration
kyndryl
Login Information
User Name
Password
Submit
©Copyright Kyndryl Solutions 2003, 2021. All Rights Reserved.

2. Enter the Username and Password in the respective fields.

   Note -

   - The default super administrator username is “drmadmin” and the password is “<Password[1]>”.

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

   - Username and Password are not prompted if the user has already been successfully authenticated via Active Directory mode. However, the user will need to enter the Username and Password in case the user is not already authenticated via Active directory.

- For System Authentication mode:
  - The super administrator configures the usernames
  - The password length is a minimum of 15 and a maximum of 25 alphanumeric characters including at least one digit for login to Kyndryl Resiliency Orchestration, as a part of GDPR enhancement

3. Click **Submit** to open the Kyndryl Resiliency Orchestration console.

FQDN Support

In Kyndryl Resiliency Orchestration, components/endpoints can be discovered using their IP address or name (which could be a hostname or a fully qualified domain name (FQDN)). You can use either the IP address or the name (which could be a hostname or Fully Qualified Domain Name (FQDN) for launching the Resiliency Orchestration User Interface (UI).

If you are using a name server or DNS server to resolve host names/FQDN, the host name/FQDN must be configured on the DNS server. If you are not using a name server or DNS server, an entry must be made in the /etc/hosts for the host name/FQDN to be resolved into an IP address.

Solutions that support FQDN

All DR solutions support FQDN until Group Discovery.
The following solutions are certified end-to-end with FQDN -

- Kyndryl GDPS Global Mirroring Replication
- VM to VM using NetApp Snap Mirror
- VM Protection with Resiliency Block Replicator

Support of Special characters in passwords used for Linux and Windows Operating Systems

This section describes the special characters that are supported in the Subsystem during discovery of Components in Kyndryl Resiliency Orchestration.

For Linux

Special characters	Comments

,?*.=:;}{}+%)^@!##-_(&/\$	It is recommended to choose a strong password that has a mix of alpha-numeric characters and special characters. Note: recommended not to use the below characters |`

For Windows

Special characters	Comments
,?*.=:;}{}+%)^@!##-_(&	It is recommended to choose a strong password that has a mix of alpha-numeric characters and special characters. Note: recommended not to use the below characters `$|\/

Special Characters in Usernames

This section describes the special characters that are supported in the username fields for the following solutions during discovery in Kyndryl Resiliency Orchestration.

- MySQL solution with Streaming Replicator
- Oracle Logs with DataGuard Replicator
- MSSQL solution with Log shipping Replicator

The table below lists the various special characters that are supported for the different subsystems.

Subsystems	Special Characters	Comments
Oracle/Oracle DG	_ $ #	It is recommended to choose a strong username that has a mix of alpha-numeric characters and special characters, with a minimum length of 32. It is recommended not to use reserved characters & @ Set of invalid characters not to be used

		`~!%^()-+=[]\{}:;'"<>.?/,
MySQL	. ! # % * ? - < , : ~ / > $ _	It is recommended to choose a strong username that has a mix of alpha-numeric characters and special characters, with a minimum length of 32. **Note**: Characters to be avoided in username are |'\"+ &$+=[]{()})
MSSQL	_ @ $. - , = * # / [! :] ~ % (?	It is recommended to choose a strong username that has a mix of alpha-numeric characters and special characters, with a minimum length of 32. **Note**: Characters to be avoided in username are not valid -; &+`'"\\|<>

Special Characters in Passwords

This section describes the special characters that are supported in the password fields for the following solutions during discovery in Kyndryl Resiliency Orchestration.

- VM to VM solutions with Zerto, SRM Hitachi, and NetApp Replicators.
- MySQL solution with Streaming Replicator
- Oracle Logs with DataGuard Replicator
- MSSQL solution with Log shipping Replicator

The table below lists the various special characters that are supported for the different subsystems.

Subsystems	Special Characters	Comments
Oracle/Oracle DG	‘ ~ ! # $ % ^ * ( ) _ - + = { } [ ] / < > , . ; ? ' : |	It is recommended to choose a strong password that has a mix of alpha-numeric characters and special

<table>
<tr><td></td><td></td><td>characters, with a minimum length of 32.
You must escape the following special characters while entering the password
' ~ !;?:|()[]#
To escape use the backslash escape character \
<b>Example</b> - "<Password>"

While entering the password in RO UI, do not give quotes. Use as <Password>

It is recommended not to use reserved characters & @</td></tr>
<tr><td>MySQL</td><td>~!@#$%^&*=>.,;?()_<}:`^{/!]-[</td><td>It is recommended to choose a strong password that has a mix of alpha-numeric characters
and special characters, with a minimum length of 32.
You must escape the following special characters while entering the password
~ !;?
To escape use the backslash escape character \
<b>Example</b> - '<Password>'
<b>Note</b> - 1. While entering the password in RO UI, do not give quotes. Use as <Password>
2. As a best practice, the password should begin with non-numeric characters
3. Characters to be avoided in the password are |'\"+</td></tr>
<tr><td>MSSQL</td><td>_@ $. - , = * # / [! :] ~ % (?</td><td>It is recommended to choose a strong password that has a mix of alpha-numeric characters
and special characters, with a minimum length of 32.
<b>Note</b>: Characters to be avoided in the password are
not valid - ;&+`'"\|<></td></tr>
</table>

Using Resiliency Orchestration GUI

Kyndryl Resiliency Orchestration GUI is divided into the following partitions:

Navigation Bar

Working Area

Event Alarm

Note -

Using the browser's back button may not work for a few pages and clicking on it will refresh the same page. Please use the navigation links available in the product to move out of the page.

Using Online Help

About Online Help

The console includes an HTML-based, cross-platform online help system. It provides information about using Kyndryl Resiliency Orchestration features and enables you to find information about a specific task.

For best results, view the help in Internet Explorer version 5.0 or later and Mozilla.

Launching Online Help

You can launch the online help system by clicking **Help > Help Contents**.

The online help opens in your default web browser. In the web browser, the left pane contains the **Contents**, **Index**, **Search,** and **Glossary** tabs. Navigate to different topics by clicking on them.

The Browser Environment

You can use the browser's navigation aids to navigate through the online help. You can resize the browser window to the desired size.

Use the **Back** button of the browser to return to the previously viewed topic. Use the **Forward** button to go to the topic that was displayed before going back.

Hiding / Showing the Navigation Pane

If you want to hide the navigation pane in the online help system, which includes the Contents, Index, Search, and Glossary tabs, click ☒ at the top left of the navigation pane. If you have hidden the navigation pane and want to see it again, click the **Contents**, **Index**, **Search**, or **Glossary** buttons.

Navigation Bar

The **Navigation Bar** in the Kyndryl Resiliency Orchestration window provides shortcut options to navigate through the different features of the product.

You can click the corresponding tab in the navigation bar to use the relevant features of Kyndryl Resiliency Orchestration. The **Navigation Bar** provides the following tabs:

Monitor

Manage

Drills

Reports

Discover

Admin

Logout

Note
At any point, if you want to go to the Home page, click the **Resiliency Orchestration** icon.

Breadcrumbs

The Kyndryl Resiliency Orchestration windows display breadcrumbs, a type of secondary navigation that enables users to identify their location in the application. Breadcrumbs provide a trail of the pages visited by the users. Links to these pages help the user to access the required page from the current location with a single click.

Breadcrumbs appear horizontally below the navigation and title bars.

Working Area

This is the key functional area of the Kyndryl Resiliency Orchestration window. This area displays windows for different features depending on the tabs chosen on the navigation bar. You can also view the current execution windows and perform different BCO operations.

Right Pane

This pane displays the list of configured Groups along with a drop-down menu from which you can select the criteria for displaying the Group information.

This information is displayed on the Right pane for any tab chosen on the navigation bar. Additionally, you can perform certain configuration operations by clicking the link or by selecting different options displayed in the pane. For example, on the Notifications window, click **Add Notification List** in the right pane to set up a new notification list to receive Event notifications.

Administration Overview

Kyndryl Resiliency Orchestration Administration console allows you to perform various administration activities like creating, modifying, or deleting the users, configuring notification lists, agents, and backup managers, managing logs, and handling Kyndryl Resiliency Orchestration Server failover.

You need to click **Admin** on the Kyndryl Resiliency Orchestration Home page to view the Administration Tasks Summary page.

About Kyndryl Resiliency Orchestration

You can view the Kyndryl Resiliency Orchestration Environment and Version information by entering the following command in the Kyndryl Resiliency Orchestration server -

./$EAMSROOT/bin/panaces version

The version command displays the following information about Kyndryl Resiliency Orchestration:

- Current Version details

- Kyndryl Resiliency Orchestration Environments

- Server Details

Limitation - Kyndryl Resiliency Orchestration users cannot find the Upgrade version history using the panaces version command. Previously the upgrade version history was available in the **Help** >**About** page in RO UI, which was removed due to security reasons. Please note that this limitation will be fixed in the upcoming releases in the panaces version command.

Log Out

Logs out the current user from Kyndryl Resiliency Orchestration. You are then taken to the Kyndryl Resiliency Orchestration Login page to log on to the product again.

Help

Select **Help** to navigate through the following options in the secondary navigation bar:

- **Contents & Index** - Provides quick accessibility to online information about the product.
- **About Kyndryl Resiliency Orchestration** - Displays the following information on Kyndryl Resiliency Orchestration:

  Product information
    Version details
    Copyright information

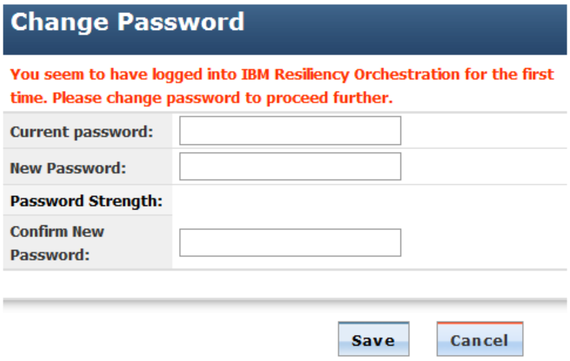
Note

You can also view the version of Kyndryl Resiliency Orchestration by entering the following command at `$EAMSROOT/bin location` in the Kyndryl Resiliency Orchestration server:

```
./panaces version
```

Changing Password

The Resiliency Orchestration administrator creates the login credentials of the user, the user needs to log in to the Resiliency Orchestration system to change the password. If the user has logged in for the first time, changing the password is mandatory. The following figure displays the Resiliency Orchestration Change Password screen, which prompts the user to change the password.



Change Password

You seem to have logged into IBM Resiliency Orchestration for the first time. Please change password to proceed further.

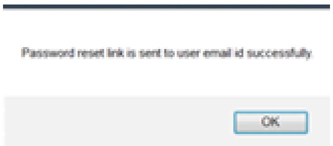
Current password:	
New Password:	
Password Strength:	
Confirm New Password:	

Note

The Resiliency Orchestration administrator creates the first login credentials for a user.

Reset Password

The Super Administrator only can reset the password of a user. The Super Administrator can initiate the change password option through the admin screen. Then the user receives an e-mail to the e-mail id configured in the profile, as shown in the following figure:



Password reset link is sent to user email id successfully.

The user needs to click the password reset link to reset the password. The Super Administrator needs to use this procedure to unblock the user.

Architecture Overview

Overview

Kyndryl Resiliency Orchestration is the industry-leading application and continuity management software for open system applications and databases. It is a framework-based continuity management software that enables consistent operational interfaces and reduces the expertise required to configure and operate the application continuity and disaster recovery solutions.

Kyndryl Resiliency Orchestration encapsulates all the required intelligence – processes and procedures required to interface with the application, replication mechanism, servers, storage, and networks to automate deployment and operation of the continuity solution.

Kyndryl Resiliency Orchestration offers a single console view of enterprise IT continuity health. It interfaces with the various layers of the continuity solutions and reports deviation on the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of the application, in real-time.

With its application-aware framework, Kyndryl Resiliency Orchestration significantly reduces the operational costs associated with the management of continuity assets, increases the productivity of the operations staff, and provides continuity assurance for mission-critical applications.

Kyndryl Resiliency Orchestration provides coherent and consistent binding of the state of applications and status of data at the time of an outage, so that recovery is quick, reliable, and needs little or no expertise.

Key Features

Key features of Kyndryl Resiliency Orchestration include:

Disaster recovery management for multi-site DR environments with the Continuity Monitoring, Continuity Management, Test Exercise Management, Continuity Reports, Discovery, and so on capabilities.

Continuity Monitoring

- Provides a dashboard view of the real-time status of the disaster recovery environment including the health of the sites, applications, replication mechanisms, and readiness of the disaster recovery systems for recovery.
- Provides a visual representation of the entire disaster recovery environment.
- Application-aware Event Manager provides support for multiple severity events.
- Supports multiple notification mechanisms, including EMS, e-mails, and text messages.
- Computes and tracks current recovery points for each application and reports deviations against set RPO.
- Detects application environment and configuration changes and provides alerts on impact.
- Provides real-time reports on data lag between primary and DR systems.
- Provides events dashboard across all applications.
- Correlates various infrastructure failures and events and provides support for root cause analysis.
- Monitors and provides real-time information on LAN link utilization and health.
- Estimates the recovery time for the various components of the solution – server, application, data recovery, and data consistency. Provides breakup of recovery steps, and estimated recovery time for each of these steps.
- Performs real-time monitoring of replication infrastructure and provides replication details including replicated data sizes, failure and success events, and vendor-specific replication object details.
- Provides database-specific transaction information on primary and remote systems.
- Provides uniform replication monitoring interface to all replicators.

Continuity Management

- Provides best practice template-based application provisioning into the Continuity infrastructure.
- Provides extensive customization capability of the templates using a visual workflow editor.
- Provides automated failover and fallback management, integrating into industry-standard databases and applications.
- Provides automated switchover and switchback management.
- Provides interfaces to start and stop continuity and replication operations for maintenance purposes.
- Provides RPO management to maintain the current data loss within the continuity objectives. Replication can be prioritized for applications managed by Kyndryl Resiliency Orchestration.
- Provides unified replication management, integrating into third-party replication products.
- Provides template-based policies and automated execution of policies for Events.

- Provides control to perform operations at an individual application level as well as a group of applications.

Test Exercise Management

- Provides intrusive and non-intrusive testing capability and tests DR readiness without impacting production services.
- Allows test suite customization to meet specific environments.
- Provides pre-packaged template-based test exercises.
- Restores the replication state after performing testing.
- Displays the real-time status of the test execution.
- Facilitates testing on snapshot copy apart from the target copy on the DR site.
- Displays "pre-test" checks to improve test success.
- Provides the option to start, stop, abort, roll back, and continue the test.
- Provides per application test dashboard.

Continuity Reports

- Graphical and tabular reports on various continuity management and monitoring areas including RPO, RTO, Continuity operations, , and data replication.
- Provide daily, weekly, monthly, quarterly, and yearly reports per the configurable options.
- Provides comprehensive filters based on RPO, and RTO (list of filters to provide).

Support for Heterogeneous Technologies

Support for Clusters

Clustering is the common term for distributing a service over several servers to increase fault tolerance and to support loads larger than a single server can handle. It is often used for large-scale and mission-critical applications where there can be no downtime. A cluster contains servers that share states at some level.

Kyndryl Resiliency Orchestration supports Hardware Clustering and Software Clustering:

- High availability clusters (also called Failover clusters, Hardware Clustering, etc.) are used to make sure no loss of service occurs when the primary server fails. Usually, in this case, secondary hardware is present to take over.
- Software Clustering (also called Application Clusters) is a method of turning multiple computer servers into a cluster (a group of servers that acts like a single system). Clustering software is installed in each of the servers in the group. Each of the servers maintains the same information and collectively they perform administrative tasks such as load balancing, determining node failures, and assigning Failover tasks.

Hence, Kyndryl Resiliency Orchestration supports application clusters by monitoring the application cluster nodes and ensuring when the entire cluster is not available to enable remote disaster recovery sites to take over.

Support for Software and Hardware Data Protection Technologies

In real-time data protection, the data is protected on a real-time basis wherein the data from the host server is copied onto the remote location as soon as the data is changed, over the network. Kyndryl Resiliency Orchestration supports the following types of protection technologies:

Storage-Based replication

Storage-based replication does not operate on the host computer. This kind of replication occurs at the storage device level. The disk arrays manage the replication of data between sites, relieving the hosts of the replication process.

Switch-based Replication

The replication is at the storage network level. The switch replicates the data from one site to a switch that receives the data at another site.

Host-Based Replication

Host-based replication typically resides at the file system or logical volume level within the operating system. Like storage-based offerings, it's usually transparent to the application, but certainly not transparent to the host operating system or hardware. Advantages of this method of replication include the ability to replicate to heterogeneous storage and similar (not necessarily identical) systems and the ability to reduce the required bandwidth.

- File-based Replication Technologies

  Host-based file replicator products

  The modified data at the primary site is identified based on the file modification time stamps and shipped over the network using the file replicator. This method combines the best of the benefits of remote mirroring technologies and software protection technologies.

- Database Replication Technology

  Data replication is at the logical level by re-constructing the database transactions at the remote server. This method has the advantage of minimizing the bandwidth required. It also supports protection against rolling disasters and user errors.

- Support for Databases and Cluster Applications

  Kyndryl Resiliency Orchestration monitors all the servers and applications assets across the sites and ensures workflow co-ordination among them.

  Kyndryl Resiliency Orchestration performs database setup on the near site with an initial copy of the database from the production to deploy new applications into DR.

- ***Support for Infrastructure***

  Kyndryl Resiliency Orchestration is configured into various devices like servers, storage, network, and WAN to monitor the continued health of the devices.

Key Benefits

Kyndryl Resiliency Orchestration enables an organization to effectively manage the continuity solutions and provide continuity assurance to the business with the following advantages:

- Accurate state information on the health of continuity systems, help IT managers resolve problems quickly.
- Automated monitoring significantly reduces the load on the operations staff and increases their productivity.
- Automated continuity management assures application continuity and makes recovery reliable and uniform across the enterprise.
- Deep application integration reduces the load on various IT administrators/ operations staff and increases their productivity.
- Provisioning of new applications into continuity assets is very fast and non-intrusive to production.
- Disaster readiness verification becomes practical and achievable with test automation.
- Cost avoidance in DR drills, as more tests can be performed within the same period with less vendor support.
- Increased uptime for the production applications, as production systems are not impacted during testing.
- CIOs get a consolidated business view of all the systems covered under Continuity.
- Detailed historical reports enable department and business unit heads to identify deviations in internal processes and enable corrective measures.
- SLA management becomes easy with real-time information available on various elements of the continuity infrastructure.
- By automating several monitoring functions, Kyndryl Resiliency Orchestration increases the productivity of the skilled administrative staff.
- Assists in identifying problems through event correlation and helps fix the DR systems timely.
- Automated template-based solutions make provisioning of new applications into DR, quick and non-intrusive to IT operations.
- Automated continuity operations and RPO management assures continuity and makes the recovery uniform across the enterprise.
- Pre-defined and automated execution of policies ensures uniform event response across the enterprise, irrespective of the time of day and non-availability of people and expertise.
- Automated testing ensures zero errors.
- No production downtime - Test DR site readiness without impacting production services.
- Comprehensive reports provide a high-level test status, execution details, and differences with past testing results.

How Kyndryl Resiliency Orchestration Works?

Kyndryl Resiliency Orchestration architecture is a distributed approach that ties together business goals, DR workflow, and solution infrastructure management to deliver an enterprise-class continuity manager product.

The **Business Layer** provides a way to specify business goals and monitor and manage how well they are met. Specifically, the Business Layer:

- Translates application continuity goals to RPO metrics.
- Translates time of day-based responses to coordinated action for each part of the solution.

The **Process Layer** provides proven, industry-tailored templates for automating the DR workflow involved in deploying and supporting IT continuity solutions. Specifically, the Process Layer:

- Standardize interactions and automates sequences of steps required for data consistency and application continuity.
- Provides a Policy engine to program and automate time-of-day-based responses to events.
- Automates tasks such as scheduled testing, report generation, and configuration change discovery.

The **Operations Layer** interfaces with the various components in the solution to monitor and manage to meet the overall business continuity goals. Specifically, the Operations Layer:

- Supports a distributed framework for component management.
- Supports an event bus and interfaces with other management packages.

Kyndryl Resiliency Orchestration offers a single web-based console and wizard-based setup and configuration. It inter-operates with leading vendor applications, replication products, and server, storage, and network environment.

Discovery

Discovery Overview

Discovery provides information on Sites, Subsystems, and Groups associated with the DR environment. Discovery allows you to configure Subsystems into the DR infrastructure. This has to be performed immediately after creating sites.

Use the below link to information on creating Sites, Subsystem,

https://pages.github.kyndryl.net/Resiliency-Orchestration/RODocumentation/topics/out/subsystem_discovery.html

You can View Sites, Subsystems, and Groups by clicking the **Discovery** tab on the navigation bar.

The **Discovery** tab provides the following links:

- Sites
- Subsystems

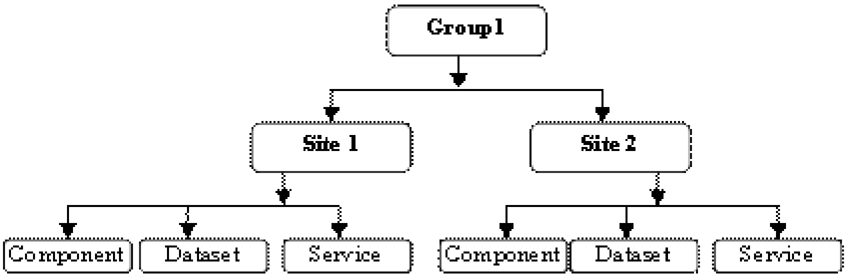
- Groups

Sites Overview

A **Site** defines a location. It can be a PR site or a DR site or a Remote site. A site is the location of Components, Datasets, and Protection Schemes in a DR environment.

Kyndryl Resiliency Orchestration supports Disaster recovery management for two and three-sites DR environments.

The diagrammatic representation of the two sites' DR environment is as shown below:



The Sites on the Home page window provides quick information on several configured sites.

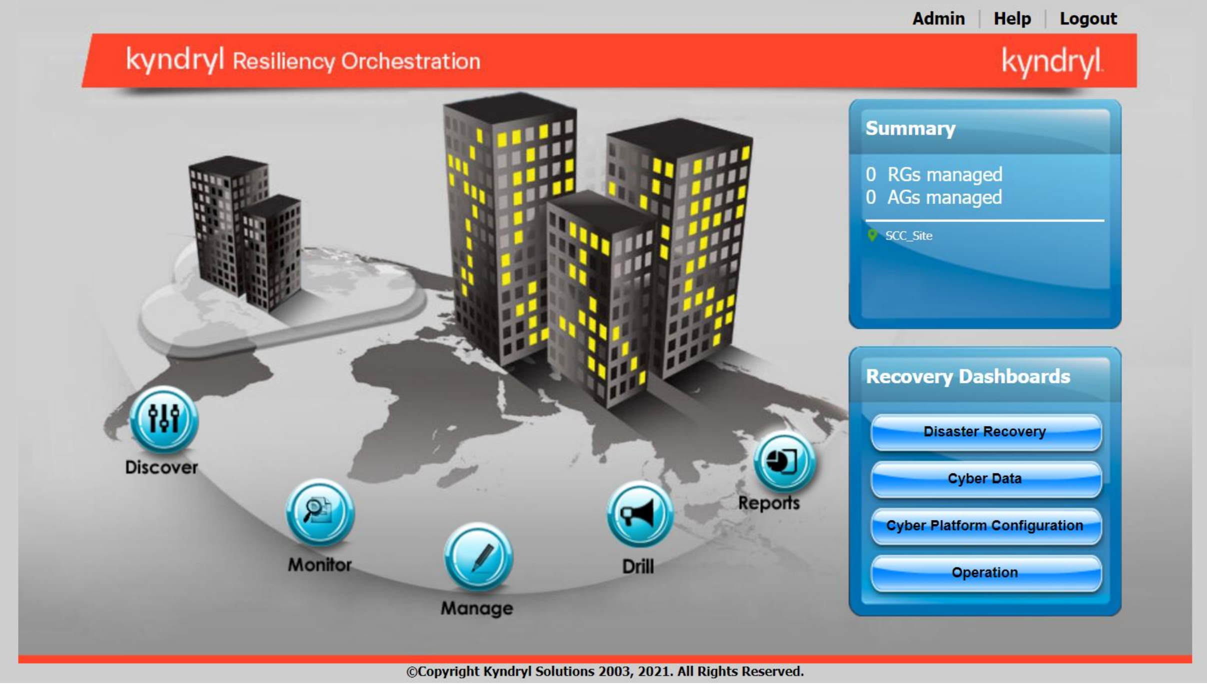
The different status of a site is as follows:

Status	Description
Active	The site is Active when all the Groups of the site are Active.
Inactive	The status refers to the non-working condition of the site. The site is Inactive when none of the Groups belonging to the site are Active.
Degraded	A site is Degraded if there are a few Active Groups and a few other Groups that are Inactive or Degraded on this site.
N/A (Not Applicable)	Site status becomes Not Applicable when no Groups are available for the site.

Note: When the group is in Maintenance mode, the site status might not get updated as site status is computed based on the Group status.

Home Page

This page is the start-up page that helps the user to connect to the various modules of the Kyndryl Resiliency Orchestration application. It displays the information such as user name, number of managed groups, etc., that is configured on the application.



The four icons (Monitor, Manage, Drill, and Reports) will be enabled if the module is licensed.

Note - Reports icon is always enabled since it is always licensed.

Clicking the icons will direct you to the following pages:

- **Monitor:** It directs you to the sites page.

- **Manage:** It directs you to the group's page.
- **Drills:** It directs to the Drills page.
- **Reports:** It directs to the Reports page.

The pane on the right-hand side of the page contains the following information:

- Name of the customer.
- The number of groups that are currently being managed.
- The site names that are discovered.
- Disaster Recovery Dashboard: It redirects to the **DR Manager Dashboard** page.
- Cyber Data Dashboard: It redirects to the **Cyber DR Dashboard** page.
- Cyber Platform Configuration: It redirects to the **Platform Recovery Dashboard** page.
- Operation Dashboard: It redirects to the **DR Operational Dashboard** page.

The links on the top will direct to the following pages:

- Admin: It directs to the **Agents** page.
- Discover: It directs to the **Groups** page.
- Help: It pops up the online help file of Kyndryl Resiliency Orchestration.
- Logout: This logs out the user.

Subsystems Overview

A **Subsystem** can be a Component, Dataset, or Protection Scheme. Subsystems together form a Group.

Click **DISCOVER > Subsystems** on the navigation bar, and the **Subsystems** page appears. The user can view the list of components, datasets, and protection schemes that have been discovered.

Groups Overview

A **Group** comprises of Component, Dataset, and Protection Scheme that are referred to as Subsystems. Dataset and Protection Schemes are dependent on the Component. Each Group is connected to a pair of sites (Production and DR site) and has an independent protection mechanism. Kyndryl Resiliency Orchestration users can be associated with multiple Groups, which in turn are connected to multiple sites.

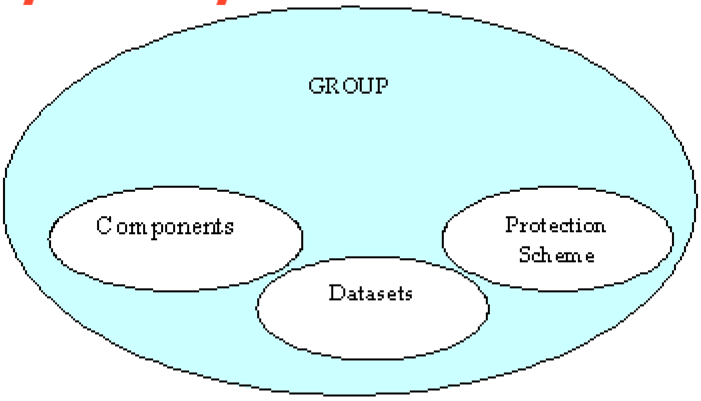
The following list provides a detailed explanation of the group entities:

Dataset - Represents an application whose data is to be protected.

Component – Represents the physical infrastructure on which the dataset is dependent.

Protection Scheme - Represents the mechanism by which you want to protect (replicate/ backup) the data.

Following is the pictorial representation of a Group:



A Continuity Group is called the Recovery Group (RG). In general, the RG is a basic unit of data. It is created for each application whose data protection has to be monitored and managed by Kyndryl Resiliency Orchestration. It comprises Datasets, Protection Schemes, and Components. These with their interdependencies represent the data to be protected (Datasets), the location of the data (Component), and the mechanism used to protect the data (Protection Scheme). One or more RG's are linked together to form an Application Group.

You can list Groups by performing the following steps:

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click the Recovery Group or Application Group tab, and the respective Group Listing page appears.
3. Click the desired Group in the **GROUP NAME** column to view the Group details in the **Group Details** window.

   - You can navigate to the Monitor, Manage, Reports, or Tests page of a displayed Group by clicking the respective icon Discover Monitor Manage Drills Reports at the top right corner of the window.check and change as required with screenshot

Refer to help- AD2C User guide - generic AD2C Edit group information.

Recovery Group

A Recovery Group (RG) is a basic unit of data with associated protection and infrastructure mappings that needs to be protected and managed by Kyndryl Resiliency Orchestration.

One or more RGs are associated together to form an Application Group (AG).

Application Group

An Application Group (AG) contains a set of RGs. An RG cannot be part of more than one AG at a time. AGs can be considered a container of RGs.

RGs belonging to different solution signatures can be added to an AG. Any operation which can be executed on an RG (if it is independent) can be executed even if it is part of an AG.

Example: A banking application requires three Oracle databases and one file system directory on the Application server. There are four RGs created, one for each database and another for the file system data. All these four RGs form a single AG.

Status of a Group

A Group (RG or AG) can undergo state change during its life cycle. The status of the Group is shown along with its name in the **Groups** window of the **DISCOVERY** page.

The status value of a Group provides information such as:

- If any critical, serious, or warning events are raised in the group.
- If the Group is in Managed or Maintenance mode.

The Group status information is divided into two parts:

Execution Mode

Group Status

Execution Mode

The Execution Mode of a Group is given below:

Execution Mode	Description
Managed	When the Group is in Managed mode, then you can perform all operations on it. The group status computation is turned on. Note that no monitoring information is available immediately after the group is moved to managed. Hence the status can be Grey until events are raised in the group As soon as events are received the group status will be computed to Green Amber or Red
Maintenance or Unmanaged	The group status should be Grey When the Group is in Maintenance mode, you can modify the Group or maintain the Kyndryl Resiliency Orchestration server. No status computation (monitoring) can be carried out.

The Resiliency Orchestration Admin will not be able to view network down events, generic events, or resource registration events on the current events page and these events should not affect group status.

The Resiliency Orchestration Admin should be able to view the WorkFlowFailure event on the current events page which should not affect group status and an e-mail should be sent.

Execution Status

The execution state of a Group reflects the health of the production data availability and also, the status of all the dependent infrastructure components, protection, and database objects. This state information is valid only when the Group is in MANAGED mode.

This state information is ignored in other execution modes.

Following Execution State values are possible in MANAGED mode:

Execution Status	Description
🟩	The production and DR data are available for the Group and all the dependent objects are running. Group status is green when there are no critical, serious, or warning events open and only info events are present.
🟥	Production or DR data is unavailable currently. This may be due to the PR or DR server's down condition. This state may also mean that one or multiple (including all) dependent objects are down currently. Group status is changed to Red if there are any critical events raised.
🟧	Production or DR data may be in the database down condition. However, one or multiple dependent objects of the Group are down either at the PR site or the DR site. Group Status is changed to Amber if any warning and serious events are raised.
▨	Group Status is changed to Grey when no monitoring information is available. When no monitoring information is available(there are no actionable events available). When the Monitoring license is not enabled for the group E.g.: group status is not applicable for Test only license.

Group Health Status of a Group is computed automatically, whenever a change in the state of any of the dependent objects is detected. During BCO execution, the Group will have the following change status for the described conditions:

Group Health Status change during BCO	Description
Green to Amber	This transition occurs if any action associated with the Group fails or is awaiting input from you. If the Group is already in Amber or Red state, the status will not change.

Group Health Status change during BCO	Description
Amber to Green	If you have provided the required input and resumed the BCO execution. If there are no further failures, the Group execution status will be changed from Amber to Green.
Amber to Green	If you have aborted the action requiring the input, it will be taken as an input and the execution status will be changed to Active. However, the continuity status of the Group will change to DR Impaired, as you have aborted the action.

For the above conditions, the change in RGs execution status will be immediate. However, similar changes for AGs will take up to one minute.

Note:

Wait for events to compute status when the group is in maintenance mode.

After Switchover or Switchback, it takes time to display the group status.

Recovery Status

Recovery status reflects the current state of the Group concerning either crash recovery or backup/ recovery from Kyndryl Resiliency Orchestration software metadata (Internal Database).

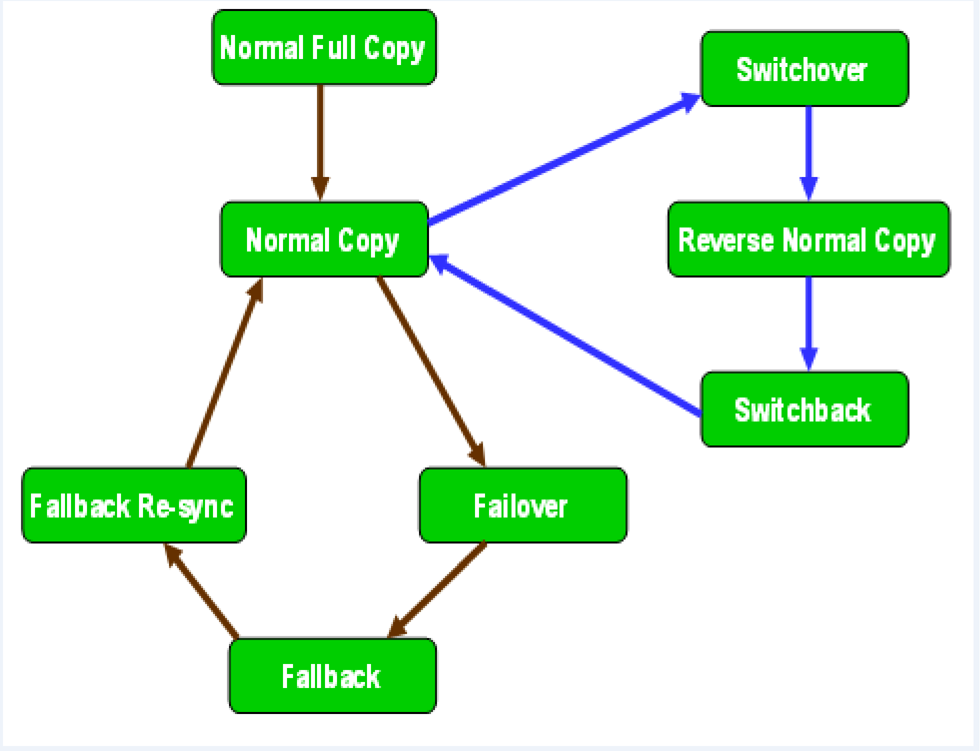
Valid Recovery State values are:

Recovery status	Description
NEED RECOVERY	A Group will be put into this Recovery State when the Kyndryl Resiliency Orchestration server is started with a recovery option. In this state, no continuity operations are allowed to be executed. Events will not be reported.
RECOVERING	A Group, whose state information is being recovered by the Recovery Wizard, is put into this state. During this state also, no new operations may be executed on Group. Events will not be reported.

Note: An RG may be in one of the above Recovery states, while it is in any of the execution modes. The system automatically sets this state depending on the above conditions.

The Execution Mode of the Application Group could be UNMANAGED, MANAGED, and MAINTENANCE. When an AG is moved from one mode/state to another, the associated Recovery Groups will also move to the corresponding mode. The group status of the Application Group is RED, even if one of the associated Recovery Group is RED i.e. only if all the Recovery Groups are Green, the Application Group is GREEN. If at least one Recovery Group is AMBER, the Application Group is AMBER.

The following chart explains the life-cycle of a Group.



Continuity Operations on a Group

Points to remember while working with Continuity Operations:

1. If any BCO fails on an RG associated with an AG, then the BCO is considered to be failed at the AG level.
2. For a BCO on an AG to be successful, the same should be successful on all the FG's associated with the AG.
3. Failover of an entire AG occurs when Failover on RG is triggered either manually or because of any events.
4. Before the Failover of AG, all the operations that are currently being performed on all dependent RG's are stopped.
5. For RG's that are independent, Failover occurs at the respective RG level only.
6. Failover can happen at AG level and not at RG level. All the RG's are required to be active for an AG to be active. There is an ordered dependency of RG's under an AG. So, if a Failover or Fallback at AG should happen it happens on all RG's under it in the order that is defined.
7. Every Group (AG and RG) has to be managed in the DR environment.

Note:

In all the list pages, the row is highlighted in case the group is in failover mode.

Business Continuity Modes

Business Continuity Modes (BCM) represents the current mode of Continuity Group whose data is protected. Typical modes are Normal, Failover, and Fallback.

BCM defines one or multiple continuity operations, such as Normal Copy and Failover. These operations enable a Group to transit from one BCM to another mode and one ***Business Continuity State*** to another state. Each continuity operation is represented by a workflow. Every Business Continuity Solution defines this operation and provides suitable configuration interfaces.

The business Continuity State represents the relationship of the Production Dataset concerning the DR Dataset.

Supported Business Continuity States are:

- *Normal*
- *Failover*
- *Fallback*

Business Continuity Modes	**Operations**	
Normal	The day-to-day process of data protection occurs between PR and DR sites. There are two continuity operations in this mode.	
	NormalFullCopy (Initial)	The process of copying the entire Dataset from the PR site to the DR site. This is a one-time process. This process can be paused and resumed by clicking the Pause/ Resume button respectively for the Application Recovery on AWS solution (VMware to AWS)
	NormalCopy (Recurring)	The data difference between the PR server and the DR server is transferred from the PR site to the DR site and applied to the DR server.
Failover	The process of transferring control or business continuity from the Production site to the DR site when the Production site is down or inactive.	
Fallback	A full dump of data is taken on the current PR server and applied to the configured PR server. The business control is transferred from the current PR server (DR server) to the configured PR server. In this operation, the PR server is brought into production. At the end of this operation, the PR server's data is ready for replication and the DR server is made standby.	
FallbackResync	This operation brings the production server and DR server in sync. The PR and DR servers are made ready for NormalCopy operation.	

Business Continuity Modes	Operations
Change Continuity State	This continuity operation allows you to move the BCM of a Group from the current BCM to a new BCM. This operation is possible only when the Group is not executing any continuity operations currently. A Group may be moved into only four targets BCM's: 1. NORMAL RESET 2. NORMAL INACTIVE 3. FAILOVER ACTIVE 4. FALLBACK ACTIVE Note: This operation may be used only by an advanced administrator to bypass certain operations or recover from certain failures. Usage of this operation may significantly impact the Continuity Management of the Group, if not performed correctly.

Business Continuity States

The following table provides the definitions of each of the Business Continuity States along with the corresponding message displayed on the GUI:

State	Description	Message Displayed on the GUI
Normal Reset	In this state, the DR dataset is not in a known replication state. It has to be synchronized with the PR dataset for any DR activity to take place. This is the initial state of the Group.	DR impaired. DR operations have not started.
Normal Transit	A state change is occurring into Normal mode. Replication is not occurring in this state however; the PR and DR datasets may be getting synchronized during this state. In the end, the Group goes to a Normal Inactive state.	DR Enabled. Initial Synchronization is in progress.
Normal Inactive	In this state, the DR dataset and PR dataset are in a known replication state; but replication is not occurring between them.	DR Ready. Synchronization stopped.
Normal Active	PR and DR datasets are in a known replication state and a normal mode of data replication and restoration is occurring.	DR Ready. Synchronization is in progress.
Normal Failed	PR and DR datasets are in a known replication state however, the	DR Ready. Synchronization stopped.

State	Description	Message Displayed on the GUI
	normal mode of data replication and restoration failed for some reason.	
Normal Degraded	PR and DR datasets are in a replication state and a normal mode of data replication and restoration is occurring. However, the system encountered intermittent errors in the normal mode of processing in the last 'X' minutes.	DR Active. Failover recovery in progress.
Failover Transit	The PR is down and the system is transferred to the DR site for production. Replication of the log is suspended.	-
Failover Failed	During the transit to Failover BCM, failures occurred. The functioning of PR is down, replication is not occurring.	DR impaired.
Failover Active	The control of business is switched to the DR site. PR dataset is down on the PR site and replication does not occur on this site.	DR Active. Recovery complete.
Fallback Transit	PR is transferred from the DR site to the PR site. No replication process is going on.	DR Ready. Fallback in progress.
Fallback Failed	Transition to PR site failed. Resume Fallback again to recover. No process of replication is going on. PR is on DR site.	-
Fallback Active	PR is switched to the PR site. PR dataset may be up or down. But the DR dataset and PR dataset are not ready for replication yet.	DR Ready. Fallback in progress.
Normal Shutdown	If Kyndryl Resiliency Orchestration software crashes or a forceful shutdown of the server is performed, Business Continuity Operation at that time will be changed to Normal Shutdown state.	-
Normal Stopping	This is a transient state operation. If Normal Copy is stopped manually (i.e., by clicking the Stop Normal Copy button), then the Group is	-

State	Description	Message Displayed on the GUI
	moved into this state until the operation is completely stopped.	
Normal Test	If a test exercise is initiated on a Group, the Group is moved into this state. Test exercise can be initiated only when the Group is in a Normal Inactive state.	-

About RPO, RTO

Recovery Point Objective

It is an acceptable amount of data loss from the last good backup before the point of failure.

For example, if you consider an overnight backup, the Recovery Point Objective will often be the end of the previous day's activity.

- **Data RPO –** This is for the replication mechanism in your set-up. Data RPO of 10 minutes means data till 10 minutes ago is replicated into DR from PR.
- **App RPO** – App RPO is based on the database transaction timestamps. App RPO of 10 minutes means the last transaction applied on DR and the last transaction applied on PR differed by 10 minutes.

Recovery Time Objective

The time taken for the business to be back online after a disaster i.e. the time taken to get back to Business Continuity.

Example: Let us assume that the data replication is happening between the PR and DR site. A retailer determines that, in case of a system failure at the PR site, it is acceptable to lose business data for the last two hours (RPO). But after two hours the retailer cannot afford to lose business and somehow the data must be made available to restart the business. This is done by bringing up the DR site as a PR site until the PR site is up again. The required time taken by the retailer to start the business application at the DR site and to move the business forward is one hour, which is known as RTO.

Managing RPO and RTO

Kyndryl Resiliency Orchestration provides constant monitoring of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) values and provides alerts to indicate any deviations from these goals based on the configured tolerance limits. It also provides enough control to tune some replication parameters using which, one can alter the RPO value, Kyndryl Resiliency Orchestration provides the following key capabilities for RPO and RTO management, for each database under protection:

Compute Current App RPO

Displays the desired and current RPO values and the supporting solution-specific information, such as the last log/file transaction id or name and the time when the File System was most recently updated or modified on the PR server.

Compute current Data RPO

Displays the desired and current Data RPO values and the supporting replication-specific information, such as the last file modified timestamp for PR & DR.

Note: Data RPO is supported only for the following replication mechanisms

- PFR
- EMC SRDF
- Kyndryl Global Mirror
- NetApp Snap Mirror

The Resiliency Orchestration framework is also designed to support Data RPO for replication mechanism that falls under the category of **Other Replicators**. Refer to Other Replicator Features and Other Replicator Oracle Archive Logs for more information.

Compute current RTO and display the desired RTO and estimated RTO values

Monitors current RPO and RTO values and raise alerts if deviations are noticed beyond a configurable tolerance limit.

The reliability and latency of the network link play an important role in RPO value.

Terms	Definition
Recovery Point Objective	The acceptable amount of data loss from the last good backup before the point of failure.
Recovery Time Objective	Time is taken to bring a system back online following a failure.

The RPO/ RTO Manager provides support to configure RPO/ RTO values.

Note:

‘RPO Compute Interval’ determines the minimum time interval for the RPO graph.

RPO and RTO computations are completely dependent on the underlying Business Continuity Solution (BCS) and are handled by the individual BCS. If RPO or RTO are found to be outside their threshold values, an event is raised with appropriate severity by BCS.

RPO/ RTO configured values and the current values are displayed in the **Monitor** or **Manage** page, under the Recovery Groups window. If RPO and RTO are set at the AG level, then the same applies to all the RG's associated with it. Every RG of this AG doesn't need to be consistent at any point in time.

This window lists RPO/ RTO details as given in the following table:

Field	Description
Current App RPO Value	Displays recently computed App RPO value for the RG.
Current App RPO Time	Displays recently computed App RPO time stamp. For example, The current App RPO time stamp is 12p.m, Monday, 4th June 2004. The current time is 12.30 P.M., Monday, 4th June 2004. Therefore, the App RPO time-stamp indicates 30 min time lag on the date.
Configured App RPO Value	These are user-specified values for accomplishing recovery within the stipulated time.
The time when RPO computed	It is the time when the App RPO was computed.
App RPO deviation	Displays the percentage deviation between the current App RPO and the configured App RPO. When the current value exceeds the configured value, it flashes in red color.
Additional RPO details	Displays the dataset and the RG-specific details.

The following table explains the terms associated with RTO:

Field	Description	
Current RTO Value	Displays the recently computed RTO value for the RG.	
Current RTO Time	Displays the recently computed RTO time stamp.	
Configured RTO value	These are user-specified values for accomplishing recovery within the stipulated time.	
A time when RTO computed	Displays the time when RTO was computed.	
RTO deviation	Displays the percentage deviation from the configured RTO. When the current value exceeds the configured value, it flashes in red color. Note: The current RTO is always greater than the computed RTO.	
RTO Breakup	It specifies the time duration to execute various recovery procedures that constitute the overall recovery. i.e. Failover.	
	Recovery step name	This tells about individual recovery procedures for the RGs.
	Expected Completion time	This gives the amount of time remaining to complete the specified step if recovery is in progress.

The following are the additional details that are shown in the 'Additional App RPO Details' section.

Field	Description
Transaction ID	The transaction id in the database on both the PR and DR servers.
Transaction Time	The time at which the last transaction happened on both the PR and DR servers.

The additional details are displayed only during NormalCopy when the replication is happening.

Immediately after starting NormalCopy Operation, the DR database transaction time stamp is always shown ahead of the PR, because the last action of NormalFullCopy is a transaction on the DR. But once the first log is applied, the timestamp is always shown of the transaction on the Production.

Note:

The timestamps of both the PR and DR servers must be synchronized. Using a common time server or synchronously changing the clock time on both Production and DR could achieve a synchronous timestamp. If the timestamps of Production and DR are not the same, the RPO calculation may show zero or a negative value.

The Recovery Point (RPO) of an AG is dependent on the following:

The highest RPO of RGs if they have been selected to have an impact on AG during the AG group creation.

The recovery time (RTO) of an AG is dependent on the following:

- A sum of RTO of all RG's (if serially failed over).
- Factor in parallel execution of Failover of Recovery Group.

The window below lists the details of RPO and RTO at the Application Group level. This displays the terms associated with RPO/RTO and displays the configured and current values of the RPO/ RTO. The RPO/RTO values are shown during NormalFullCopy and NormalCopy operations only.

During Failover Active mode, the RPO/ RTO page of the Application Group is exactly similar to the RPO/RTO page of the Recovery Group. Failover at the AG level implies Failover on all RG's associated with the AG. The Failover time of the AG is calculated as the sum of the recovery time of all RG's associated with the AG.

The information on RPO/RTO window during Failover-Active mode is given below:

Field	Description
Current Continuity Mode	Displays the mode of continuous operation. The different modes could be NormalFullCopy, NormalCopy, Failover, Fallback, and FallbackResync.

Field	Description
Current Continuity State	Displays the current continuity state. The different continuity states are Active, Inactive, and Degraded.
Time of Failover	Displays the time stamp when the Failover has been completed.
The Data was recovered to	Displays the time stamp when the data was recovered to the DR site.

Refer to DR Solutions Supported by Kyndryl Resiliency Orchestration for information on solution-specific RPO and RTO.

RPO Calculation

The RPO calculation is done via RO implementation only, there is no external replicator for the App Native solution. The backups are taken through the RO scheduler frequency which will calculate the RPO. The Metadata stored in the RO database can be replicated via MariaDB replication only.

Prerequisites

- The network connection bandwidth must be sufficient to support replication from primary to DR.
- Administrator/ root equivalent privileges are required for Kyndryl agents.
- Kyndryl requires remote console access to the servers.
- Disk space should be allocated on the database servers to hold transaction logs for up to 3 business days and full backup (equal to the size of the database itself).
- There must be two sites (logical). The first one is termed the Production site, which under normal operating conditions has the PR database/ application. The second site is termed the DR site, which under normal conditions has the database/ application operating as a standby.
- The two sites are connected over an IP network connection. The network connection bandwidth must be sufficient to support the replication of log files from the Production to the standby.
- Kyndryl Resiliency Orchestration's primary server ideally resides on the DR site. There is a Kyndryl Resiliency Orchestration server on the Production site that is configured as the standby Kyndryl Resiliency Orchestration server.
- Kyndryl Resiliency Orchestration's primary server has network access to the Production and standby servers and all other components of the DR Solution.

Additional Support

In addition to providing documentation, Kyndryl offers the following services:

For assistance with Kyndryl Resiliency Orchestration, contact technical support at orchestration.support@kyndryl.com

Starting and Stopping Kyndryl Resiliency Orchestration Server Services

To start and stop Kyndryl Resiliency Orchestration server services manually, perform the following steps:

1. Log in to the Kyndryl Resiliency Orchestration server machine as a user with administrative privileges.
2. At the command prompt, enter one of the following commands:
   - To start: $EAMSROOT/bin/panaces start
   - To stop: $EAMSROOT/bin/panaces stop

NOTE

When continuity operations are being executed, you should not stop the Kyndryl Resiliency Orchestration server service.

If you are executing any BCO, perform the following steps to stop the executing BCO before stopping the service:

1. Click **Manage**> **Executing Workflows**. The **Executing Workflows** page is displayed.
2. Select the Recovery Group filter from the drop-down list.
3. Click the **Executing** link in the **Status** column for the specific group name. The workflow page appears.
4. Click **Abort**.
5. Log off from Kyndryl Resiliency Orchestration GUI.

On Server Restart

After restarting the Kyndryl Resiliency Orchestration server, continuing NormalCopy automatically starts. If it does not start, you may need to increase the start-up delay settings for Agents.

To resume NormalCopy, open the **panaces.properties** file on the Kyndryl Resiliency Orchestration server and set the below parameter to an appropriate value.

```
panaces.server.startupDelayForAgents
```

Starting and Stopping Kyndryl Resiliency Orchestration Agents

The scripts deployed at the time of agent installation starts the agents when the server is rebooted. However, the agents can be started manually without rebooting the server. Similarly, they can be stopped using manual procedures. Moreover, the agent status can be verified.

Starting Kyndryl Resiliency Orchestration Agents

Starting of Agents on Windows Server

Note

Ensure that the clock setting on the Kyndryl Resiliency Orchestration server and the agent server are in sync.

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the agents installed on the server, perform the following steps:

1. Go to Control Panel and click Administrative Tools.
2. Click the **Services** icon on the Administrative Tools window. You can see the agents installed on the server.
3. Right-click the respective service on the **Services** window and select **Start** from the context menu to start the service.

Starting Agents on the UNIX Server

To start the Agents, enter the following in the command prompt as mentioned in the table below:

Agent	**Commands**
OS Agent	For Solaris: # cd $EAMSROOT # nohup ./SolarisOSAgent.sh start &
	For Linux: # cd $EAMSROOT # nohup ./LinuxOSAgent.sh start &
	For AIX: # cd $EAMSROOT # nohup ./AIXOSAgent.sh start &
	For HPUX: # cd $EAMSROOT # nohup ./HPUXOSAgent.sh start &
SFR Service	# cd $EAMSROOT # nohup ./PFR.sh start &
PFR Agent	# cd $EAMSROOT # nohup ./PFRAgent.sh start &
Sybase Agent	# cd $EAMSROOT # nohup ./SybaseAgent.sh start &

Agent	Commands
SRS Agent	# cd $EAMSROOT # nohup ./SRSAgent.sh start &
Data Guard Agent	# cd $EAMSROOT # nohup ./DataGuardAgent.sh start &
SRDF Agent	# cd $EAMSROOT # nohup ./SRDFAgent.sh start &
Oracle Agent	# cd $EAMSROOT # nohup ./OracleAgent.sh start &
HP XP Agent	# cd $EAMSROOT # nohup ./HPXPAgent.sh start &
TrueCopy Agent	# cd $EAMSROOT # nohup ./TrueCopyAgent.sh start &
PostgreSQL Agent	# cd $EAMSROOT # nohup ./PostgresAgent.sh start &

Stopping Kyndryl Resiliency Orchestration Agents on Window Server

Note

Ensure that the clock setting on the Kyndryl Resiliency Orchestration server and the agent server are in sync.

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the Agents installed on the Windows server, perform the following steps:

1. Go to Control Panel > Administrative Tools.
2. Click the **Services** icon on the Administrative Tools window. You can see the agents installed on the server.
3. Right-click the respective service on the **Services** window and select **Stop** from the context menu to stop the service.

Stopping Agents on the UNIX Server

To stop the Agents, enter the following in the command prompt as mentioned in the table below.

Agent	Commands
OS Agent	For Solaris: # cd $EAMSROOT # nohup ./SolarisOSAgent.sh stop &
	For Linux: # cd $EAMSROOT # nohup ./LinuxOSAgent.sh stop &
	For AIX: # nohup ./AIXOSAgent.sh stop &
	For HPUX: # nohup ./HPUXOSAgent.sh stop &
SFR Service	# cd $EAMSROOT # nohup ./PFR.sh stop &
PFR Agent	# cd $EAMSROOT # nohup ./PFRAgent.sh stop &
Sybase Agent	# cd $EAMSROOT # nohup ./SybaseAgent.sh stop &
SRS Agent	# cd $EAMSROOT # nohup ./SRSAgent.sh stop &
Data Guard Agent	# cd $EAMSROOT # nohup ./DataGuardAgent.sh stop &
SRDF Agent	# cd $EAMSROOT # nohup ./SRDFAgent.sh stop &
Oracle Agent	# cd $EAMSROOT # nohup ./OracleAgent.sh stop &
HP XP Agent	# cd $EAMSROOT # nohup ./HPXPAgent.sh stop &
TrueCopy Agent	# cd $EAMSROOT # nohup ./TrueCopyAgent.sh stop &
PostgreSQL Agent	# cd $EAMSROOT # nohup ./PostgresAgent.sh stop &

Verifying Kyndryl Resiliency Orchestration Agents

Verifying Agents on Windows Server

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the agents installed on the server, perform the following steps:

Go to **Control Panel > Administrative Tools**.

Click the Services icon on the Administrative Tools window. You can see the agents installed on the server.

Check whether the agents are installed and started or not.

Verifying Agents on UNIX Server

To verify the Agents, enter the following in the command prompt as mentioned in the table below:

Agent	**Commands**
OS Agent	For Solaris: # cd $EAMSROOT # nohup ./SolarisOSAgent.sh status &
	For Linux: # cd $EAMSROOT # nohup ./LinuxOSAgent.sh status &
	For AIX: # nohup ./AIXOSAgent.sh status &
	For HPUX: # nohup ./HPUXOSAgent.sh status &
SFR Service	# cd $EAMSROOT # nohup ./PFR.sh status &
PFR Agent	# cd $EAMSROOT # nohup ./PFRAgent.sh status &
Sybase Agent	# cd $EAMSROOT # nohup ./SybaseAgent.sh status &
SRS Agent	# cd $EAMSROOT # nohup ./SRSAgent.sh status &
Data Guard Agent	# cd $EAMSROOT # nohup ./DataGuardAgent.sh status &
SRDF Agent	# cd $EAMSROOT # nohup ./SRDFAgent.sh status &

Agent	Commands
Oracle Agent	# cd $EAMSROOT # nohup ./OracleAgent.sh status &
HP XP Agent	# cd $EAMSROOT # nohup ./HPXPAgent.sh status &
TrueCopy Agent	# cd $EAMSROOT # nohup ./TrueCopyAgent.sh status &
PostgreSQL Agent	# cd $EAMSROOT # nohup ./PostgresAgent.sh status &

Verifying the Processes of Agents on the UNIX Server

Enter the following command to check whether the processes of agents have been running or not.

- # ps –ef | grep –i LAX

This command will list the names of the agents that have been running.

Refreshing Details

You can configure the Refresh Rate of **Recent Workflow Execution Status** page. For other pages, it is already configured.

The following table shows the refresh rates of each page and subsections.

Page/ tab Title	Refresh Rate (in Seconds)
Main Dashboard Tables	
Sites	30
Groups Continuity Summary	10
In Progress	10
Groups	20
Events Summary	10
Test Summary	20
Replication Summary	10
Users	20
Monitor	
Continuity	20
Replication	20

Page/ tab Title	Refresh Rate (in Seconds)
Events	20
Recovery Group Dashboard	
Group Snapshot tab	30
RPO/RTO tab	30
Replication tab	30
Application Group Dashboard	
Group Snapshot tab	8
Manage	
Workflow List	10
Groups List	20
Manage Groups	
Group Information tab	10
Normal Copy Advance Details section	4
Manage DR Solution tab	30
Manage Replication section	300
Recovery Workflows tab	300
Crash Recovery section	30
Drills	
Drills	20
Group Workflow Listing	10
Test Exercise Dashboard	10
Reports	
Reports Group List page	20
Discovery Sites	
Sites List	10
Discovery Subsystems	
Components tab	10
Datasets tab	10
Protection Scheme tab	10

Page/ tab Title	Refresh Rate (in Seconds)
Subsystems right pane section	10
Discovery Groups	
Groups List	20
Admin	
Agents	10
Workflow Recent Execution Status	
Recent Execution Status section	50 (Configurable)
Workflow Graph & Inputs	50 (Configurable)
Workflow Actions	50 (Configurable)

Configuration

Configuring Kyndryl Resiliency Orchestration

On completing the installation, configure Kyndryl Resiliency Orchestration in the following order:

- Tomcat Configuration
- Configuring Agents
- Sites
- User Management
- Discover Subsystem
- Notifications
- Business Process Integration
- Workflow Manager
- Group Creation
- Recovery Automation Library (RAL)
- Agent Node Configuration
- Vault Integration
- Converged

Multiple-Node Solution supported configuration

Custom/Field solutions enable the end-user to have multiple node servers on the primary and secondary. To create a recovery group on the RO Master Server, the user must add the solution signatures with a comma (,) separated under *$EAMSROOT/installconfig/MultiNodeSolution.properties*.

For example: MultiNodeSolutions=DB2 Protection with HADR, VMProtection with DB2

Apache Tomcat Configuration

Steps to Enable HTTPS in Tomcat:

1. Go to the machine tomcat installation directory
2. Default ”keystoreFile/Password(Certificate)” is shipped with the product. To use the Customer certificate, get the Keystore file and password from the customer and modify the keystoreFile value with the keystore file path and keystorePass value with the password (check yellow marks for placeholders)
3. Open $TOMCAT_HOME/conf/server.xml
4. Search for below snippet of code if not available add the below

```
Connector port=“8443” protocol=“HTTP/1.1” maxHttpHeaderSize=“8192”
maxThreads=“150” minSpareThreads=“25” maxSpareThreads=“75”
enableLookups=“false” disableUploadTimeout=“true”
acceptCount=“100” scheme=“https” secure=“true”
clientAuth=“false” sslProtocol=“TLS”
keystoreFile="/$EAMSROOT/installconfig/keystore/sanovi.keystore”
keystorePass="<Password[1]>” SSLEnabled=“true”/>
```

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

All panaces should be pointed to the Resiliency Orchestration installation directory.

If the connecter is commented uncomment and restart the tomcat server.

5. Restart the Tomcat.

Note

If the machine does not start, restart the panaces.

Steps to Disable HTTP in Tomcat

1. Open $TOMCAT_HOME/webapps/{webapp_to_diable_HTTP}/WEB-INF/web.xml Ex: $EAMSROOT/tomcat/webapps/PanacesGUI/WEB-INF/web.xml
2. Make sure redirectPort is set to HTTPS port. For example, see the below snippets on server.xml

```
<Connector port="8080" maxHttpHeaderSize="8192"

    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
```

```
          enableLookups="false" redirectPort="8443" acceptCount="100"

          connectionTimeout="20000" 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"

          clientAuth="false" sslProtocol="TLS" keystoreFile="/opt/panaces/installconfig/keystore/Kyndryl.keystore" keystorePass="<Password>"/>
```

3. Add below snippet of code below after all Mappings

```
     <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>
```

This code will automatically redirect all HTTP requests to HTTPS. This setting is per web application.

Steps to Change the Port Numbers 8080 or 8443 to Different Ones

1. Open $TOMCAT_HOME/conf/server.xml
2. Search for Connector and change the port number. The port number should be in the range of 1025 to 65535. For example, see the below snippet

```
<Connector port="8081" maxHttpHeaderSize="8192"
     maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
     enableLookups="false" redirectPort="8443" acceptCount="100"
     connectionTimeout="20000" disableUploadTimeout="true"
     URIEncoding="utf-8" />
```

3. Before changing the port check/confirm if Firewall/IDS is not blocking the port and is not used by other applications running on the same server.

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/c
ss,
text/javascript,text/json,application/x-javascript,
application/javascript,application/json”
connectionTimeout=“20000” 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/c
ss,
text/javascript,text/json,application/x-javascript,
application/javascript,application/json”
clientAuth=“false” sslProtocol=“TLS”
keystoreFile="/opt/panaces/installconfig/keystore/IBM.keys
tore” keystorePass=“<Password>”/>
```

To Start/Stop the tomcat outside panaces script, follow the procedure below:

1. Change directory to $TOMCAT_HOME/bin
2. Run startup.sh/startup.bat depending on the OS to start the server.
3. Run shutdown.sh/shutdown.bat deepening on OS to stop the server.
4. If Tomcat is started using step 2, it has to be stopped with step 3 only. Panaces script can’t be used to stop Tomcat.

Tomcats Logs Rotation

For Tomcat logs (catalina.out) rotation, follow the procedure below:

1. Create this file /etc/logrotate.d/tomcat
2. Copy the following contents into the above file.

   ```
   $TOMCAT_HOME/logs/catalina.out {
   ```

```
copytruncate
daily
rotate 7
compress
missingok
size 10M
}
```

3. Run the following command to run the cron job manually

```
/usr/sbin/logrotate /etc/logrotate.conf
```

Agent Configuration

An agent is a software component that runs on your application server to manage and monitor a specific Component, Dataset, or Protection Scheme. Agents are installed on remote servers locally (using CD installations).

Note: Uniagent is the only supported model.

To monitor and modify the configured agents, perform the following steps:

1. Click **Admin** on the navigation bar. The **Administration** page appears.
2. Click on **Agents Summary**. The Agents page appears.

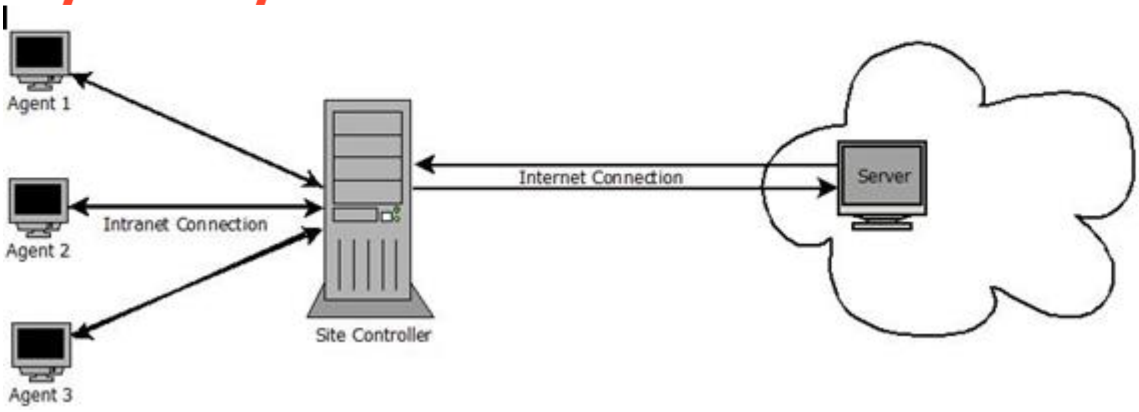
To configure the solution-specific agents, refer to the respective solution guide under DR Solutions Supported by Kyndryl Resiliency Orchestration.

Note: Every end point will either have Local Agents or Remote Agents but cannot have both.

Site Controller

Agents communicate to Resiliency Orchestration Server over the network (LAN). Agent communication to the Resiliency Orchestration server over the LAN requires the opening of necessary ports between all the applicable PR/DR (client) servers and the Resiliency Orchestration Server. Hence, the ports that need to be opened for communication are proportional to the number of PR/DR servers.

The site controller augments by acting as a gateway for the set of agents for communicating with the Resiliency Orchestration server. The site controller is capable of managing its agents, hence when the Site controller is installed within LAN, it helps in reducing the bandwidth usage as the communication over WAN to the Resiliency Orchestration Server is greatly reduced.



There are multiple supported configurations for the Site Controller, they are:

1. Agents are configured to run locally – the agents are configured to communicate to a Site Controller and all the deployed Site Controller(s) are configured to communicate to the Kyndryl Resiliency Orchestration Server. Since the Site Controller acts as a gateway, ports for agent communication need to be opened between the Site Controller and the Kyndryl Resiliency Orchestration Server. Hence the ports that need to be opened are proportional to the number of Site Controller Server(s).

For Example, Site Controller-PR is the Site Controller on Primary and Kyndryl Resiliency Orchestration is running on the DR site. All the agents on the primary are installed on PR Servers. The agents leverage Site Controller-PR for communication to Kyndryl Resiliency Orchestration, while Site Controller-PR will manage the health of the agents.

   a. In the absence of a Site Controller, agent communication ports between every PR/ DR server and Kyndryl Resiliency Orchestration Server need to be opened over WAN.

   b. With Site Controller, only agent communication ports between Site Controller-PR and Kyndryl Resiliency Orchestration Server need to be opened over WAN. The ports for communication of agents and Site Controller-PR need to be opened but only over LAN.

2. Agents Run remotely on Site Controller Server (s) – The Site Controller augments Agent Node functionality by acting as a gateway for all the agents running on that agent node. This brings the advantages of the remote agent, agent node, and Site Controller together.

For Example, Site Controller-PR is the Site controller on Primary and Kyndryl Resiliency Orchestration is running on the DR site. All the agents on the primary are installed on the same Site Controller Server. The agents leverage Site Controller-PR for communication to Kyndryl Resiliency Orchestration, while Site Controller-PR will manage the health of the agents.

   a. In the absence of a Site Controller, with a dedicated Agent Node, agent communication ports between the Agent Node and Kyndryl Resiliency Orchestration need to be opened. However, Kyndryl Resiliency Orchestration will manage the health of the agents over WAN.

b. With Site Controller, while only agent communication ports between Site Controller-PR and Kyndryl Resiliency Orchestration Server need to be opened over WAN, the health of agents is managed by Site Controller and not by Kyndryl Resiliency Orchestration. Thus reducing the network usage over WAN.

3. Some agents are local and some agents are remote (mixed) – this is the combination of the above two deployment models.

FAQs

1. How does the communication between Kyndryl Resiliency Orchestration, Site Controller, and endpoints on MSSQL/Oracle happen to perform a health check?

   Kyndryl Resiliency Orchestration Agent monitors the status of endpoints (MSSQL / OS / Oracle and so on) and sends the event to Kyndryl Resiliency Orchestration through Site Controller, apart from this, the Kyndryl Resiliency Orchestration agent sends its health status in form of heartbeat to Kyndryl Resiliency Orchestration Server through Site Controller. Site Controller performs some optimization on heartbeat and sends it to Kyndryl Resiliency Orchestration Server.

2. How the execution takes place? Is it directly between the Kyndryl Resiliency Orchestration and end points or between the Kyndryl Resiliency Orchestration and Site Controllers?

   Kyndryl Resiliency Orchestration Agent is responsible for operating on the endpoint subsystem. All the communication happens between the Kyndryl Resiliency Orchestration Server and the Kyndryl Resiliency Orchestration Agent through the Site Controller.

3. What happens if the Site Controller fails or does not respond? What is the monitoring part, does this happen?

   The agent will be disconnected to Kyndryl Resiliency Orchestration. All the event and health monitoring will be impacted till the Site Controller is up.

4. What if the Site Controller fails or not respond? What is the execution part, does this happen?

   The agent will be disconnected to Kyndryl Resiliency Orchestration. All the call fails till the Site Controller response is up.

5. Does Kyndryl Resiliency Orchestration support multiple Site Controllers so that if one fails, the other takes over?

   Yes, multiple Site Controllers can be configured.

Agentless

Kyndryl Resiliency Orchestration software supports an Agentless model where users need not install and run any Resiliency Orchestration-specific software component on their data/application servers. Resiliency Orchestration software accesses the customer servers using industry-standard remote access mechanisms like SSH/ WMI/ JDBC.

Note:

- The agentless model is not supported for DB2, Sybase, and SRS solutions.
- For remote agents: Create Kyndryl Resiliency Orchestration node component as local.
- When we invoke a command from RAL into Resiliency Orchestration in the Agentless model, we do not load the bash profile. For example, If you set the Environmental variable, then the value of the variable will not appear.
- Command configuration in RAL with relative path will not work.

Prerequisites

The target system should meet the following prerequisites for Kyndryl Resiliency Orchestration to work in the Agentless model:

Enabling SSH on Unix/Linux subsystem

1. Firewall setting: SSH port should be open for access from the Resiliency Orchestration Server.
2. SSH server should be running on the target server that allows connections from the Resiliency Orchestration Server for the configured user.

   Note: The configured user should not be having nologin setting on the Linux subsystem.
3. The Sftp module should be enabled for ssh and it can be enabled by editing a file in the operating system.

For example, in Linux edit /etc/ssh/sshd_config by un-commenting line 'Subsystem sftp /usr/libexec/openssh/sftp-server, execute command service sshd reload.

Converting OpenSSH Private key to RSA Private key

The Kyndryl RO UI accepts only the RSA Private key. If you upload the OpenSSH Private key, then the UI displays an exception error.

Perform the following steps to convert an OpenSSH Private key to RSA Private key:

1. Copy the OpenSSH Private key to the Linux VM on one location.
2. Execute the following command to provide proper permission:

```
chmod 0600 id_rsa_fra05
```

3. Execute the following command to convert the OpenSSH private key to RSA private key:

```
ssh-keygen -p -N "" -m pem -f id_rsa_fra05
```

4. Validate if the id_rsa_fra05 file is converted to RSA private key.
5. Copy the id_rsa_fra05 key file to the local machine, upload it in RO UI, and validate.

Enabling PowerShell on Windows subsystem

Enable PowerShell on Windows (SiteController/Endpoints) servers with the below commands for remote operations:

1. Select **Start** in the Windows system and then enter **PowerShell**.
2. From the listed programs, navigate to **Windows PowerShell**, right-click, and then select **Run as administrator**.
3. In the Windows PowerShell command prompt, enter the following commands. Use the required IP and username, where these are applicable:
    - To enable PowerShell remoting in the Site Controller PowerShell console, run the following command as administrator:

      ```
      Enable-PSRemoting –Force
      ```

    - To add your Windows End Points' IP to the trusted host, run the following command:

      ```
      Set-Item wsman:\localhost\client\trustedhosts *

      Example:

      Set-Item WSMan:\localhost\Client\TrustedHosts -Value
      '192.168.152.4'
      ```

    - To enable the PowerShell session in all Windows SC machines, run the following command. For Windows-based solutions, you need to run this command in the PowerShell terminal to enable the session:

      ```
      Restart-Service WinRM
      ```

To connect remotely to DCOM, follow the below steps:

1. Start > run > dcomcnfg. The Component Services page appears.
2. Expand Component Services > Computers.
3. Right-click on **My Computer** > select **Properties**. The **My Computer Properties** window appears.
4. Click the **COM Security** tab and in the **Launch and Activation Permissions** section do the following:
    - Select the **Edit Limits** button and perform the steps from 5 – 7.
    - Select the **Edit default** button and perform the steps from 5 – 7. The **Launch Permission** screen appears.
5. Select under Group or User names as Administrator.

   Note

   If the Administrator option is not available, create a new one.

    a. Select the **Add** button
    b. Enter Administrator in **Enter the Object names to select** field.
    c. Click the **Check Names** button and click **OK**.
6. Under the **Permissions for Administrators** section, select the **Allow** check boxes of the below options:

- Local Launch
- Remote Launch
- Local Activation
- Remote Activation

7. Click **OK**.

To connect remotely to WMI, follow the below steps:

1. Start > Run > type wmimgmt.msc. The Windows Management Infrastructure page appears.
2. Right-click on WMI control and select Properties. The WMI Control (Local) Properties page appears.
3. Select the Security tab. Select **Roots > CIMV2**. The **Security** page appears.
4. Select under Group or User names as Administrator.

   Note

   If the Administrator option is not available, create a new one.

   a. Select the **Add** button
   b. Enter Administrator in **Enter the Object names to select** field.
   c. Click the **Check Names** button and click **OK**.
5. Select the checkboxes of **Execute Method** and **Remote Enable**.
6. Click **OK**.

Known Limitations

Issue:
There were unusable UniAgent present on the Site Controller, which caused other existing UniAgent to fluctuate.

Resolution:

1. Navigate to the Service Listing page using - (Windows + Run > services.msc)
2. Locate the unusable UniAgent.
3. Copy the unique name of the UniAgent service.
4. Delete the *UNI_AGENT_SERVICE_NAME* from the Site Controller.

Change / Replace Ownership

Administrator users require taking ownership to perform registry operations for CLSID/AppID. If a user is unable to create Strings for CLSID keys, perform the following steps.

Note: Follow the same steps for AppID.

1. Start > Run > regedit. The Registry Editor page appears.
2. HKEY_CLASSES_ROOT > CLSID > {76A64158-CB41-11D1-8B02-00600806D9B6}.

3. In the right-hand pane, right-click **New > String Value.**

   Note:

   If you get an error message displaying "Error creating value", do the following steps:

   a. Select the key value {76A64158-CB41-11D1-8B02-00600806D9B6} > Right-click> Permissions. The Permission screen appears.

   b. Under the **Security** tab, select **Administrator** and select the **Advanced** button.

   Note:

   If the Administrator option is not available, create a new one.

   - Select the **Add** button
   - Enter Administrator in **Enter the Object names to select** field.
   - Click the **Check Names** button and click **OK**.

- Double-click on Administrator. The Advanced Security Setting window appears.
- Go to the **Owner** tab, and select the **Administrator** in the **Change Owner to** section.
- Select Replace owners and sub-containers in the objects checkbox and click OK.

Open Custom Range of ports WMI/ RPC:

To enable WMI, we need to have open ports between 49152-65535. If you don't want to open the full range, then you can also configure it in Registry Editor with a specific range example: 50000-50100 (this will be used for any RPC, WMI, etc)

In Windows Server 2008 and later versions, and in Windows Vista and later versions, the default dynamic port range changed to the Start port: 49152 - End port: 65535

Note:

If your computer network environment uses only Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows 8, Windows 7, or Windows Vista, you must enable connectivity over the high port range from 49152-65535.

Range configuration for WMI/RPC

1. Start > Run > regedit. The Registry Editor page appears.
2. Select HKEY_LOCAL_MACHINE > Software.
3. Select Microsoft > Rpc > Internet.

   Note

   If the Internet key is not available, create a new key. Right-click under **Rpc > New > Key >** enter the name as the **Internet**.

4. Select the Internet key and In the right-hand pane,

   1. Right-click **New > Multi-string Value** (to create multi-string value).
   2. Right-click **New > String Value** (to create string value).

Note

Create a total of 3 strings – 1 with multi-string value and 2 with string value as shown below:

- "Ports" (MULTI_SZ),
- "PortsInternetAvailable" (REG_SZ),
- "UseInternetPorts" (REG_SZ).

For example, the new registry key appears as follows:

```
Ports: REG_MULTI_SZ: 50000-50200
PortsInternetAvailable: REG_SZ: Y
UseInternetPorts: REG_SZ: Y
```

5. Restart the server. All applications that use RPC dynamic port allocation use ports 50000 through 50200, inclusive.

Note

In most environments, a minimum of 200 ports should be opened, because several system services rely on these RPC ports to communicate with each other.

Additional settings on the PFR subsystem

Firewall settings:

- Port 46000, 46001, and 46443 where PFR service is listening should be open for Kyndryl Resiliency Orchestration Server access.
- The PFR Agent version and SFR Service version should be the same.

Configuration

When the Agentless model is used, Resiliency Orchestration software needs additional configuration.

As part of subsystem discovery, the user needs to provide additional information that is used to access customer servers remotely. This includes credential information to access a customer server. These are described on the subsystem discovery page in detail.

If multiple servers can be accessed using the same credential information, Resiliency Orchestration provides an option to enter the credentials once and then can be attached to any number of subsystems. This is explained under **Credentials**.

To use Kyndryl Resiliency Orchestration as an Agentless model, the user needs to discover the Resiliency Orchestration server machine as a component and start an agent on the Resiliency Orchestration server system.

Refer to **Management**, to start the agent and refer to Configuration, to discover a component. Once this step is done, the user can go ahead with other subsystems and group discovery.

Monitoring

When the Agentless model is used, Resiliency Orchestration software provides additional monitoring.

Kyndryl Resiliency Orchestration software keeps monitoring the credential information and informs users about failure by raising alerts and changing the status. The following events are raised to indicate the change in credential status.

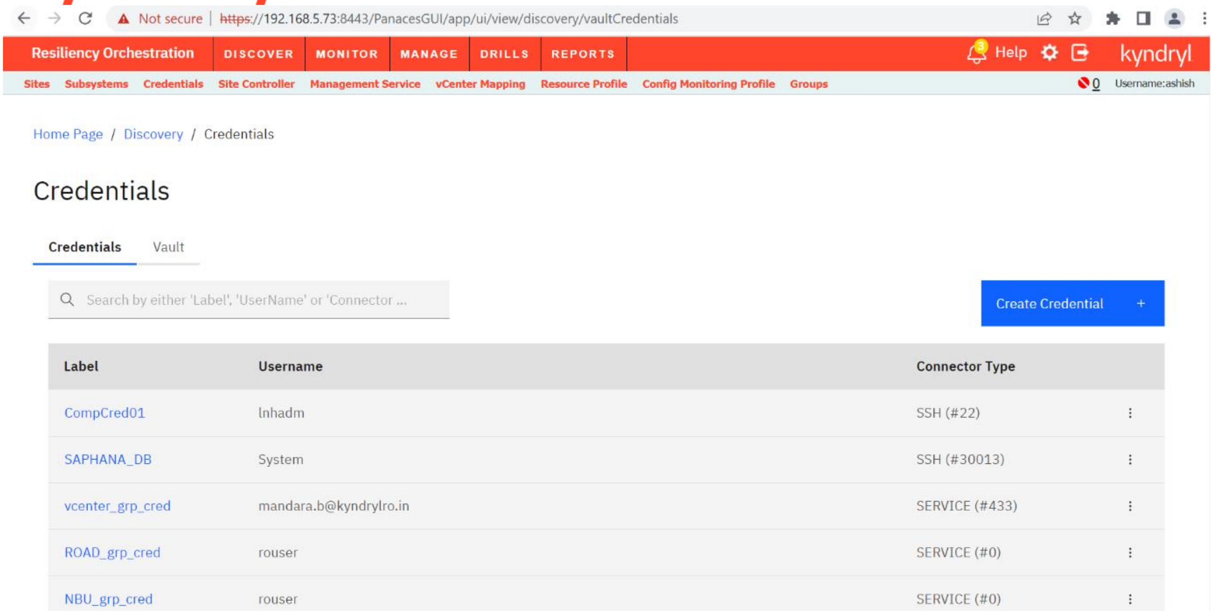
Event ID	Event Description	Event Impact
LoginFailedOnDRServer	Login failing on the DR Server	Recovery and Monitoring may be impacted
LoginFailedOnPrimaryServer	Login failing on Primary Server	Recovery and Monitoring may be impacted
LoginSuccessOnDRServer	Login Success on the DR Server	Recovery and Monitoring will work normally
LoginSuccessOnPrimaryServer	Login Success on Primary Server	Recovery and Monitoring will work normally
PrimaryServerAccessible	The Primary Server is accessible	Recovery and Monitoring will work normally
PrimaryServerNotAccessible	Unable to connect to Primary Server	Recovery and Monitoring may be impacted
DRServerAccessible	DR Server is accessible	Recovery and Monitoring will work normally
DRServerNotAccessible	Unable to connect to the DR Server	Recovery and Monitoring may be impacted

The status of the credentials is shown for each subsystem on the subsystem listing page or subsystem details page. Click **Discover > Subsystems** to view the credentials.

The following icons display the credential status:

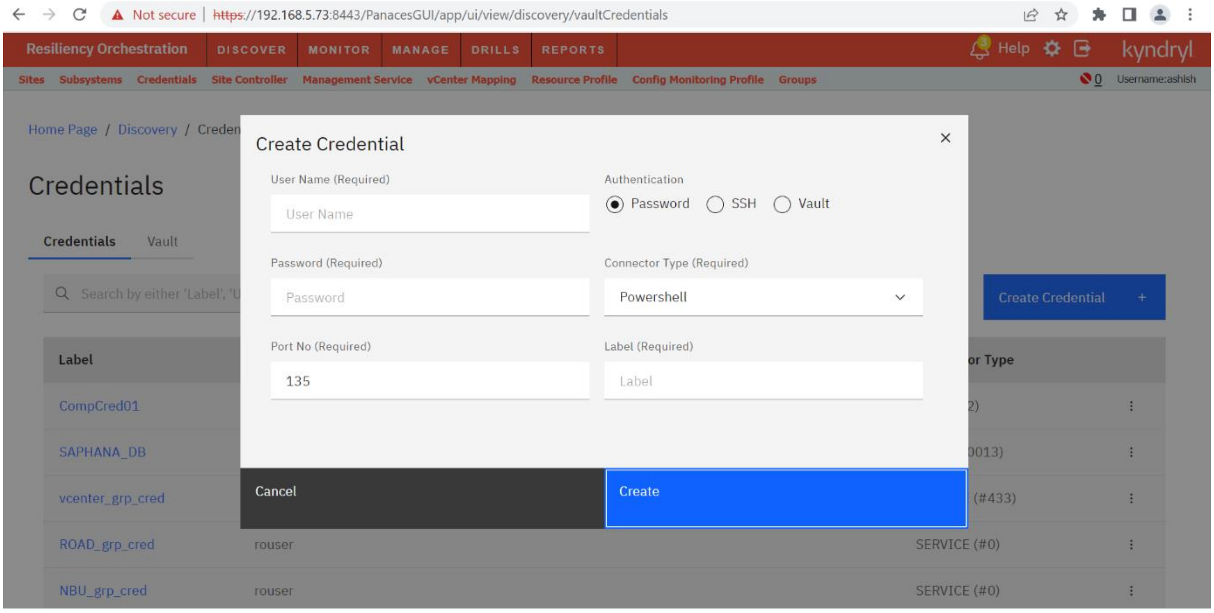
✓ - given credentials are good.

✗- given credentials are failing.



Credentials

Label	Username	Connector Type
CompCred01	lnhadm	SSH (#22)
SAPHANA_DB	System	SSH (#30013)
vcenter_grp_cred	mandara.b@kyndrylro.in	SERVICE (#433)
ROAD_grp_cred	rouser	SERVICE (#0)
NBU_grp_cred	rouser	SERVICE (#0)



Create Credential

User Name (Required): User Name

Authentication: ● Password ○ SSH ○ Vault

Password (Required): Password

Connector Type (Required): Powershell

Port No (Required): 135

Label (Required): Label

N.A - Not applicable – when agents run locally or credentials are not required for technology.

Unknown – Initial status or when no credentials are provided.

Note:

If the target system is down or the agent is down, the credential status will remain the last known status.

Management

When the Agentless model is used, Resiliency Orchestration software provides additional Agent management.

1. At any point in time or for maintenance, the user can stop/start Agents as follows:
2. Click **Admin** on the navigation bar. The **Kyndryl Resiliency Orchestration Administration** page appears.
3. Scroll down to the **Agents Summary** and click **Go to Agents**. The **Agents** page appears.
4. Click **the Stop/ Start** button for the required Subsystem.

No further call will go to the target server after stopping the Agent for the server. Users will receive an alert message saying *"agent managing the subsystem is down/ up*" depending on the Stop/ Start option.

Note

Start / Stop all the Agents individually for a component.

Users can also start and stop these processes using the command line. Go to $EAMSROOT/bin and enter the following command:

Servers	Commands
SOLARIS	Go to $EAMSROOT/bin > SolarisOSAgent.sh <start|stop> <ip address> SOLARISSERVER
LINUX	# cd $EAMSROOT/bin > LinuxOSAgent.sh <start|stop> <ip address> LINUXSERVER
HPUX	# cd $EAMSROOT/bin > HPUXOSAgent.sh <start|stop> <ip address> HPUXSERVER
AIX	# cd $EAMSROOT/bin > AIXOSAgent.sh <start|stop> <ip address> AIXSERVER
WINDOWS	# cd $EAMSROOT/bin > WindowsOSAgent.sh <start|stop> <ip address> NTSERVER
ORACLE	# cd $EAMSROOT/bin > OracleAgent.sh <start|stop> <ip address> <SOLARISSERVER|LINUXSERVER|HPUXSERVER|AIXSERVER|NTSERVER>
DATAGUARD	# cd $EAMSROOT/bin > DataGuardAgent.sh <start|stop> <ip address> <SOLARISSERVER|LINUXSERVER|HPUXSERVER|AIXSERVER|NTSERVER>
TrueCopy	# cd $EAMSROOT/bin > TrueCopyAgent.sh <start|stop> <ip address> <SOLARISSERVER|LINUXSERVER|HPUXSERVER|AIXSERVER>

Servers	Commands
HPXP	# cd $EAMSROOT/bin > HPXPAgent.sh <start|stop> <ip address> <SOLARISSERVER|LINUXSERVER|HPUXSERVER|AIXSERVER>
PFR	# cd $EAMSROOT/bin > PFRAgent.sh <start|stop> <ip address> <SOLARISSERVER|LINUXSERVER|HPUXSERVER|AIXSERVER|NTSERVER>

If the user wants to start/ stop/ check the status of multiple subsystem agents, do the following:

- To START: Resiliency OrchestrationAgentsStart.sh

This can be used to start multiple agents as specified by options. The options and arguments are described in the table below. This is primarily used during the patch process. This command starts agents that are currently not running and the user has not specifically stopped it (The user has stopped the agent from GUI).

Resiliency OrchestrationAgentsStart.sh <option1> [option2 option3 ...]

Example: > Resiliency OrchestrationAgentsStart.sh WINDOWSOS LINUXOS

- To STOP: Resiliency OrchestrationAgentsStop.sh

This can be used to stop multiple agents (remote agents) as specified by options. This is primarily used during the patch process.
Resiliency OrchestrationAgentsStop.sh <option1> [option2 option3 ...]

Example: > Resiliency OrchestrationAgentsStop.sh WINDOWSOS LINUXOS

- To Check the Status: Resiliency OrchestrationAgentsStatus.sh

Users can use this to see the current status of agents according to the options specified.

Resiliency OrchestrationAgentsStatus.sh <option1> [option2 option3 ...]

Example :> Resiliency OrchestrationAgentsStatus.sh WINDOWSOS LINUXOS

The "options" arguments can be one or many. The full list of options is listed in the table.

Resiliency Orchestration Agents option argument	Description
WINDOWSOS	All Windows OS.
LINUXOS	All Linux OS agents.
AIXOS	All AIX OS agents.
HPUXOS	All HPUX OS agents.
SOLARISOS	All Solaris OS agents.
OSAGENTS	All OS agents.
ORACLE	All Oracle dataset agents.
MSSQL	All MSSQL dataset agents.

Resiliency Orchestration Agents option argument	Description
DATASETAGENTS	All dataset agents.
PFR	All PFR protection agents.
TRUECOPY	All TrueCopyprotection agents.
DATAGUARD	All Data Guard protection agents.
HPXP	All HPXP protection agents.
PROTECTIONAGENTS	All protection agents.
NETAPPONTAPOS	All NetAppOnTAP OS agents.
PostgreSQL	All PostgreSQL dataset agents.
MSExch	All MS Exchange dataset agents.
ALL	All OS agents, All dataset agents, All protection agents, and ALL Management Service Agents.
NETAPP	All NetApp protection agents.
SybaseASE -	All Sybase dataset agents.
DATASETAGENTS	All dataset agents.
SRDF	All EMC SRDF protection agents.
UCSD	All UCSD Mgmt Service agents.
AWS	All AWS Mgmt Service agents.
VCENTER	All VCENTER Mgmt Service agents.
MANAGEMENTSERVICEAGENTS	ALL Management Service Agents.

Note

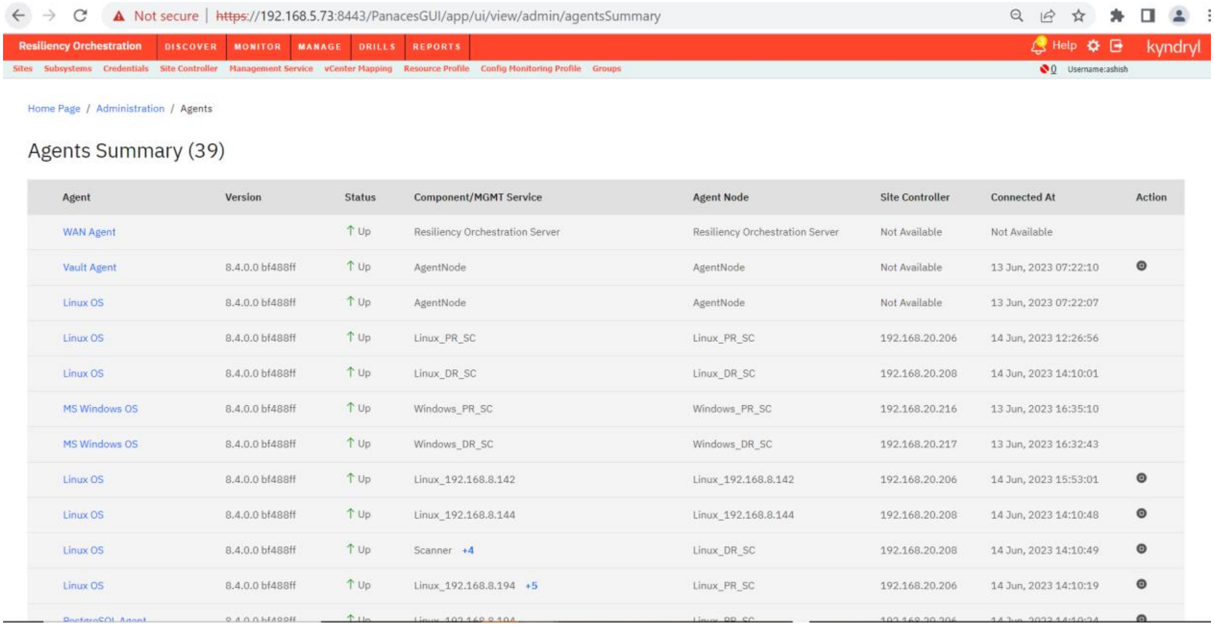
1. For incorrect inputs or if no inputs are provided for the script, then the exit status is 1, or else it is 0.
2. If an agent is started by a script, then it displays "AGENT_TYPE agent started successfully for IP: IP_ADDRESS".
3. If an agent is already running, then it displays "AGENT_TYPE agent is already running for IP: IP_ADDRESS".
4. If an agent fails to start, then it displays "AGENT_TYPE agent could not be started for IP: IP_ADDRESS".
5. If there are no remote agents found for a given agent type, it will display "No AGENT_TYPE agents found".
6. The script will take a valid input only once, even if the same input is given more than once.

Migration

Remote Agent Migration Tool (MigrateRemoteAgentCLI.sh**):**

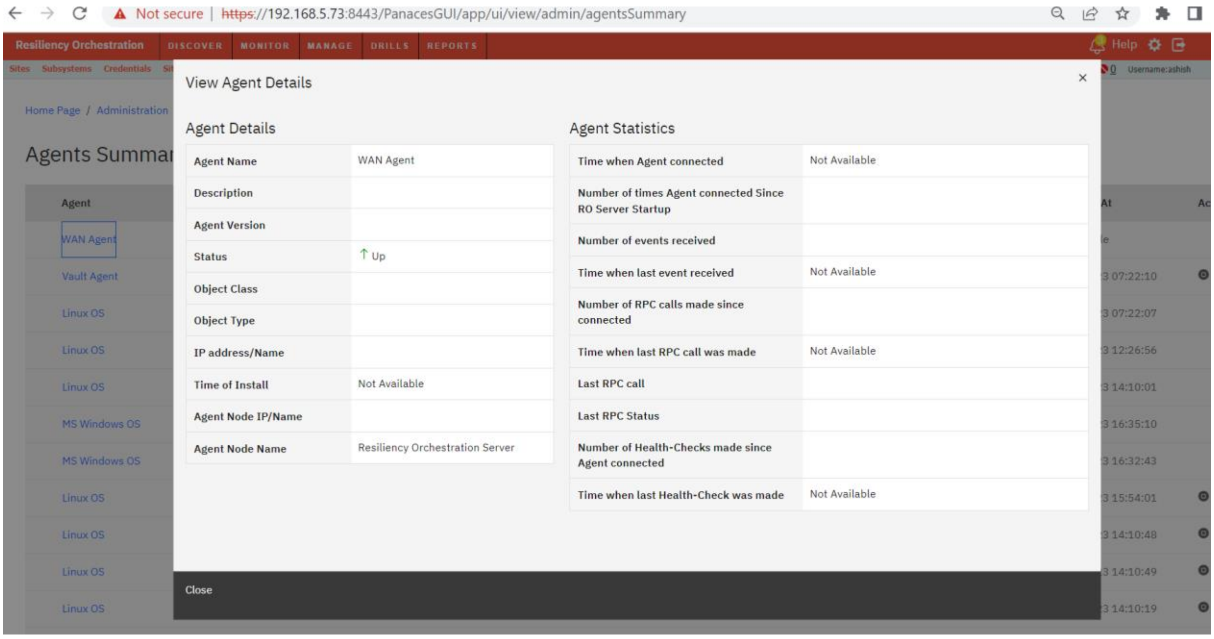
All or a subset of agents mapped to run on one site controller can be migrated to another site controller using the remote agent migration tool. The agents that are running on the agent node can be migrated to the Site controller. The agents to be migrated are specified in MigrateRemoteAgents.json.

Note: Supported through AD2C, the edit is not supported in UI.



Agents Summary (39)

Agent	Version	Status	Component/MGMT Service	Agent Node	Site Controller	Connected At	Action
WAN Agent		↑ Up	Resiliency Orchestration Server	Resiliency Orchestration Server	Not Available	Not Available	
Vault Agent	8.4.0.0 bf488ff	↑ Up	AgentNode	AgentNode	Not Available	13 Jun, 2023 07:22:10	⚙
Linux OS	8.4.0.0 bf488ff	↑ Up	AgentNode	AgentNode	Not Available	13 Jun, 2023 07:22:07	
Linux OS	8.4.0.0 bf488ff	↑ Up	Linux_PR_SC	Linux_PR_SC	192.168.20.206	14 Jun, 2023 12:26:56	
Linux OS	8.4.0.0 bf488ff	↑ Up	Linux_DR_SC	Linux_DR_SC	192.168.20.208	14 Jun, 2023 14:10:01	
MS Windows OS	8.4.0.0 bf488ff	↑ Up	Windows_PR_SC	Windows_PR_SC	192.168.20.216	13 Jun, 2023 16:35:10	
MS Windows OS	8.4.0.0 bf488ff	↑ Up	Windows_DR_SC	Windows_DR_SC	192.168.20.217	13 Jun, 2023 16:32:43	
Linux OS	8.4.0.0 bf488ff	↑ Up	Linux_192.168.8.142	Linux_192.168.8.142	192.168.20.206	14 Jun, 2023 15:53:01	⚙
Linux OS	8.4.0.0 bf488ff	↑ Up	Linux_192.168.8.144	Linux_192.168.8.144	192.168.20.208	14 Jun, 2023 14:10:48	⚙
Linux OS	8.4.0.0 bf488ff	↑ Up	Scanner +4	Linux_DR_SC	192.168.20.208	14 Jun, 2023 14:10:49	⚙
Linux OS	8.4.0.0 bf488ff	↑ Up	Linux_192.168.8.194 +5	Linux_PR_SC	192.168.20.206	14 Jun, 2023 14:10:19	⚙



View Agent Details

Agent Details

Agent Name	WAN Agent
Description	
Agent Version	
Status	↑ Up
Object Class	
Object Type	
IP address/Name	
Time of Install	Not Available
Agent Node IP/Name	
Agent Node Name	Resiliency Orchestration Server

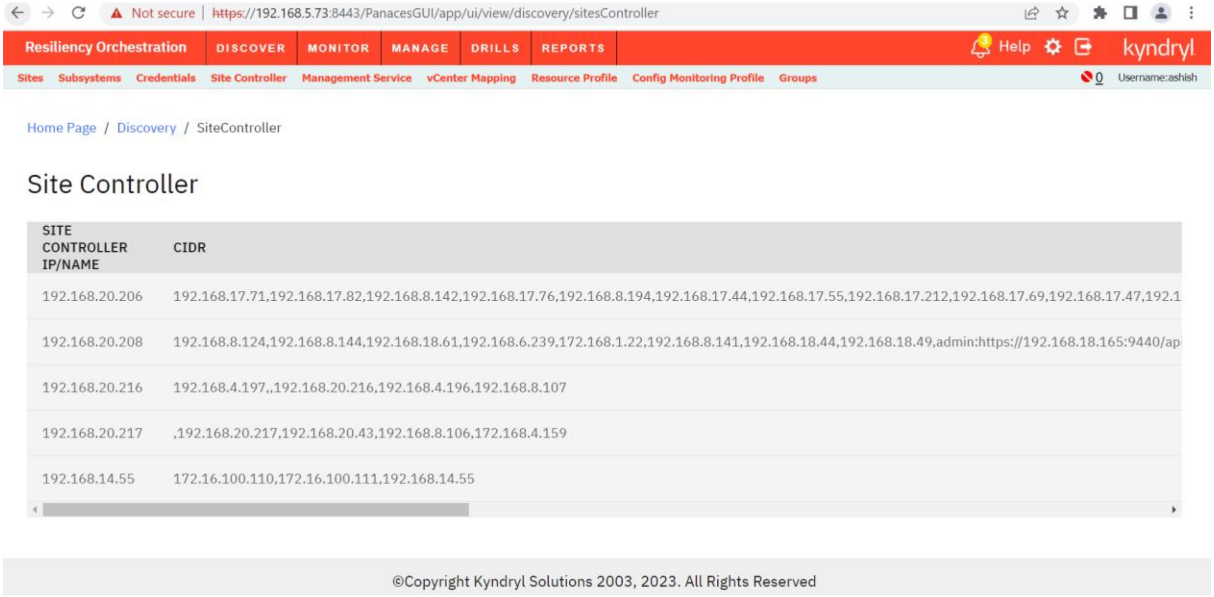
Agent Statistics

Time when Agent connected	Not Available
Number of times Agent connected Since RO Server Startup	
Number of events received	
Time when last event received	Not Available
Number of RPC calls made since connected	
Time when last RPC call was made	Not Available
Last RPC call	
Last RPC Status	
Number of Health-Checks made since Agent connected	
Time when last Health-Check was made	Not Available

Case 1: Migration from Agent node to Site Controller:

- Add the agents to target site controller mapping.
- For example: Let us say, you want to migrate remote agents 192.168.20.129 and 192.168.20.137 from source SC 192.168.20.212 to target SC 192.168.20.210.

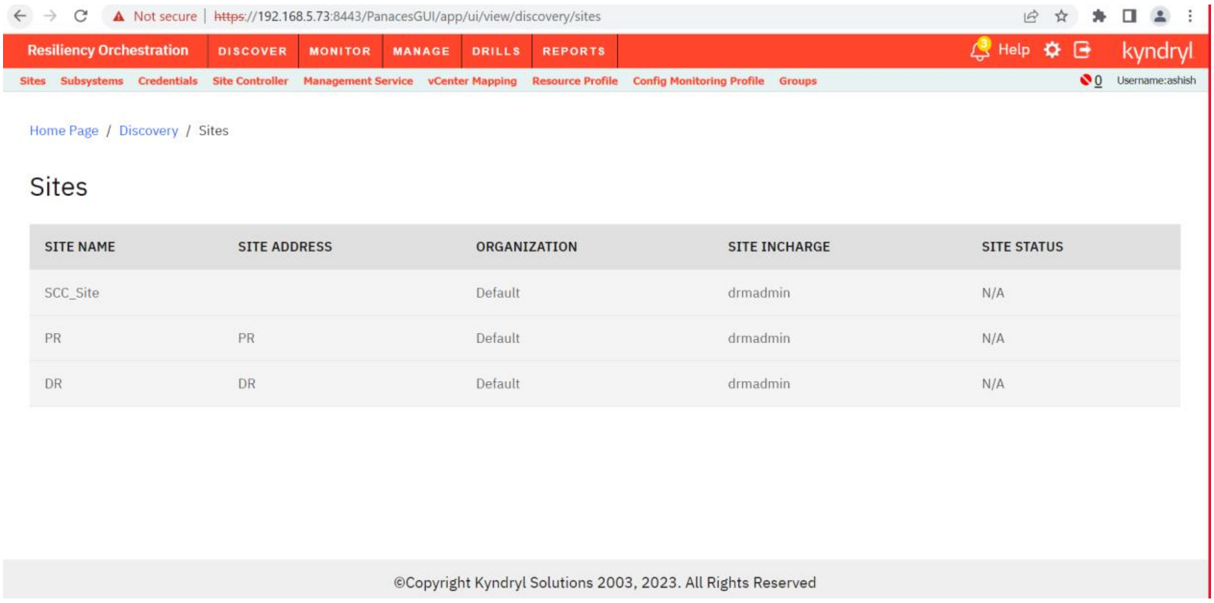
(SC mapping before Edit)



Site Controller

SITE CONTROLLER IP/NAME	CIDR
192.168.20.206	192.168.17.71,192.168.17.82,192.168.8.142,192.168.17.76,192.168.8.194,192.168.17.44,192.168.17.55,192.168.17.212,192.168.17.69,192.168.17.47,192.1
192.168.20.208	192.168.8.124,192.168.8.144,192.168.18.61,192.168.6.239,172.168.1.22,192.168.8.141,192.168.18.44,192.168.18.49,admin:https://192.168.18.165:9440/ap
192.168.20.216	192.168.4.197,,192.168.20.216,192.168.4.196,192.168.8.107
192.168.20.217	,192.168.20.217,192.168.20.43,192.168.8.106,172.168.4.159
192.168.14.55	172.16.100.110,172.16.100.111,192.168.14.55

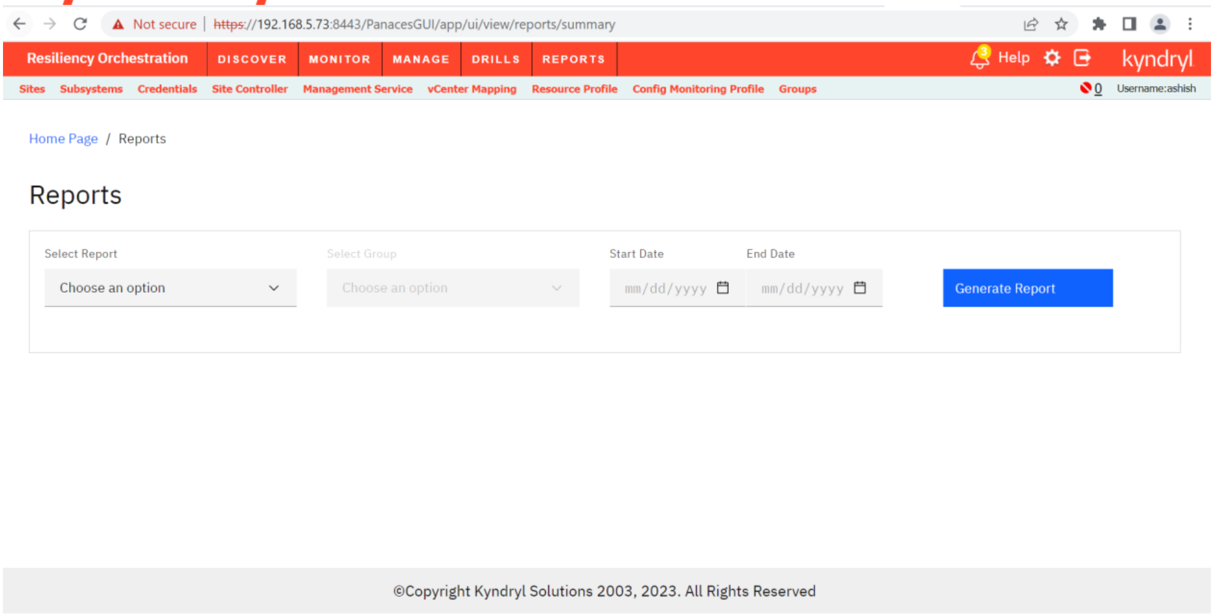
©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

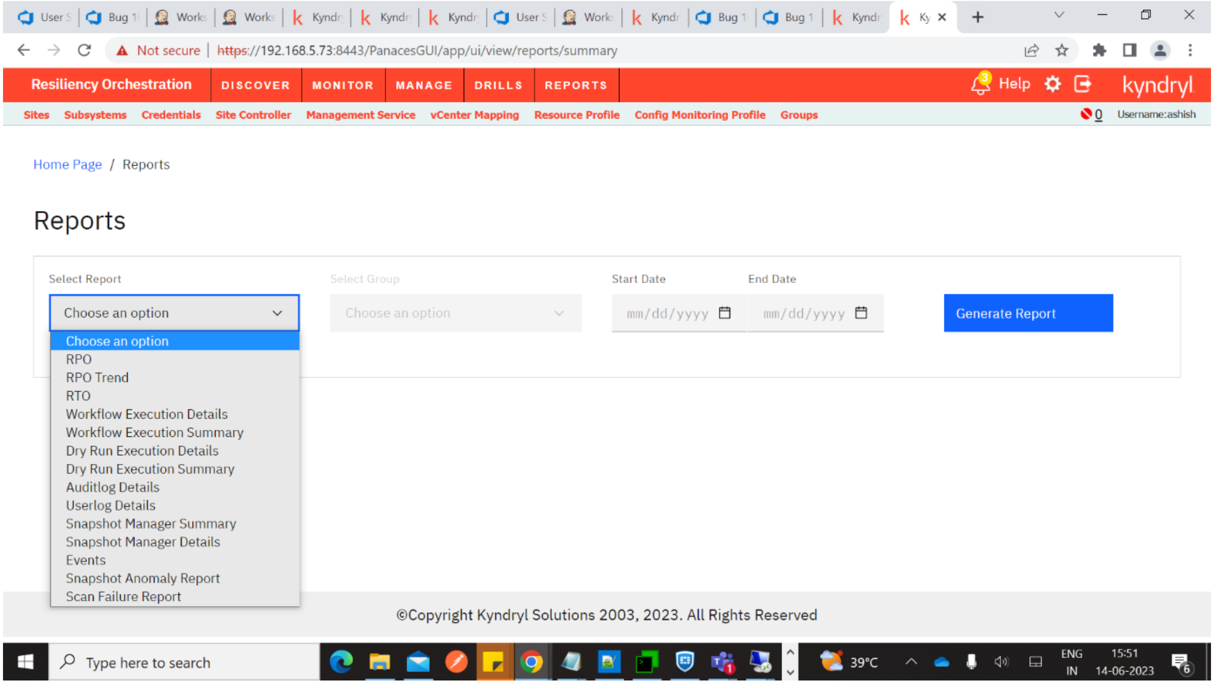


Sites

SITE NAME	SITE ADDRESS	ORGANIZATION	SITE INCHARGE	SITE STATUS
SCC_Site		Default	drmadmin	N/A
PR	PR	Default	drmadmin	N/A
DR	DR	Default	drmadmin	N/A

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved





The following steps in the given sequence must be executed to migrate the agents.

Step 1:

a. Ensure the Target Site Controller’s Local Agent and Site Controller are running.
b. Ensure remote agents to be migrated are in connected status and the subsystems are in an Active state.
c. Edit EAMSROOT/installconfig/MigrateRemoteAgents.json to provide the below information for the migration:
    1. Endpoints that are to be migrated

2. Source site controller
3. Target site controller

For example:

```
{

"endpointList":"192.168.1.1,192.168.1.2,esx018.iclou
d.kyndryl.local,192.168.1.0/24",
"sourceSC":"192.168.0.1",
"targetSC":"192.168.0.2"

/*
Note:
sourceSC -> Specify AgentNode/Site controller
endpointList -> Specify endpoint IP
address/FQDN/CIDR range
targetSC -> Specify the target Site controller where
all the agents need to move.
*/

}
```

d. Run EAMSROOT/bin/MigrateRemoteAgentCLI.sh
e. On the Migration prompt, execute command startphase1 as below-
Migration $startphase1
f. When prompted; enter yes to continue and wait for the command to finish.
g. This script is supported for Migrating NetApp Agents from Agent node to SiteController"

Step 2

Edit Site Controller mapping

Case 1: In the Site Controller page, remove the agents to be migrated from the source Site Controller and:

- Add them to target site controller mapping.
- Wait until both source and target site controllers come to the CONNECTED state.

Case 2: Migration from Agent node to Site Controller:

- Add the agents to target site controller mapping.
- For example: Let us say, you want to migrate remote agents 192.168.20.129 and 192.168.20.137 from source SC 192.168.20.212 to target SC 192.168.20.210.

(SC mapping before Edit)

Agent Listing

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the configured agents, perform the following steps:

1. Click **Admin** on the navigation bar. The **Kyndryl Resiliency Orchestration Administration** page appears.
2. Click on **Agents Summary**. The Agents page appears.

Field	**Description**
AGENT	Lists the agent's name.
VERSION	Displays the version of the agent when the agent is connected. If the agent version is not available or the agent is not connected, then "-" will be shown.
STATUS	Displays the agent's status. The various status is: ▪ **CONNECTED** – The agent is connected to the server. ▪ **NOT CONNECTED** – Connection to the server does not exist due to some failure. ▪ **CONNECTING** / **NOT CONNECTING** - The process of establishing a connection or disconnecting with the server during establishing a connection. **Note**: Only if the server is remotely managed, the **Start/Stop** option will be displayed.
COMPONENT/MGMT SERVICE	Displays the server machine on which the agent is installed.
AGENT NODE	Displays the name of the agent node server, from where the agent is running, only if the server is remotely managed.
SITE CONTROLLER	Displays the Site Controller
CONNECTED AT	Displays the time when the agent last connected to the Kyndryl Resiliency Orchestration server.
ACTION	Displays the Start/Stop action of the agent

The agent can be installed on more than one server machine. Click the respective Agent link to view agent details and statistics. In the right pane, you can view the **Event Polling Interval** in seconds, configured for the respective agents.

The **Agent Details** page displays the following:

Agent Details	
Agent Name	Displays the Agent's name.

Agent Details	
Description	Displays the description of the Agent.
Agent Version	Displays the version of the agent when the agent is connected. If the agent version is not available or the agent is not connected, then "-" will be shown.
Status	Displays the current status of the Agent.
Object Class	Displays whether the agent is related to a Component, Dataset, or Protection Scheme.
Object Type	Displays the type of object that is being managed by the respective agent. For example, if the Object class is 'Component', then this specifies whether the Components is of type 'NT Server' or 'Solaris Server', etc.
IP Address/Name	Displays the IP address or Name (hostname or FQDN) of the server on which the agent is installed.
Time of Install	Displays the time of installation of the Agent on the server.
Agent Node IP/Name	Displays the IP address or Name of the Agent Node.
Agent Node Name	Displays the Name of the Agent Node.
Agent Statistics	
Time when Agent connected	Displays the time at which the agents were connected to the Kyndryl Resiliency Orchestration server (put the def of Time when the connection was established after getting the confirmation from GUI).
Number of times Agent connected Since RO Server Startup	Displays the number of times the agent was connected to the Kyndryl Resiliency Orchestration ™ server since the server is active.
Number of events received	Displays the number of events received.
Time when last event received	Displays the time of the last received event.
Number of RPC calls made since connected	Displays the number of RPC (Remote Procedure calls) made since connected to the Kyndryl Resiliency Orchestration ™ server.
Time when last RPC call was made	Displays the time of the last RPC call.

Agent Details	
Last RPC call	Displays the name of the last RPC call.
Last RPC status	Displays the status of the last RPC call.
Number of Health- Checks made since Agent Connected.	Displays the number of health checks made since the agent is connected.
Time when last Health check was made	Displays the time of the last health check.

You can modify the configured agent by clicking the 📝 icon.

Handling Agent Plugins

Registering Plugins

To register plugins for the subsystem and management system as well as solution discovery using the RPD framework, perform the following steps.

Steps

1. For the subsystem and management service discovery,
   a. Navigate to location $EAMSROOT/bin/.
   b. Execute registerRPDPlugin.sh –r <plugin path>.
2. For solution discovery,
   a. Navigate to location $EAMSROOT/bin/
   b. Execute registerRPDSolutionPlugin.sh –r <solution plugin path>.

Updating Plugins

To update plugins for the subsystem and management system as well as solution discovery using the RPD framework, perform the following steps.

Prerequisite

Ensure that the plugin version to be installed is higher than the currently installed plugin version.

Note:

- For subsystem and management services, existing RALs and events are not affected during the update. However, new RALs and Events will be added.
- Discovery UI will be updated.
- For Solution discovery, the workflows will be updated.

Steps

1. For the subsystem and management service discovery,
   a. Navigate to location $EAMSROOT/bin/.
   b. Execute registerRPDPlugin.sh –u <absolute plugin path>.
2. For solution discovery,
   a. Navigate to location $EAMSROOT/bin/
   b. Execute registerRPDSolutionPlugin.sh –u <absolute solution plugin path>.

Adding RALs

In case the solution uses the RPD framework, please follow the below steps to register the RALs.

Steps

1. Create a plugin having Plugin.xml, Command.xml, event.xml, and ral.xml files.
2. Use registerRPDPlugin.sh with option '-r' and supply the zip file to add the plugin.

Adding Events

In case the solution uses the RPD framework, please follow the below steps to register the events.

Steps

1. Create a plugin having Plugin, Command, and event XML.

2. Use registerRPDPlugin.sh with option '-r' and supply the zip file to add the plugin.

Note: When creating an event, you need to collect the name of the monitoring entity during discovery.

Registering Plugin for Optional Type Attribute

This topic covers the registration of subsystem plugins to add a 'type' attribute. The 'type' attribute accepts alphanumeric characters with a maximum allowed length of 50.

A new property file is introduced to validate the mandatory RAL names that must be

defined within RAL.xml. The property file can be found on the Kyndryl Resiliency Orchestration server at $EAMSROOT/rpd/config/PluginSupportedRals.properties. The following entry is available by default:

copyDataManager=GetBackupData,ExecuteMountOnESX

1. Define the Type attribute in the plugin.xml file.

Example:

```
<Plugin name="<plugin_name>" description="<plugin description>"
version="2.0" objClass="MANAGEMENT_SERVICE"
        objType="<plugin name>"
```

type="<plugin_type>" />

2. In case you need to make the RAL(s) mandatory, then update the PluginSupportedRals.properties file with the above plugin type as a key.

Example:

```
<plugin_name> = <RAL Name1>, <RAL Name 2>, <RAL Name 3>, …..<RAL
Name N>
```

Note:

- You will need to fill in the RAL name in the above example excluding the plugin name prefix such as <plugin name>_<RAL name>.
- Ensure that the RAL ID defined in RAL.xml conforms to the following specification.

  Example: <RAL id> ="<plugin_name_abc>"

Organization Configuration

A single instance of Resiliency Orchestration Server can support one Organization or multiple Organizations.

Organization

An Organization is a distinct set of users who own a set of resources and work together to achieve a common purpose. The words Tenant or Organization are used interchangeably in this document, and they mean the same.

Single Organization Support

Resiliency Orchestration defaults to Single Organization mode which is termed as "Default" Organization. If you intend to support only one Organization or Tenant, you can skip the rest of this section.

Multiple Organization Configuration

Resiliency Orchestration provides fine-grained Role Based Access Control (RBAC) and strict access control to allow only authorized Users to perform actions on Organization data.

Resiliency Orchestration supports this use case in general and is specifically certified for DRaaS using Zerto vCD.

Service Provider Role

The Service Provider manages DR infrastructure for multiple Organizations and does the administrative tasks for Organizations. Service Provider discovers the Recovery Groups and Application groups and manages their life cycle on behalf of the Organizations.

Organization Role

Organizations under the Service Provider monitor RPO/RTO and other SLA adherence and can perform DR Drills as required.

Multitenancy Integrated with AD

Prerequisites

These are the prerequisite steps for configuring multiple organizations using AD Authentication in the RO Server –

Multiple Organization Configuration is supported with AD and Basic Authentication Modes (Non-AD).

1. As a first step though, Resiliency Orchestration should be installed using basic authentication mode before switching to the AD-based authentication for handling multiple organizations.

Note: For installing RO in basic authentication mode, refer to the Kyndryl Resiliency Orchestration Installation guide.

2. After you have successfully installed Resiliency Orchestration, log in once using drmadmin user and then follow the below steps for switching to AD-based multiple organization.

Note: Once RO is configured for multiple organizations, you cannot switch back to basic authentication mode.

3. After ensuring RO-AD Server connectivity, Import the AD Certificates. Refer to the section **Importing CA Certificate to Kyndryl Resiliency Orchestration Server**.

Define Appropriate Roles

Before configuring the AD servers, ensure you have performed the following steps:

You must create necessary custom roles to support Multiple Organizations. This can be achieved by importing role schema. Manual role creation is not necessary.

Import customroles.sql located at $EAMSROOT/lib/customroles.sql using command –

```
mysql -u<username> -p<password> < customroles.sql
```

The above file will create 4 custom roles in Resiliency Orchestration and the necessary privileges for each role.

- **SPAdmin** – Role for service provider admin. This role is given create and modification privileges in different modules like Discovery, Monitor, Manage, Reports, and Admin sections
- **SPOperator** – Role for Service Provider operator. This role is given only view privilege.
- **TenantAdmin** – Role for Tenant admin. This role is given view, execute, and approve workflow privileges in different modules like the Discovery, Monitor, Manage, and Reports sections.
- **TenantOperator** – Role for Tenant operator. This role is given only view privilege in different modules.

Note: The Service Provider decides the RBAC privileges to be provided for each user/role.

Multi-tenancy Roles and Permissions

The following are the Multi-tenancy roles and permissions.

Note: The Multi-tenancy roles and permissions are applicable for Non-AD Authentication mode as well.

Page	Fields	SPAdmin	SPOperator	TenantAdmin	TenantOperator
User	Create, Edit, Delete	Y	N	N	N
	View	Y	Y	Org Tenant users	Self only

Page	Fields	SPAdmin	SPOperator	TenantAdmin	TenantOperator
	(Create/Edit user) Organization & Role Dropdown	Hierarchy org, Org Relevant roles	N	N	N
	(Create/Edit user) Assign Groups Multiselect	All groups are relevant to the selected org.	N	N	N
	Edit Full Name	Edit Full Name	Self only	Self only	Self only
	Edit Email id	Y	Self Only	Self Only	Self Only
	Enable/Disable User Login	Y	N	Y	N
vCenter Mapping	Cluster Mapping (Create, Delete)	Y	N	N	N
	Port Group Mapping (Create, Delete)	Y	N	N	N
	Placeholder Datastore (Create, Delete)	Y	N	N	N
	Cluster Mapping (view)	Y	Y	N	N
	ESX (View)	Y	Y	N	N
	resourcePool	Y	Y	N	N
Sites	Create, Edit, Delete	Y	N	N	N
	View	Y	Y	Y	Y
Subsystems	Create, Edit, Delete	Y	N	N	N
	View	Y	Y	Y	Y
Credentials	Create, Edit, Delete	Y	N	N	N
	View	Y	Y	N	N
Site Controller	Create, Edit, Delete	Y	N	N	N
	View	Y	Y	Y	Y
Management Service	Create, Edit, Delete	Y	N	N	N
	View	Y	Y	Y	Y
Groups	Create, Edit, Delete	Y	N	N	N
	View	Y	Y	Y	Y
Monitor	Sites	Y	Y	Y	Y

Page	Fields	SPAdmin	SPOperator	TenantAdmin	TenantOperator
	Application Groups (View)	Y	Y	Y	Y
	Application Groups (Pending Data Refresh button)	Y	N	N	N
	Recovery Groups (View)	Y	Y	Y	Y
	Recovery Groups (Pending Data Refresh button)	Y	N	N	N
	Recovery Groups (Validation Rules)	Y	Y	N	N
	Recovery Groups (Config Exposures -> Scan Now button)	Y	N	N	N
Manage	Sites	Y	Y	Y	Y
	Application Groups (View)	Y	Y	Y	Y
	Application Groups (Pending Data Refresh button)	Y	N	N	N
	Application Groups (WF->Edit, Create, Publish)	Y	N	N	N
	Application Groups (Dry Run Execute)	Y	Y	Y	Y
	Application Groups (WF Execute)	Y	N	Y	N
	Application Groups (WF Approver)	Y	N	Y	N
	Recovery Groups (View)	Y	Y	Y	Y
	Recovery Groups (Pending Data Refresh button)	Y	N	N	N

Page	Fields	SPAdmin	SPOperator	TenantAdmin	TenantOperator
	Recovery Groups (Validation Rules-> View)	Y	Y	N	N
	Recovery Groups (Validation Rules-> Execute, Customize)	Y	N	N	N
	Recovery Groups (Dry Run Execute)	Y	Y	Y	Y
	Recovery Groups (WF Execute)	Y	N	Y	N
	Recovery Group (WF Approver)	Y	N	Y	N
Drills	Summary (View, Dry Run)	Y	Y	Y	Y
	Summary (Edit, Create, Publish, Schedule)	Y	N	N	N
	Summary (Execute)	Y	N	Y	N
	Scheduled (view, Dry Run)	Y	Y	Y	Y
	Scheduled (Edit, Create, Publish, Schedule)	Y	N	N	N
	Scheduled (Execute)	Y	N	Y	N
Reports	Reports Across All Groups	Y	Y	Y	Y
	Compliance Reports	Y	Y	Y	Y
	Custom Reports	Y	Y	N	N
	Common Reports	Y	Y	N	N
	Snapshot Manager Report (View)	Y	Y	Y	Y
	Snapshot Manager Report (Edit schedule, Edit Email	Y	N	N	N

Page	Fields	SPAdmin	SPOperator	TenantAdmin	TenantOperator
	Recipients, Mail report)				
	Reports Per Group	Y	Y	Y	Y
Go To Role Management	View	Y	Y	N	N
	Edit, Add custom role	Y	N	N	N
Go To Organizations	View	Y	Y	N	N
Go To Notification	Email Server (View)	Y	Y	N	N
	Email Server (Add, Edit)	Y	N	N	N
	Notification List (View)	Y	Y	Y	Y
	Notification List (Add, Edit, Delete)	Y	N	Y	N
	SNMP Trap Forwarder (View)	Y	Y	N	N
	SNMP Trap Forwarder (Add, Edit, Delete)	Y	N	N	N
Go To Agents	View	Y	Y	N	N
	Start/Stop	Y	N	N	N
Go To Agent Upgrade	View	Y	Y	N	N
	Upgrade	Y	N	N	N
Go To Logs	Debug Level (View)	Y	Y	N	N
	Debug Level (Edit)	Y	N	N	N
	Fetch Log (View)	Y	Y	N	N
	Fetch Log (Fetch)	Y	N	N	N
	System Capture (View)	Y	Y	N	N
	System Capture (Fetch)	Y	N	N	N
Go To Backup	View Backup	Y	Y	N	N
	Configure/Delete/Start Backup	Y	N	N	N

Page	Fields	SPAdmin	SPOperator	TenantAdmin	TenantOperator
Go To Server Failover	Failover Configuration (View)	Y	Y	N	N
	Failover Configuration (Add, Edit)	Y	N	N	N
	Status (View)	Y	Y	N	N
GoTo System Events	View, Edit	Y	N	N	N
Go To Group Labels	View	Y	Y	N	N
	Edit	Y	N	N	N
Go To License	View, Print	Y	Y	N	N
Go to Operational History	View	Y	Y	N	N
	Save Config, Purge Log	Y	N	N	N
Go to Site Ticker	View	Y	Y	N	N
	Add, Update, Delete	Y	N	N	N
Go to Global Console	View	Y	Y	N	N
	Add, Delete	Y	N	N	N
Events	View	Y	Y	Y	Y
	Show SOE	Y	Y	Y	Y
	Execute Policy	Y	N	Y	N
	Change State	Y	N	N	N
	Event Details-> Comment -> edit	Y	N	N	N

Configuring AD for Service Providers and Organizations

Actor	Action	Sub-Actions
RO Super Administrator	Onboard Service Provider (SP)	1. Add SP 2. Add AD settings for SP 3. Identify SP Users 4. Create Groups 5. Map AD Role to RO Role for SP Users

SP Administrator	Onboard Organizations	1. Add Organizations 2. Add AD settings per Organization 3. Identify/Register users per Organization for login 4. Map AD Role to RO Role per Organization
SP Administrator	Manage Access	1. Allow SP users to manage the Organization

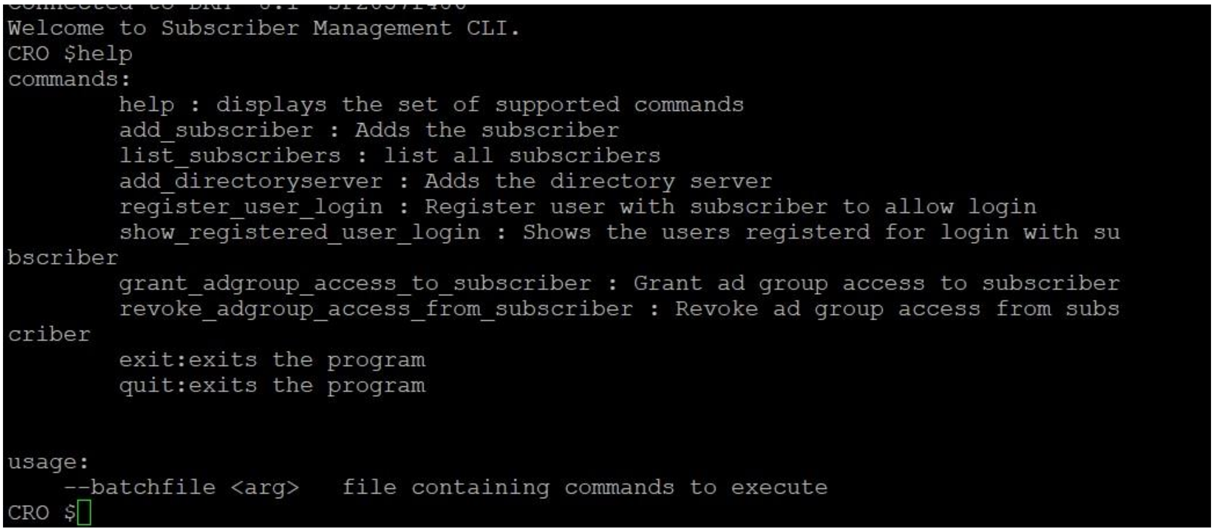
Manage Organizations

Accessing the CLI

Ensure you perform the following CLI-based configuration steps in the RO Server location:

/opt/panaces/bin/SubscriberManager.sh

At the prompt ***CRO $***, type help. The usage help for the CLI is listed as shown in the screenshot below.



```
Welcome to Subscriber Management CLI.
CRO $help
commands:
        help : displays the set of supported commands
        add_subscriber : Adds the subscriber
        list_subscribers : list all subscribers
        add_directoryserver : Adds the directory server
        register_user_login : Register user with subscriber to allow login
        show_registered_user_login : Shows the users registerd for login with su
bscriber
        grant_adgroup_access_to_subscriber : Grant ad group access to subscriber
        revoke_adgroup_access_from_subscriber : Revoke ad group access from subs
criber
        exit:exits the program
        quit:exits the program


usage:
    --batchfile <arg>   file containing commands to execute
CRO $
```

Add Organization

1. To add the service provider or other tenants as an organization, use the CLI command: ***add_subscriber***
   Refer to the section **Accessing the CLI** for the procedure to access the command line tool.
2. Enter the organization's unique name: For example: *MyServiceProvider*
3. Enter the description: For example: *My Service Provider*
4. Enter the subscriber, key in 0 or 1.

   - 0 for Service Provider

- 1 for Subscriber

Key in 0 for adding a service provider. The service provider *MyServiceProvider* is successfully added.

Add Directory Server

It is a prerequisite that AD servers are reachable from the RO server.

Make sure the **prerequisite** steps to configure the AD Server are performed before executing the below command.

1. To add a directory server, use the CLI command: ***add_directoryserver***
2. Enter the directory server's unique name: for example, *MyServiceProvider_AD*
3. Enter the directory server display name: For example, *MyServiceProvider_AD*
4. Enter the directory server URL: For example: *ldap://<AD Server URL>:<port>*
5. Enter the directory server domain: For example, *bdi.com*
6. Enter the directory server searchbase: For example, *dc=bdi, dc=com*
7. Enter the directory server username: For example: *qaadmin*
8. Enter the directory server password: For example: *Enter the password*
9. Enter the subscriber ID for which you want to associate this directory server: For example, *MyServiceProvider*
   The directory server is successfully added for Organization *MyServiceProvider*.

   Repeat the procedure to add a directory server for each organization.

Identify Users per Organization

To Identify/Register users per Organization for login purposes, follow the below steps.

1. You can add single or multiple users using the command: ***register_user_login***

2. The following message appears, Add more user? Y/N

   - select Y to add more users to the same subscriber.
   - select N to add a single user to the same subscriber.

Repeat and add all required users to Service Provider and Tenant organizations. This is a mandatory step, and it is only to register the users with RO.

Show Registered Users

To see the list of registered users of an Organization, use the CLI command: ***show_registered_user_login***

This command displays the users who are registered to log in with the Organization.

Provide AD Group access to Organizations

SP users need to be able to access tenant organization data. This is done on the AD group level. Access is provided to the AD group, and all users belonging to the AD group can access data of the organization that they have been allowed access to.

To provide access to subscribers use the CLI command:
grant_adgroup_access_to_subscriber

Ensure you perform this step to allow access to each of the tenant organizations for the AD Group that the SP belongs to.

Revoke AD Group access from the Organization

Use the CLI command ***revoke_adgroup_access_from_subscriber*** to revoke AD group access from the organization.

Add AD Group(s) per AD server/ Organizations

To configure AD Servers in RO, refer section the **External Directory Server Details in Kyndryl Resiliency Orchestration**.

To add an AD Group per AD Server/ Organization, refer section **Allowlisting AD Groups**.

Note:

- Each AD Group should be mapped to one Organization.

Delete Organisations

The delete Organization is not supported in the current release.

Manage Users

User login can be enabled or disabled by another user with appropriate privileges. When disabled, the user will not be allowed to log into the Resiliency Orchestration portal.

Enable Users

There is a new option Enable Users in the RBAC. This is to enable users within your tenant users. Refer to **Enabling Disabling Users** in the User Management section. If the logged-in user has the privilege, then they can enable/disable other users of their organization.

Disable Users

There is a new option Disable Users in the RBAC. This is to disable users within your tenant users. Refer to **Enabling Disabling Users** in the User Management section. If the logged-in user has the privilege, then they can enable/disable other users of their organization.

Multitenancy Integrated with RO/Basic Authentication Mode (Non-AD)

Prerequisites

These are the prerequisite steps for configuring multiple organizations using Basic Authentication in RO Server -

1. First, Resiliency Orchestration should be installed using a basic authentication mode for handling multiple organizations.

Note: For installing RO in basic authentication mode, refer to the *Resiliency Orchestration Installation guide*.

2. After you have successfully installed Resiliency Orchestration, start the panaces server and define the user roles as shown below.

Define Appropriate Roles

Before configuring the basic authentication mode servers, ensure you have performed the following steps:

You must create necessary custom roles to support Multiple Organizations. This can be achieved by importing role schema. Manual role creation is not necessary.

Import customroles.sql located at $EAMSROOT/lib/customroles.sql using command –

```
mysql -u<username> -p<password> < customroles.sql
```

The above file will create 4 custom roles for Basic Authentication mode in Resiliency Orchestration and the necessary privileges for each role.

- **SPAdmin** – Role for service provider admin. This role is given create and modification privileges in different modules like Discovery, Monitor, Manage, Reports, and Admin sections and CRUD operation on the user.
- **SPOperator** – Role for Service Provider operator. This role is given only view privilege.
- **TenantAdmin** – Role for Tenant admin. This role is given to view, execute, and approve workflow privileges in different modules like Discovery, Monitor, Manage, and Reports sections.
- **TenantOperator** – Role for Tenant operator. This role is given only view privilege in different modules.

Note:

- The Service Provider decides the RBAC privileges to be provided for each user/role.
- For creating any custom roles for service providers, the role name must contain "SPAdmin" or "SPOperator" strings. For creating any custom roles for Tenant, the role name must contain "TenantAdmin" or "TenantOperator" strings.

Multi-tenancy Roles and Permissions

For more information on the Multi-tenancy roles and permissions, refer to the section "**Organization Configuration**".

Configuring Basic Authentication Mode for Service Providers and Organizations

Actor	Action	Sub-Actions
RO Super Administrator	Onboard Service Provider (SP)	1. Add SP
SP Administrator	Onboard Organizations	1. Accessing the CLI 2. Add Organizations 3. Create Users for Organizations using GUI

		4. Discover and map the RGs/AGs to the respective Organizations 5. Assign Groups to Users of respective Organizations 6. Manage Users

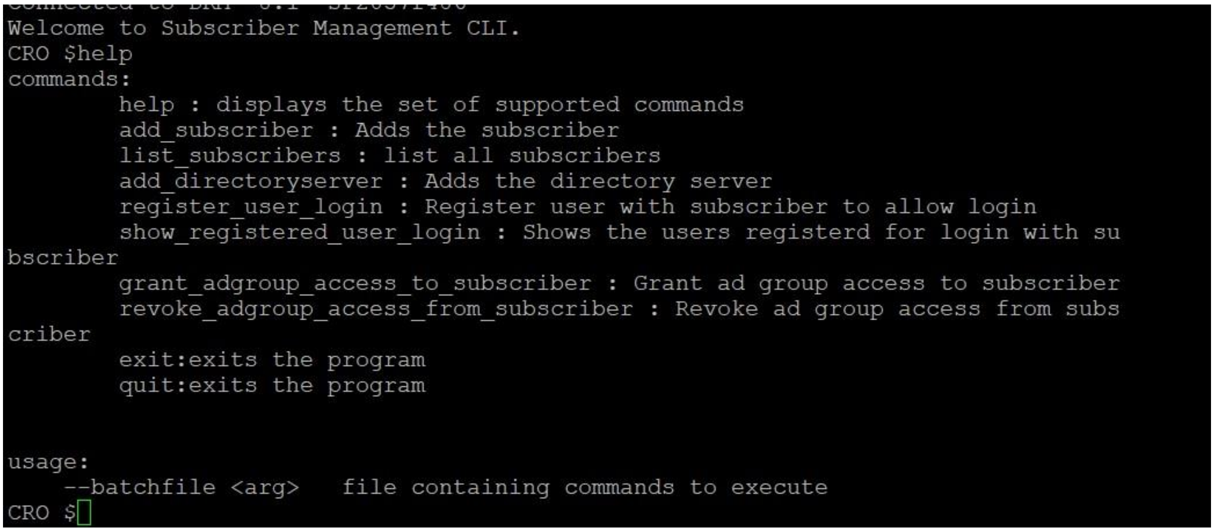
Manage Organizations

Accessing the CLI

Ensure you perform the following CLI-based configuration steps in the RO Server location:

/opt/panaces/bin/SubscriberManager.sh

At the prompt ***CRO $***, type help. The usage help for the CLI is listed as shown in the screenshot below.



```
Welcome to Subscriber Management CLI.
CRO $help
commands:
        help : displays the set of supported commands
        add_subscriber : Adds the subscriber
        list_subscribers : list all subscribers
        add_directoryserver : Adds the directory server
        register_user_login : Register user with subscriber to allow login
        show_registered_user_login : Shows the users registerd for login with su
bscriber
        grant_adgroup_access_to_subscriber : Grant ad group access to subscriber
        revoke_adgroup_access_from_subscriber : Revoke ad group access from subs
criber
        exit:exits the program
        quit:exits the program


usage:
    --batchfile <arg>   file containing commands to execute
CRO $
```

Add Organization

1. To add the service provider or other tenants as an organization, use the CLI command: ***add_subscriber***
   Refer to the section **Accessing the CLI** for the procedure to access the command line tool.
2. Enter the organization's unique name: For example: *MyServiceProvider*
3. Enter the description: For example: *My Service Provider*
4. Enter the subscriber, key in 0 or 1.

   - 0 for Service Provider
   - 1 for Subscriber

   Key in 0 for adding a service provider. The service provider *MyServiceProvider* is successfully added.

Add Directory Server

It is a prerequisite that AD servers are reachable from the RO server.

Make sure the **prerequisite** steps to configure the AD Server are performed before executing the below command.

1. To add a directory server, use the CLI command: ***add_directoryserver***
2. Enter the directory server's unique name: for example, *MyServiceProvider_AD*
3. Enter the directory server display name: For example, *MyServiceProvider_AD*
4. Enter the directory server URL: For example, *ldap://<AD Server URL>:<port>*
5. Enter the directory server domain: For example, *bdi.com*
6. Enter the directory server searchbase: For example, *dc=bdi, dc=com*
7. Enter the directory server username: For example, *qaadmin*
8. Enter the directory server password: For example, *Enter the password*
9. Enter the subscriber ID for which you want to associate this directory server: For example, *MyServiceProvider*

   The directory server is successfully added for Organization *MyServiceProvider*.

   Repeat the procedure to add a directory server for each organization.

Identify Users per Organization

To Identify/Register users per Organization for login purposes, follow the below steps.

1. You can add single or multiple users using the command: ***register_user_login***

2. The following message appears, Add more user? Y/N

- select Y to add more users to the same subscriber.
- select N to add a single user to the same subscriber.

Repeat and add all required users to Service Provider and Tenant organizations. This is a mandatory step, and it is only to register the users with RO.

Show Registered Users

To see the list of registered users of an Organization, use the CLI command: ***show_registered_user_login***

This command displays the users who are registered to log in with the Organization.

Provide AD Group access to Organizations

SP users need to be able to access tenant organization data. This is done on the AD group level. Access is provided to the AD group, and all users belonging to the AD group can access data of the organization that they have been allowed access to.

To provide access to subscribers use the CLI command: ***grant_adgroup_access_to_subscriber***

Ensure you perform this step to allow access to each of the tenant organizations for the AD Group that the SP belongs to.

Revoke AD Group access from the Organization

Use the CLI command ***revoke_adgroup_access_from_subscriber*** to revoke AD group access from the organization.

Add AD Group(s) per AD server/ Organizations

To configure AD Servers in RO, refer section the **External Directory Server Details in Kyndryl Resiliency Orchestration**.

To add an AD Group per AD Server/ Organization, refer section **Allowlisting AD Groups**.

Note:

- Each AD Group should be mapped to one Organization.

Delete Organisations

The delete Organization is not supported in the current release.

Assign Groups to Users of respective Organizations

Assigning groups to users of respective organizations is supported only for Basic Authentication Mode (or Multitenancy without AD). While creating or editing the user, groups can be assigned to the user for the respective organization.

Users can select the groups from the Assign Groups field as shown in the below figure.

Manage Users

User login can be enabled or disabled by another user with appropriate privileges. When disabled, the user will not be allowed to log into the Resiliency Orchestration portal.

Create User

The create user function is supported only for Basic Authentication Mode (or Multitenancy without AD). Organization dropdown has been introduced where the user with SPAdmin privileges can select the organization from the dropdown list, and it can view the organizations within its hierarchy only. Role and Assign Group lists are displayed based on the organization selected.

Edit Users

The edit user function is supported only for Basic Authentication Mode (or Multitenancy without AD). Organization dropdown has been introduced where a user with SPAdmin privileges can select the organization from the dropdown list, and it can view the organizations within its hierarchy only. Role and Assign Group lists are displayed based on the organization selected.

Enable Users

There is a new option Enable Users in the RBAC. This is to enable users within your tenant users. Refer to **Enabling Disabling Users** in the User Management section. If the logged-in user has the privilege, then they can enable/disable other users of their organization.

Disable Users

There is a new option Disable Users in the RBAC. This is to disable users within your tenant users. Refer to **Enabling Disabling Users** in the User Management section. If the logged-in user has the privilege, then they can enable/disable other users of their organization.

Delete Users

Users with the SPAdmin role can delete the users under its hierarchy.

Known Limitations

The following are the known issues of this new feature -

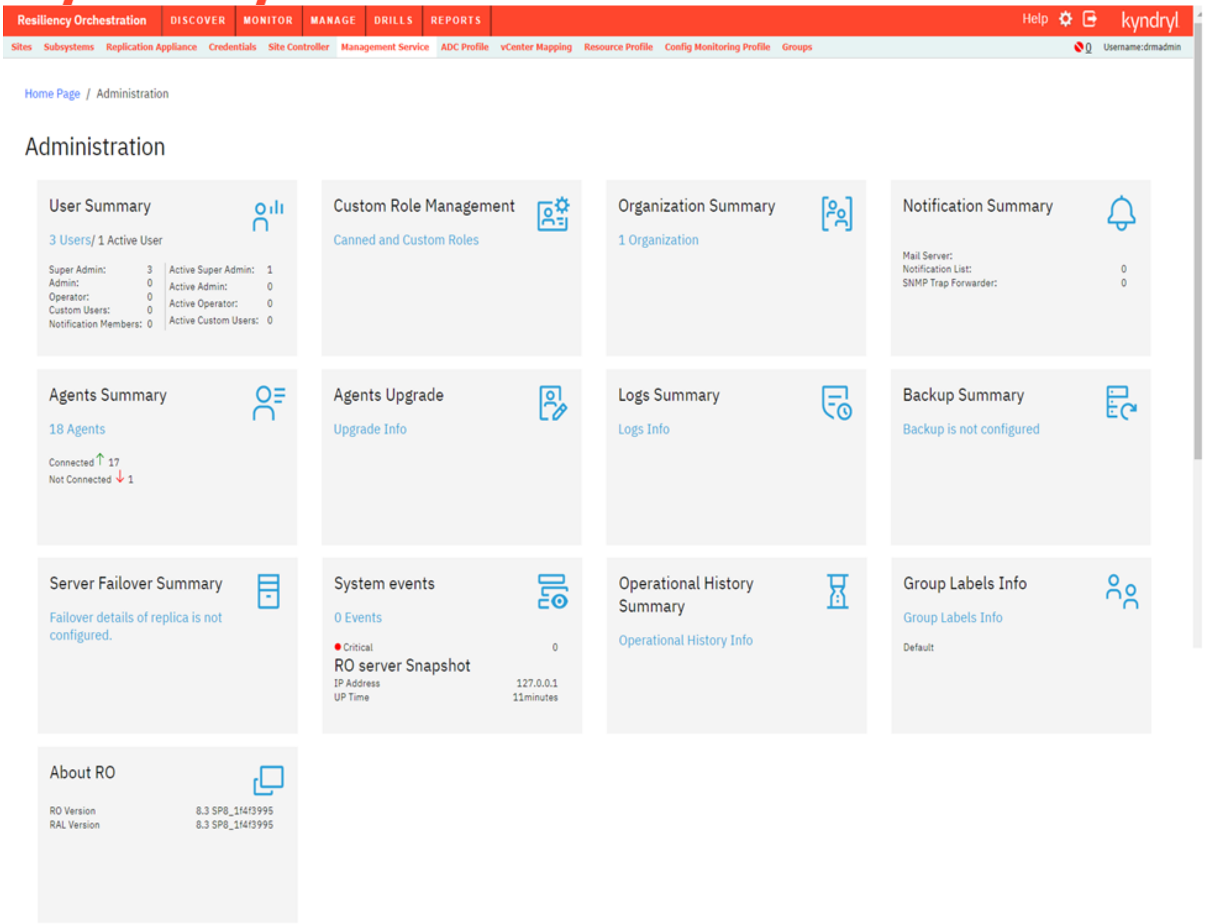
1. Resiliency Orchestration software ships with 4 roles. Refer to role details in the section **Define Appropriate Roles.** These roles should not be edited or deleted from the system.
2. BIRT Reports (Common Reports and Custom Reports) are not accessible to TenantAdmin and TenantOperator roles. It is accessible to SPAdmin and SPOperator roles.
3. Download (Export to HTML and Export to PDF link) RPO/RTO/Datalag, Workflow Execution Report Download links are accessible to the Service Provider only (SPAdmin, SPOperator roles) and not to the tenant.

4. If you get an "**Internal Error**" or "**Access problem**" error message while accessing a few pages or during certain operations, it implies you do not have the required permissions to perform the operation or view/access the page. To request access, please contact your Administrator or Service Provider.
5. The **Admin** > **User Summary** page shows the total count of users in the system. Any tenant user will be able to see this count. However, the details of the user are not available and tenants can only see the details of their organization.
6. Zerto group creation should be done as a drmadmin user. Once the AG/RGs are created, either drmadmin or SPAdmin should assign these RG/AGs to the respective Tenant Organizations.
7. If 2 VPGs have having same Failover IPs, then agents are not connecting to the Site Controller.

User Management

The Kyndryl Resiliency Orchestration Administration console allows you to perform various administration activities like creating the users, modifying the users, deleting the users, configuring notification lists, agents, backup manager, managing logs, and executing Kyndryl Resiliency Orchestration Server failover.

Click the Admin icon on the Home page to view the Administration Tasks Summary page.



Administration

User Summary

3 Users/ 1 Active User

Super Admin:	3	Active Super Admin:	1
Admin:	0	Active Admin:	0
Operator:	0	Active Operator:	0
Custom Users:	0	Active Custom Users:	0
Notification Members:	0		

Custom Role Management

Canned and Custom Roles

Organization Summary

1 Organization

Notification Summary

Mail Server:	
Notification List:	0
SNMP Trap Forwarder:	0

Agents Summary

18 Agents

Connected ↑ 17
Not Connected ↓ 1

Agents Upgrade

Upgrade Info

Logs Summary

Logs Info

Backup Summary

Backup is not configured

Server Failover Summary

Failover details of replica is not configured.

System events

0 Events

● Critical 0

RO server Snapshot

IP Address	127.0.0.1
UP Time	11minutes

Operational History Summary

Operational History Info

Group Labels Info

Group Labels Info

Default

About RO

RO Version	8.3 SP8_1f4f3995
RAL Version	8.3 SP8_1f4f3995

Setting up Users

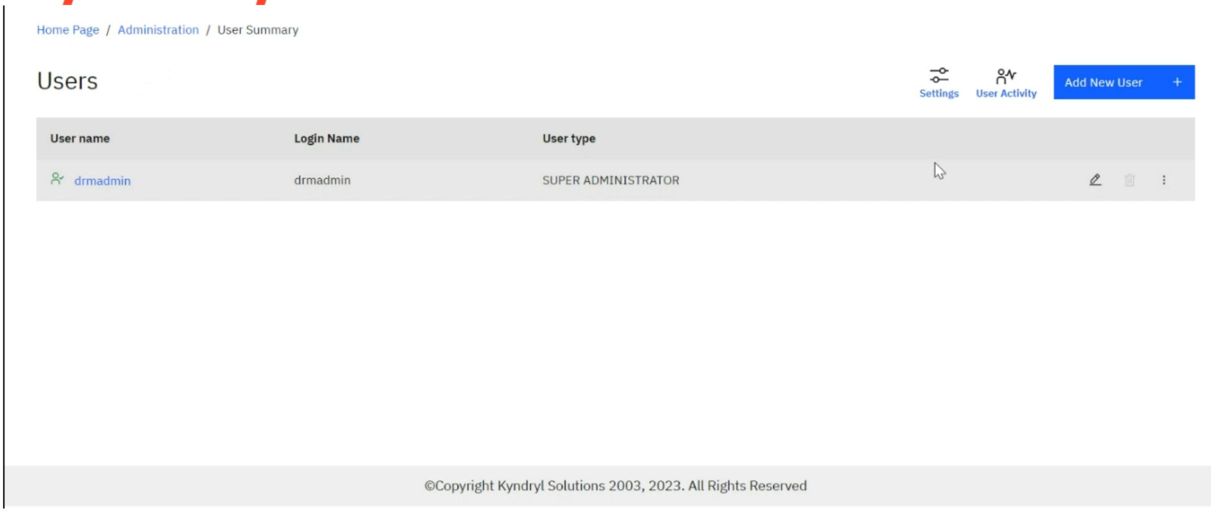
This chapter describes how to configure and setup users in the Kyndryl Resiliency Orchestration environment.

This section explains the following:

- Adding Users
- Modifying Users
- Deleting Users
- Setting System Options for Users

Adding Users

Click ***User Summary*** to see the privileges.



Home Page / Administration / User Summary

Users

User name	Login Name	User type
drmadmin	drmadmin	SUPER ADMINISTRATOR

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

To add a new user, perform the following steps:

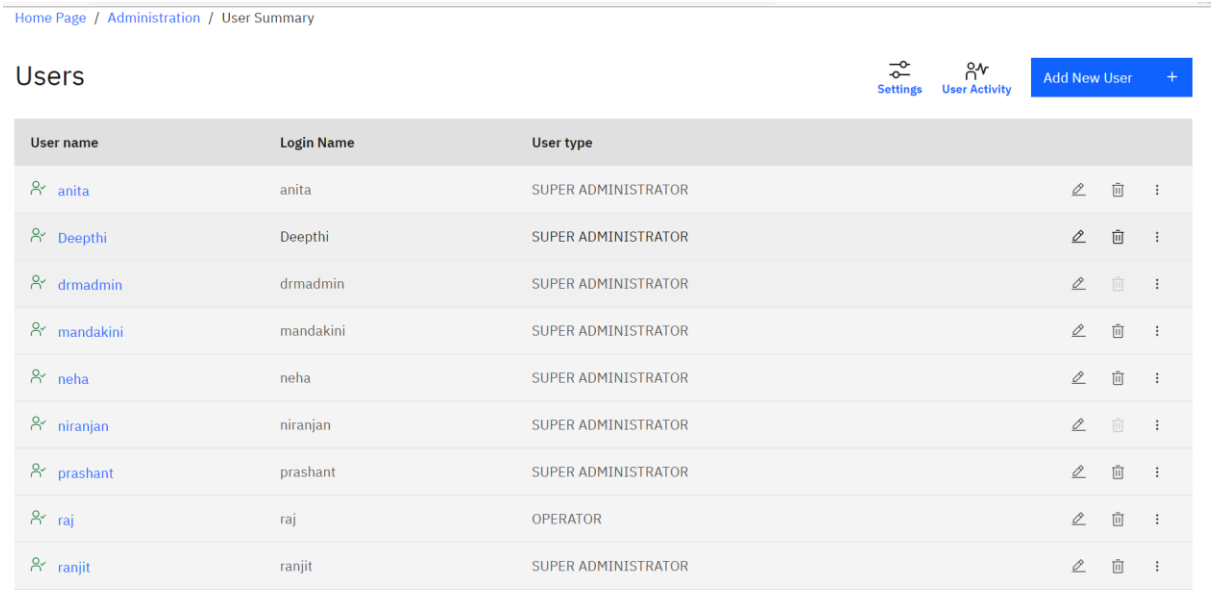
1. Click **Admin** on the navigation bar. The **Administration** page appears. In the **User Summary** tile, click on any of the user from the **User name** column. **View User Details** page displays.

   Note –

   Only the Super Administrator has the authority to add users.

2. Click **Add New User** at the top right corner of **Kyndryl Resiliency Orchestration Users** page. The **Create New User** page displays.

In the **Create New User** page, you can set details of the user along with their login information UserName and password in the Create New User page. You can create a user by providing following information.



Home Page / Administration / User Summary

Users

User name	Login Name	User type
anita	anita	SUPER ADMINISTRATOR
Deepthi	Deepthi	SUPER ADMINISTRATOR
drmadmin	drmadmin	SUPER ADMINISTRATOR
mandakini	mandakini	SUPER ADMINISTRATOR
neha	neha	SUPER ADMINISTRATOR
niranjan	niranjan	SUPER ADMINISTRATOR
prashant	prashant	SUPER ADMINISTRATOR
raj	raj	OPERATOR
ranjit	ranjit	SUPER ADMINISTRATOR

Field	Description
Login Information	
User Name (Required)	User Name is the Kyndryl Resiliency Orchestration user name that you enter while logging into Kyndryl Resiliency Orchestration. ▪ This field accepts up to 16 alphanumeric characters and must begin with a letter.
Choose Password (Required)	The password is used to authenticate the Kyndryl Resiliency Orchestration user within Kyndryl Resiliency Orchestration. The password length is minimum 15 and maximum 25 alphanumeric characters including at least one digit for login to Kyndryl Resiliency Orchestration, as a part of GDPR enhancement. Note: The password cannot contain the following character patterns: ▪ <script>(.*?)</script> ▪ Src=* ▪ Eval ▪ Expression ▪ JavaScript ▪ VBScript ▪ Onload ▪ Iframe ▪ <*>
Confirm Password (Required)	Re-enter the password to confirm it.
User Details	

Organization	Select any one of the following options from the drop down list. **Note:** Only Default option is available from the drop down list.
Full Name (Required)	Provide the user's full name. ▪ This field is mandatory. ▪ This field accepts up to 64 characters, including alphanumeric, spaces, and underscores.
Role	Select any one of the following options to assign role to the user. ▪ Super Administrator ▪ Administrator ▪ Operator ▪ Notification-Member **Note:** If you have created a custom role, it will also appear as an option in this section.
Assign Groups	▪ Click a group to select the Group that the user should be associated with from the list. ▪ To select multiple Groups, keep the CTRL key pressed and click the desired Groups one by one.
Preferences	
Home Page	Select the landing page that is displayed after logging on to Kyndryl Resiliency Orchestration. Home page options in the drop-down list. Note If you are creating a user with Operator level permissions, the list of possible Home Pages will contain only those pages that an Operator can see.
Contact Details	

Mobile	Enter the mobile number of the user.
Email (Required)	Enter the e-mail address of the user. This field accepts valid e-mail addresses in the form of name@organization.domain, for example, fred@kyndryl.com
Preferred Mode(s) of Communication	Select the mode of communication. The available choices are: ▪ Email ▪ Mobile Note Based on the mode of communication you select, make sure that appropriate values are specified in the corresponding fields.

3. Click **Create** to add the user.
   OR
   Click **Cancel** to quit the current operation.
4. On successfully adding a user, a message box is displayed.
5. Click **OK** in the message box to return to the Kyndryl Resiliency Orchestration Users page.

Deleting AD Users

The following are the use case scenarios for deleting AD users.

Use Case 1: User Deleted from the AD and not from RO UI.

In this use case, the user role will be still available in the RO UI although deleted from the AD. To delete the user role from the RO UI as well, perform the following steps:

1. From the RO UI, click **Admin** on the navigation bar.

The **Administration** page appears.

2. Select the user you want to delete and click the Delete 🗑 icon.

The user is deleted from the RO UI.

Note: The Super Administrator can also delete the user from the RO UI.

Setting System Options for Users

Super Administrator has privileges to set default settings for users.

Click ***User Summary*** to see the privileges.

To establish settings for default users:

1. Click **Admin** on the navigation bar. The **Administration** page appears. Click on **Settings** icon.
2. The **Set System Options for Users** page displays.

   In the Set System Options for Users page, the Super Administrator can set the following privileges.

Field	Description
Preferences	
Home Page	Select the landing page for all users that is displayed after login to Kyndryl Resiliency Orchestration.
Password	
All User Passwords expire in	Select the duration for the expiry of passwords. a. Enter a valid number in the text box. b. Select the unit of time from the drop-down list. The available options are: Never, Days, Weeks, and Months. **Note** Select "Never" if you do not want the password to expire.
Notify User on Password expiry	Enter the number of days prior to the expiry day when you want to notify the user regarding password expiration.
Mode of Communication	
Preferred Mode(s) of Communication	Select the mode of communication. The available choices are: ▪ Email ▪ Mobile Note: Based on the mode of communication you select, make sure that appropriate values are entered in the corresponding fields.

3. Click **Save** to save system options for users.
4. If you want to close the window without saving changes, Click **Cancel**.

Editing User Preferences

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To edit user preferences:

1. Click **Admin** on the navigation bar. The **Administration** page appears. User Names list appears.
2. Select the user you want to edit and click on ✎ icon.
3. Edit User Details page appears.
4. Change the required fields.
5. Click Update to update the changes, or Cancel to close the window without saving the changes.

Configuring LDAP

Note

The steps provided below are regarding 389 Directory Structure on Fedora.

1. Install the LDAP Directory Server on the Linux machine.
2. Login to the **Admin** console of the Directory Server.

Creating custom Class and Attributes

A "**Custom class**" for holding Kyndryl Resiliency Orchestration roles has to be created with appropriate custom attributes. This custom class will be a child of the **"groups"** class.

1. Login to the LDAP server.
2. New custom attributes can be provided in the **Schema** tab.

The following attributes for Kyndryl Resiliency Orchestration will have to be created with the type **Boolean**:

Attribute name	Type
bp-edit	Boolean
bp-execute	Boolean
failover-edit	Boolean
failover-execute	Boolean
fallback-edit	Boolean
fallback-execute	Boolean
fallbackresync-edit	Boolean
fallbackresync-execute	Boolean
groups-edit	Boolean
newdrill-edit	Boolean

Attribute name	Type
newdrill-execute	Boolean
normalcopy-edit	Boolean
normalcopy-execute	Boolean
normalfullcopy-edit	Boolean
normalfullcopy-execute	Boolean
policy-edit	Boolean
policy-execute	Boolean
reversenormalcopy-edit	Boolean
reversenormalcopy-execute	Boolean
switchback-edit	Boolean
switchback-execute	Boolean
switchover-edit	Boolean
switchover-execute	Boolean

3. For example, to create **"bp-edit"** attribute, enter the Attribute name as **bp-edit** and select the **Syntax** as **Boolean**.
4. Create attributes for rest of the values given in the table above. Ensure the feature operation attributes are in lower case and there is no mismatch in the spelling.
5. For creating the custom class, go to the **Object Classes** tab.
6. Provide the name for the custom class as **KyndrylResiliencyOrchestrationrole**. Select a **Parent** to the class name **groupofuniquenames**.
7. The custom attributes created previously should be added into the custom class. Select the required custom attributes from the **Available Attributes** list. Ensure all the relevant attributes are added and submit.

Creating pre-packaged roles for Kyndryl Resiliency Orchestration

The following pre-packaged roles are supported in Kyndryl Resiliency Orchestration, and the same should be created on the LDAP server:

Role name	Role name in LDAP
SUPER ADMINISTRATOR	SANOVI-SUPER ADMINISTRATOR
ADMINISTRATOR	SANOVI-ADMINISTRATOR
OPERATOR	SANOVI-OPERATOR
NOTIFICATION MEMBER	SANOVI-NOTIFICATION MEMBER

1. Login to LDAP server and go to the Domain Component in which Kyndryl Resiliency Orchestration roles will reside. For example, the Domain Component **Kyndryl** is selected and it will have the following **dc=Kyndryl, dc=com**.
2. An organizational unit with the name **Roles** has to be created for storing Kyndryl Resiliency Orchestration roles. Create the same in the Domain Component selected.
3. To create a new role, for example, a **SUPER ADMINISTRATOR**, go to the organizational unit **Roles** created in the previous step and create a new object with the type being **Kyndryldrmrole**. The role name should have the prefix **"SANOVI-"** to identify them as roles created for Kyndryl Resiliency Orchestration. For example, for a **SUPER ADMINISTRATOR** role, enter group name as **SANOVI-SUPER ADMINISTRATOR**.
4. Users can be added to the newly created roles through the role properties.
5. Similarly add the other pre-packaged roles and the required users.

   Note:

   The role name format after the prefix should not contain hyphen. This is because the hyphen is used as a delimiter to separate the role-prefix and the actual role name.

Creating custom roles for Kyndryl Resiliency Orchestration as LDAP or AD Authorizing Server

Custom roles can be created using any of the following feature-operations and assigned to users who already have **OPERATOR** role assigned to them.

Features/Operations	Execute [Includes Start/Stop]	Edit [Includes Create/Edit/Delete]
Switchback	X	X
Switchover	X	X
Failover	X	X
Fallback	X	X
FallbackResync	X	X

NormalCopy	X	X
NormalFullCopy	X	X
ReverseNormalCopy	X	X
Policy	X	X
BP	X	X
Tests	X	X
Groups		X

1. To create a new custom role, for example, a **SUPER ADMINISTRATOR**, go to the organizational unit **Roles** and create a new object with the type being **KyndrylResiliencyOrchestrationrole**. The role name should have the prefix **"SANOVI-"** to identify them as roles created for Kyndryl Resiliency Orchestration. For example, for the custom role having **GROUPS-EDIT** feature-operation provide a role name like **SANOVI-GROUPS ROLE**.
2. Users can be added to the newly created roles through the role properties.
3. Add the required custom attribute for the custom role through the role properties. For example for the role **SANOVI-GROUPS ROLE** the attributes **groups-edit** can be added to the custom role. Ensure the attribute value is set to **TRUE** to enable it for the role.
4. Similarly create custom roles for other required feature-operations.
    a. Note:
    b. The role name format after the prefix should not contain hyphen. This is because the hyphen is used as a delimiter to separate the role-prefix and the actual role name.

External Directory Server Details

To view the External Directory Server Details for LDAP Server, perform the following steps:

1. Click Admin on the navigation bar. The Administration page appears. Scroll down to the Directory Server Details and click Go to Directory Server Details. The External Directory Server Details page appears.
2. The LDAP Server can be selected and it has the following options:
    1. Server URL
    2. Search Base for reading roles

User Account for reading directories

- Username
- Password

Note

If anonymous directory lookup is enabled, then the configured user for accessing the directory server will be able to lookup the directory even if the credentials given are wrong.

LDAP Query

Roles are searched from the organizational unit **ou=Roles**

Users associated with the role are read by reading the attribute **uniquemember** from the role.

Configuring AD for AD Authenticate and Authorize

1. Login to the AD server.
2. An organizational unit with the name **Roles** has to be created for storing Kyndryl Resiliency Orchestration roles. Create the same in the required Domain Component.
3. Ensure the following tools are installed on the Advanced Directory server machine:

schmmgmt - Appendix A : Installation of **schmmgmt** tool on Active Directory machine.

ADSI Edit - Appendix B: Installation of **ADSI Edit** tool on Active Directory machine.

Also, the Unique **X.500** Object Id for the machine running the AD server is required while creating the

Creating custom Class and Attributes

The **schmmgmt** tool will display the list of **classes** and **attributes** being loaded into the AD server through the schema

The following **attributes** for Kyndryl Resiliency Orchestration will have to be created with the type **Boolean** using the **schmmgmt** tool.

Attribute name	Type
bp-edit	Boolean
bp-execute	Boolean
failover-edit	Boolean
failover-execute	Boolean
fallback-edit	Boolean
fallback-execute	Boolean
fallbackresync-edit	Boolean
fallbackresync-execute	Boolean
groups-edit	Boolean
newdrill-edit	Boolean
newdrill-execute	Boolean
normalcopy-edit	Boolean
normalcopy-execute	Boolean
normalfullcopy-edit	Boolean

Attribute name	Type
normalfullcopy-execute	Boolean
policy-edit	Boolean
policy-execute	Boolean
reversenormalcopy-edit	Boolean
reversenormalcopy-execute	Boolean
switchback-edit	Boolean
switchback-execute	Boolean
switchover-edit	Boolean
switchover-execute	Boolean

1. For example, to create **bp-edit**, the **common name** and **LDAP Display name** for the attribute is **bp-edit**. Assign a Unique X500 Object ID for the attribute and ensure syntax for the attribute is Boolean.
2. Similarly, create the custom attributes and ensure that each of these attributes use a unique ending sequence number for the unique X500 Object ID.
3. Create a custom class in the **schmmgmt** window and provide **common name** and **LDAP Display name** as **Kyndryl-role**. Assign a Unique X500 Object ID for the class. Ensure that **cn** is a Mandatory attribute in the custom class and all the Kyndryl Resiliency Orchestration relevant custom attributes as Optional attributes.

Creating pre-packaged roles for Kyndryl Resiliency Orchestration

The following pre-packaged roles are supported in Kyndryl Resiliency Orchestration, and the same should be created on the AD server:

Role name	Role name in AD
SUPER ADMINISTRATOR	SANOVI-SUPER ADMINISTRATOR
ADMINISTRATOR	SANOVI-ADMINISTRATOR
OPERATOR	SANOVI-OPERATOR
NOTIFICATION MEMBER	SANOVI-NOTIFICATION MEMBER

1. The **Adsiedit** tool can be used to create pre-packaged roles.

All roles should have the prefix **"SANOVI-"** to identify them as roles created for Kyndryl Resiliency Orchestration.

2. To create a pre-packaged role, for example **SUPER ADMINISTRATOR**, create a new object with type **SANOVI-role**. Provide **cn** and **sAMAccountName** as **SANOVI-SUPER ADMINISTRATOR**

3. A user can be added to a role by adding it as a member of the role through its properties.

Similarly create the other pre-packaged roles.

Creating custom roles for Kyndryl Resiliency Orchestration

Custom roles can be created using any of the following feature-operations and assigned to users who already have OPERATOR role assigned to them.

Features/Operations	**Execute [Includes Start/Stop]**	**Edit [Includes Create/Edit/Delete]**
Switchback	X	X
Switchover	X	X
Failover	X	X
Fallback	X	X
FallbackResync	X	X
NormalCopy	X	X
NormalFullCopy	X	X
ReverseNormalCopy	X	X
Policy	X	X
BP	X	X
Tests	X	X
Groups		X

1. The **Adsiedit** tool can be used to create custom roles.
2. All roles should have the prefix "SANOVI-" to identify them as roles created for Kyndryl Resiliency Orchestration.
3. To create a custom role which will handle, for example the feature GROUPS-EDIT , create a new object with type SANOVI-role. Provide cn and sAMAccountName as say SANOVI-GROUPS ROLE
4. Add the required custom attributes to the role. For example, add groups-edit to the role and ensure its value is set to TRUE to enable it for the role.
5. A user can be added to a role by adding it as a member of the role through its properties.

Similarly create the other required custom roles.

Note -

The role name format after the prefix should not contain hyphen. This is because the hyphen is used as a delimiter to separate the role-prefix and the actual role name.

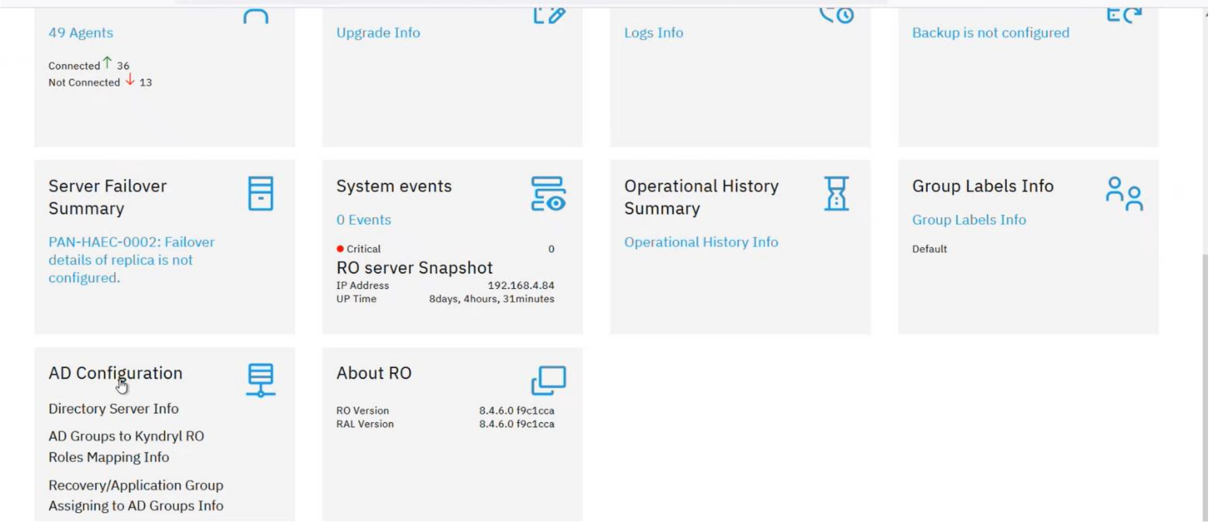
Configuring AD for AD Authenticate and Basic RO Authorize

External Directory Server Details in Kyndryl Resiliency Orchestration

To view the External Directory Server Details for AD Server, perform the following steps:

1. Log in using Admin privileges example user: drmadmin password:xxxxx.

2. Click Admin on the navigation bar. The Administration page appears.



49 Agents
Connected 36
Not Connected 13

Upgrade Info

Logs Info

Backup is not configured

Server Failover Summary
PAN-HAEC-0002: Failover details of replica is not configured.

System events
0 Events
Critical 0
RO server Snapshot
IP Address 192.168.4.84
UP Time 8days, 4hours, 31minutes

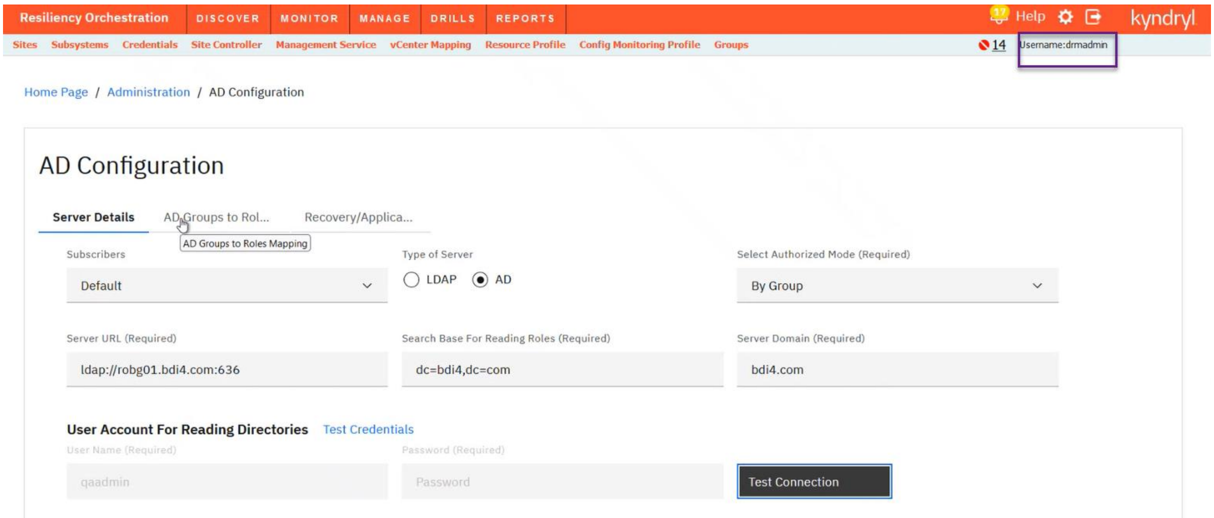
Operational History Summary
Operational History Info

Group Labels Info
Group Labels Info
Default

AD Configuration
Directory Server Info
AD Groups to Kyndryl RO Roles Mapping Info
Recovery/Application Group Assigning to AD Groups Info

About RO
RO Version 8.4.6.0 f9c1cca
RAL Version 8.4.6.0 f9c1cca

3. Scroll down to the **AD configuration** and click **Go to Directory Server Info** link. The **External Directory Server Details** page appears.



Home Page / Administration / AD Configuration

AD Configuration

Server Details | AD Groups to Rol... | Recovery/Applica...

AD Groups to Roles Mapping

Subscribers: Default

Type of Server: ○ LDAP ● AD

Select Authorized Mode (Required): By Group

Server URL (Required): ldap://robg01.bdi4.com:636

Search Base For Reading Roles (Required): dc=bdi4,dc=com

Server Domain (Required): bdi4.com

User Account For Reading Directories   Test Credentials

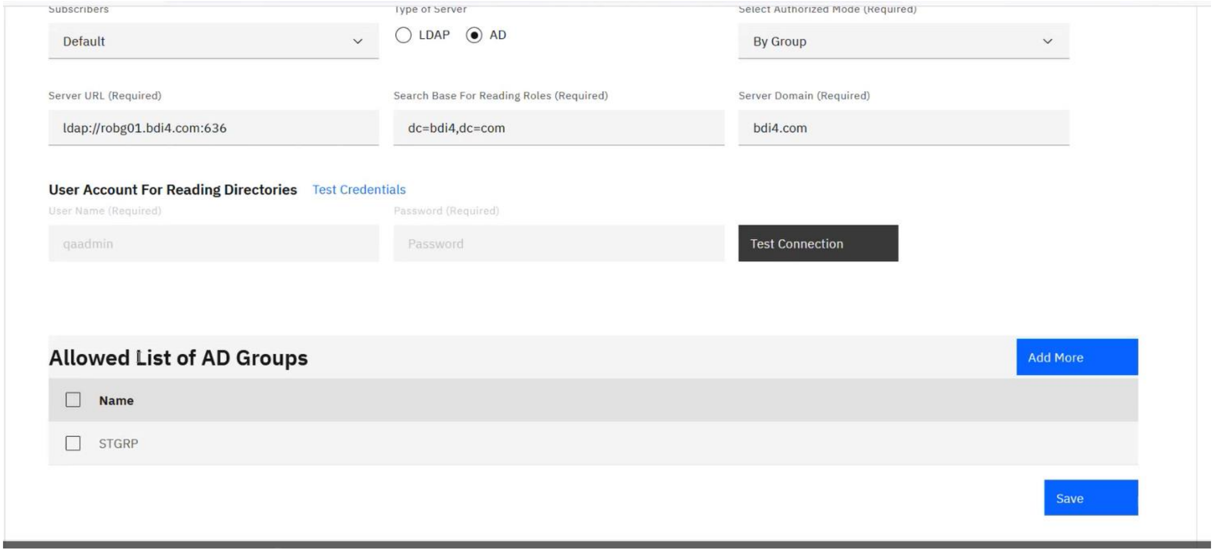
User Name (Required): qaadmin

Password (Required): Password

Test Connection

4. The AD Server is selected by default. It has the following tabs :
   - Server details
   - Ad Groups to Role
   - Recovery/Application group

Tab I



Subscribers: Default

Type of Server: ○ LDAP ● AD

Select Authorized Mode (Required): By Group

Server URL (Required): ldap://robg01.bdi4.com:636

Search Base For Reading Roles (Required): dc=bdi4,dc=com

Server Domain (Required): bdi4.com

User Account For Reading Directories

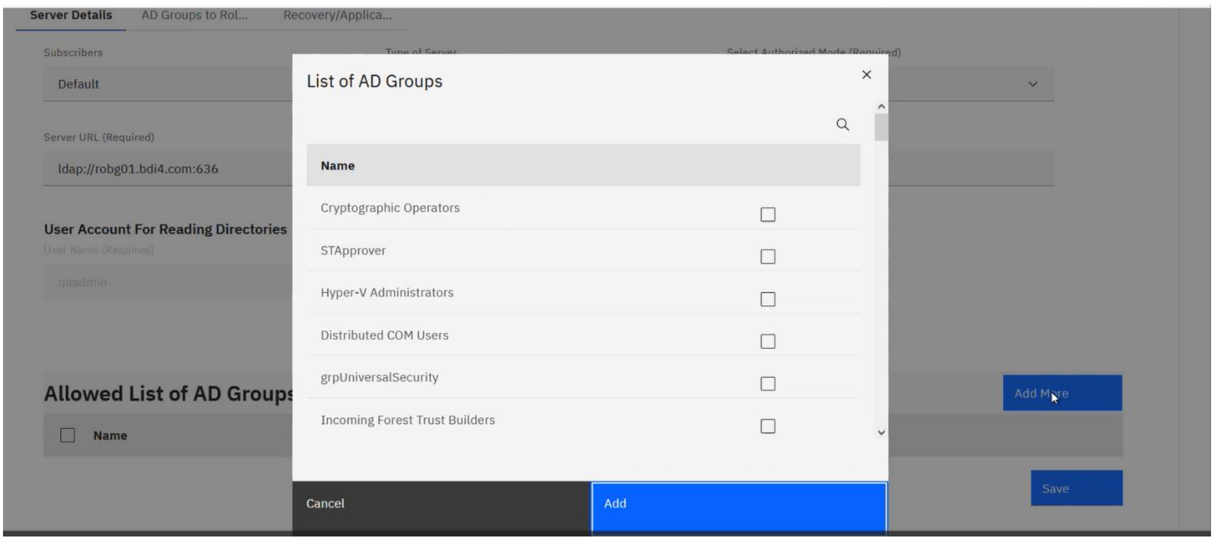
User Name (Required): qaadmin

Password (Required): Password

Allowed List of AD Groups

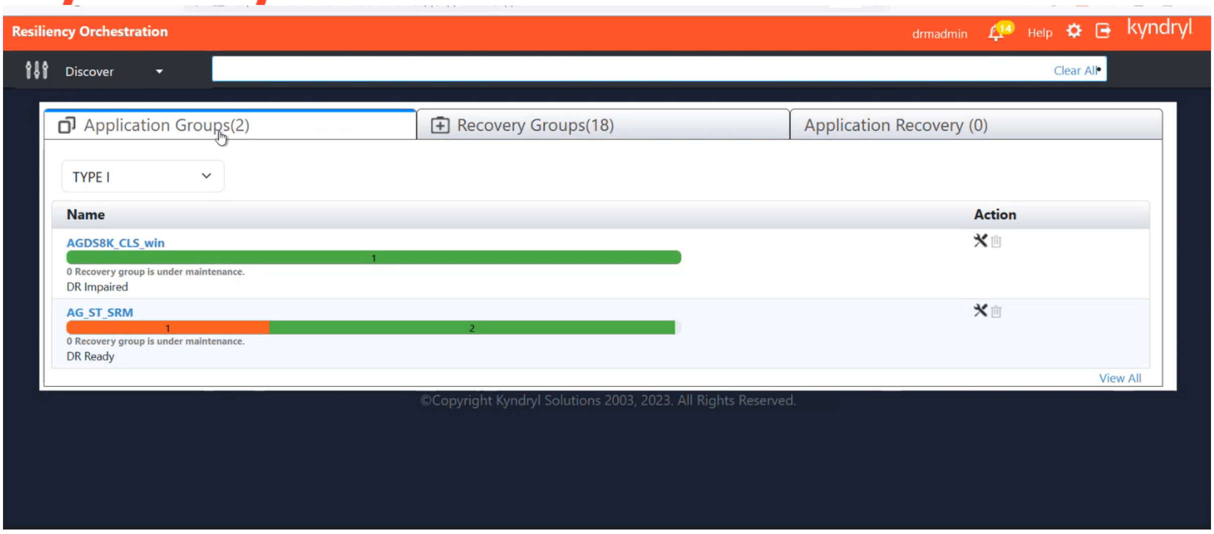
□ Name
□ STGRP

Select Add more



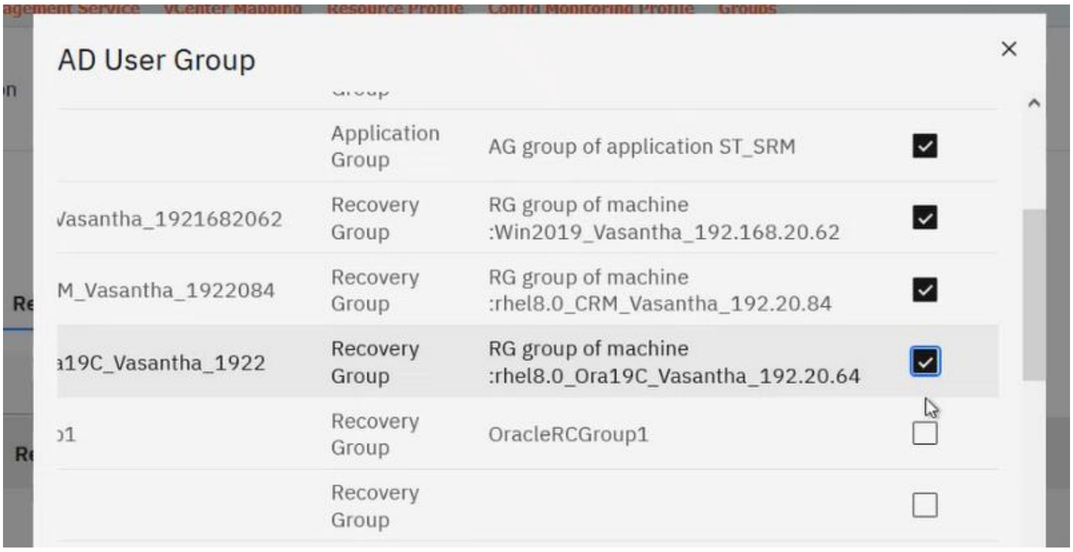
List of AD Groups

Name	
Cryptographic Operators	□
STApprover	□
Hyper-V Administrators	□
Distributed COM Users	□
grpUniversalSecurity	□
Incoming Forest Trust Builders	□



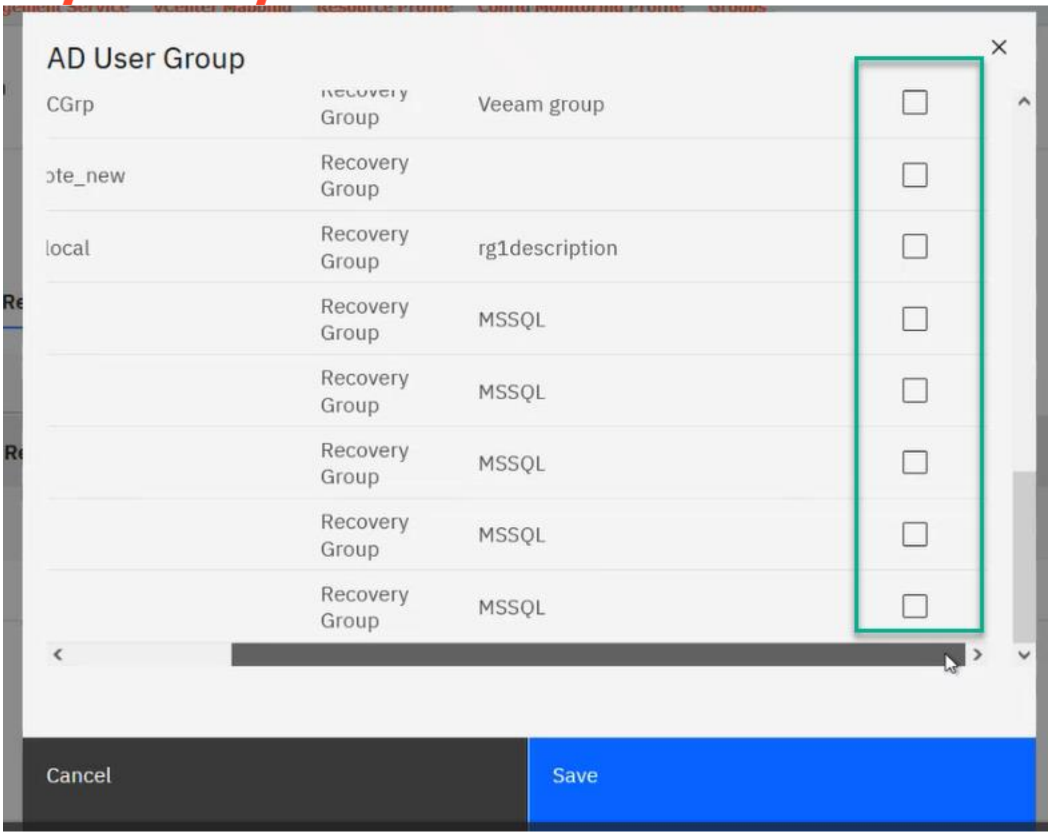
Name	Action
AGDS8K_CLS_win 1 0 Recovery group is under maintenance. DR Impaired	
AG_ST_SRM 1 2 0 Recovery group is under maintenance. DR Ready	

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved.



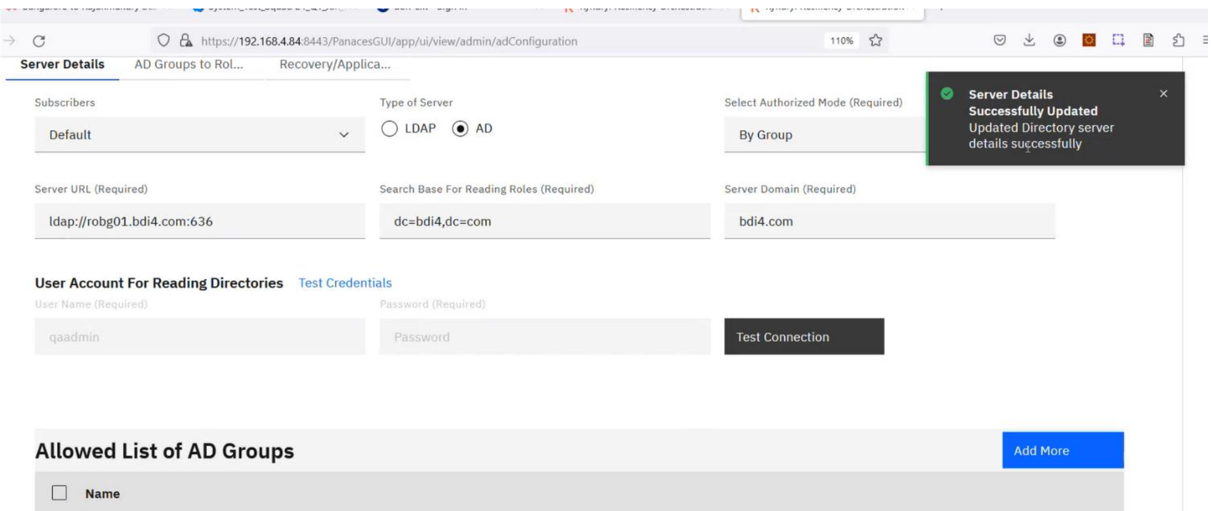
AD User Group

	Application Group	AG group of application ST_SRM	☑
/asantha_1921682062	Recovery Group	RG group of machine :Win2019_Vasantha_192.168.20.62	☑
M_Vasantha_1922084	Recovery Group	RG group of machine :rhel8.0_CRM_Vasantha_192.20.84	☑
a19C_Vasantha_1922	Recovery Group	RG group of machine :rhel8.0_Ora19C_Vasantha_192.20.64	☑
)1	Recovery Group	OracleRCGroup1	□
	Recovery Group		□



AD User Group

CGrp	Recovery Group	Veeam group	□
ɔte_new	Recovery Group		□
local	Recovery Group	rg1description	□
	Recovery Group	MSSQL	□
	Recovery Group	MSSQL	□
	Recovery Group	MSSQL	□
	Recovery Group	MSSQL	□
	Recovery Group	MSSQL	□



https://192.168.4.84:8443/PanacesGUI/app/ui/view/admin/adConfiguration
110%
Server Details
AD Groups to Rol...
Recovery/Applica...

Subscribers: Default

Type of Server: ○ LDAP ● AD

Select Authorized Mode (Required): By Group

Server Details Successfully Updated
Updated Directory server details successfully

Server URL (Required): ldap://robg01.bdi4.com:636

Search Base For Reading Roles (Required): dc=bdi4,dc=com

Server Domain (Required): bdi4.com

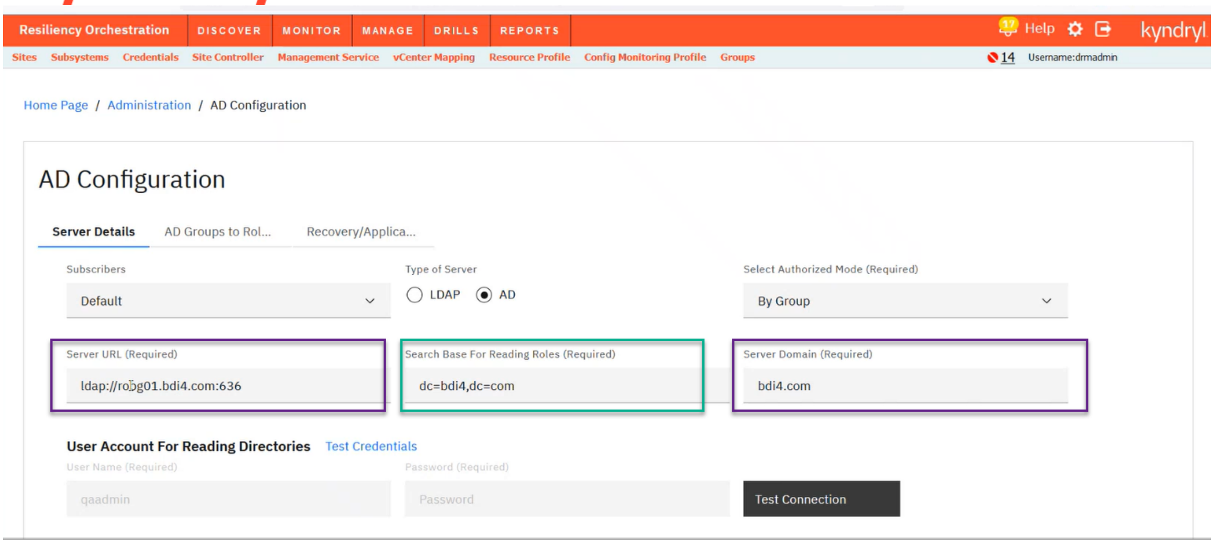
User Account For Reading Directories Test Credentials

User Name (Required): qaadmin

Password (Required): Password

Allowed List of AD Groups

□ Name



Home Page / Administration / AD Configuration

AD Configuration

Server Details | AD Groups to Rol... | Recovery/Applica...

Subscribers: Default

Type of Server: ○ LDAP ● AD

Select Authorized Mode (Required): By Group

Server URL (Required): ldap://robg01.bdi4.com:636

Search Base For Reading Roles (Required): dc=bdi4,dc=com

Server Domain (Required): bdi4.com

User Account For Reading Directories Test Credentials

User Name (Required): qaadmin

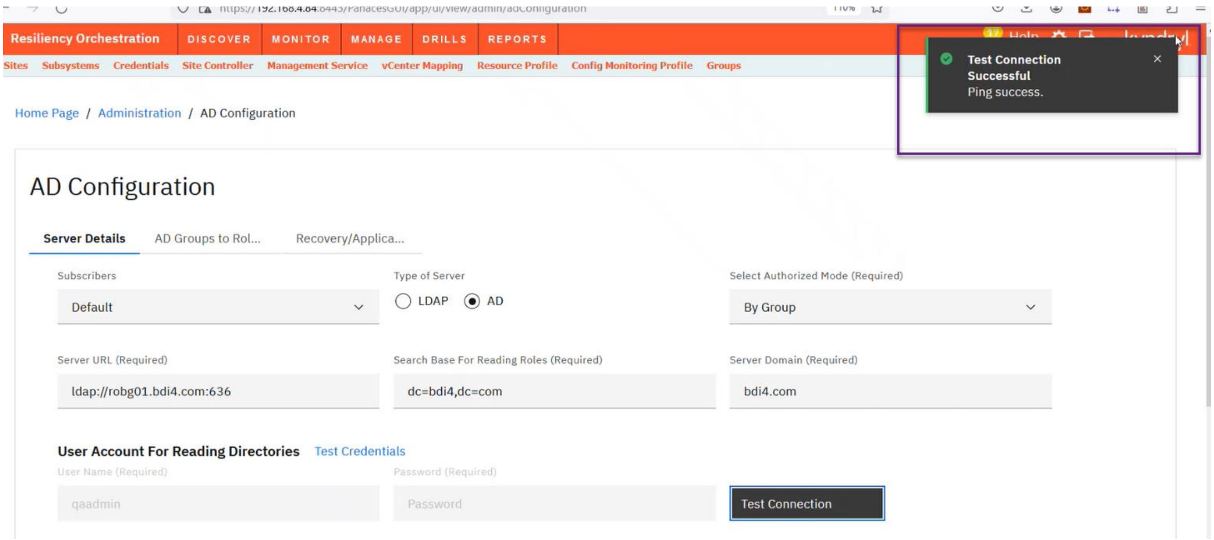
Password (Required): Password

Test Connection

Select values for the fields example values shown in screenshot above.

Press Test connection

The following screen will appear



Test Connection Successful
Ping success.

Home Page / Administration / AD Configuration

AD Configuration

Server Details | AD Groups to Rol... | Recovery/Applica...

Subscribers: Default

Type of Server: ○ LDAP ● AD

Select Authorized Mode (Required): By Group

Server URL (Required): ldap://robg01.bdi4.com:636

Search Base For Reading Roles (Required): dc=bdi4,dc=com

Server Domain (Required): bdi4.com

User Account For Reading Directories Test Credentials

User Name (Required): qaadmin

Password (Required): Password

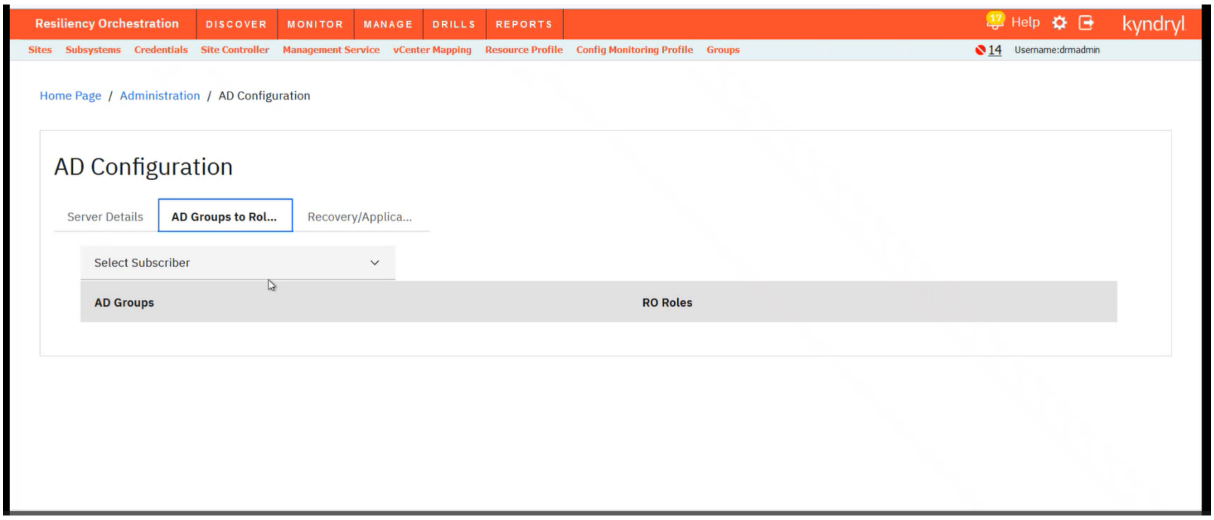
Test Connection

Tab II. Allowlisting AD Groups

In the Kyndryl Resiliency Orchestration **External Directory Server Details** page, an option to allowlist AD groups is provided. Only the users who are part of the allowed list of AD groups would be given access to Kyndryl Resiliency Orchestration.

Follow the procedure below to allowlist AD groups –

1. Click **Admin** on the navigation bar. The Administration page appears.
2. Scroll down to the **Directory Server Details** and click **Go to Directory Server Details**. The **External Directory Server Details** page appears.
3. Select **Type of Server** as "AD", if not selected already.
4. Ensure that **Select Authorized Mode** should be set to "By Group".
5. Click **Next**. The **Allowed list of AD groups** text box is empty during initial login. The AD Groups that are available and can be added to the allowlist are listed in the table.
6. Select one or more AD Groups by clicking the checkbox beside each group name and click **Save**.
   Note: You can directly allowlist an AD group by entering the name in the **Enter AD Group Name** textbox and then clicking the **ADD GROUP** button.



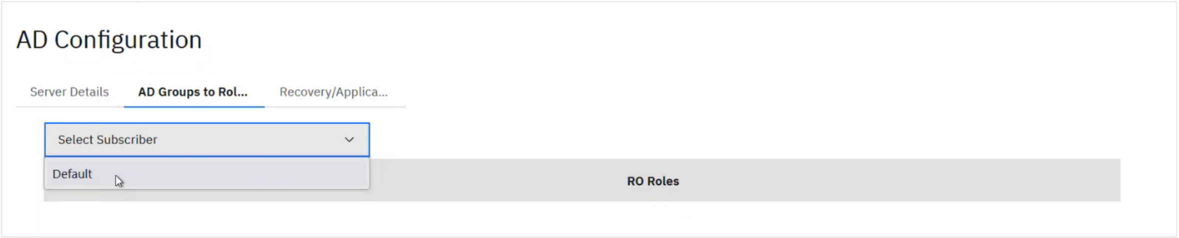
Home Page / Administration / AD Configuration

AD Configuration

Server Details | AD Groups to Rol... | Recovery/Applica...

Select Subscriber

AD Groups	RO Roles



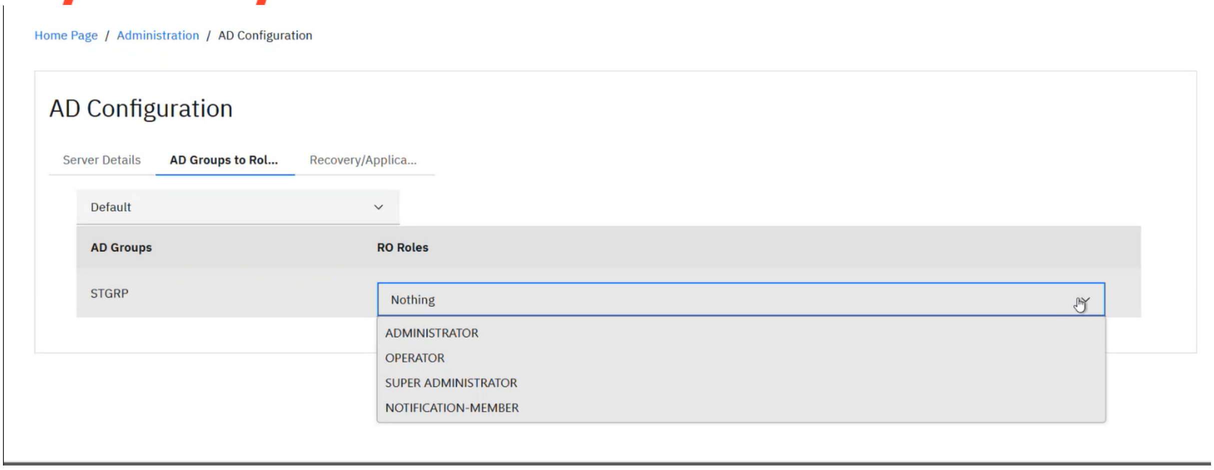
AD Configuration

Server Details | AD Groups to Rol... | Recovery/Applica...

Select Subscriber

Default

RO Roles



Home Page / Administration / AD Configuration

AD Configuration

AD Groups	RO Roles
STGRP	Nothing

The selected AD Groups are added in the **Allowed list of AD groups** text box. Multiple groups are listed as comma separated values, as shown in figure below.

7. Click **Save** to save your selection.

The required AD Groups are now in the allowlist and assigned with default role that do not have any privileges. Users of these allowed list of AD groups will be able to access Kyndryl Resiliency Orchestration only after a specific role (other than default) is assigned to the AD group.

To assign a specific role to the AD Group, refer the procedure in section **AD Groups to Kyndryl Resiliency Orchestration Roles Mapping**.

Note - If you connect to a different AD Server or if any of the allowed AD Groups are later deleted at the AD Server currently in use, the users part of that AD Group will not be able to access Kyndryl Resiliency Orchestration. However, AD groups are still listed in Kyndryl Resiliency Orchestration **Allowed list of AD groups** text box. This has to be fixed manually by selecting/unselecting the AD Group from the new tabular list and saving the changes.

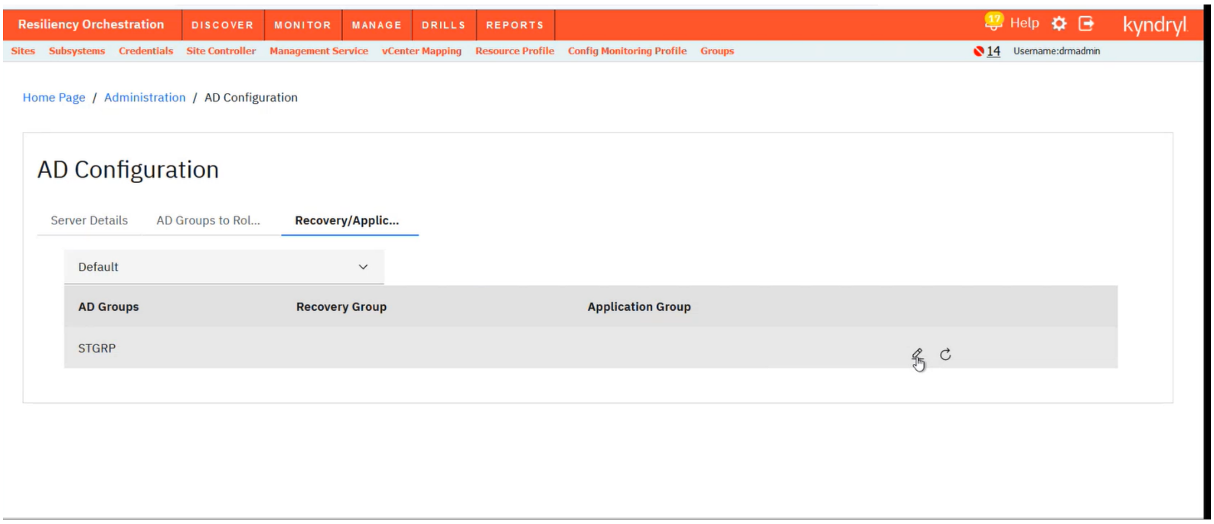
Tab III ***AD Groups to Kyndryl Resiliency Orchestration Roles Mapping***

Kyndryl Resiliency Orchestration Admin user can assign RO roles to the allowed list of AD groups using **AD Groups to RO Roles Mapping** page. All the allowed list of AD groups and RO roles (default and custom roles) are shown. These RO roles can be assigned to each AD group.

- Only one RO role can be assigned to one AD group.
- Any user who is part of the AD group inherits the right privileges that are part of the role assigned when they log in.

Follow the below procedure to do the AD Group to RO role mapping.

1. Click **Admin**.
2. Scroll down to **AD Groups to Kyndryl Resiliency Orchestration Roles Mapping** section.
3. Click the **Go to AD Groups to Kyndryl Resiliency Orchestration Roles Mapping** link. The **AD Groups to RO Roles Mapping** page appears as shown in below figure.



AD Configuration

AD Groups	Recovery Group	Application Group
STGRP		

4. Select the organization from the Subscriber drop-down and the required role from the RO Roles drop-down for each of the AD Groups.
5. Click Save to save your selection.

The AD group to Kyndryl RO role assignment details are saved.

The RO role assignment changes would take effect for all users (including currently logged in user) of the AD group. The change is triggered for all users if any user in the AD group logs in after the changes are saved.

Note – If users are part of multiple AD Groups which have different RO roles mapped, then the users cannot login to Kyndryl Resiliency Orchestration.

Note -

- Select the Subscriber for which AD is being configured.
- The password length supported from Kyndryl RO GUI is 256 characters. Enter the password as per what is supported and configured in Windows Active Directory.
- If the anonymous directory lookup is enabled, then the user configured for accessing the directory server will still be able to lookup the directory even if the given credentials are wrong.
- When AD Group based authentication is chosen, **Edit User Details** page in Kyndryl Resiliency Orchestration does not allow RO Role or RO Group assignment. The RO Role and RO Group assigned to the AD Group is applicable to all the users that are part of the AD Group.
- In case a user is created in basic mode (RO Authenticate and Authorize) however, at a later date the user management mode is changed to AD (AD Authenticate and Authorize) then login is blocked for the user in case the user already exists in the AD server. This is a limitation. The workaround would be, to delete this user from the basic RO mode before switching to AD mode.

Removing AD Groups from the Allowlist

Follow the procedure below to AD groups from the allowlist–

1. Click **Admin** on the navigation bar. The Administration page appears.
2. Scroll down to the **Directory Server Details** and click **Go to Directory Server Details**. The **External Directory Server Details** page appears.
3. In the **Allowed list of AD groups section**, select the AD group to be removed and then click **Delete**.

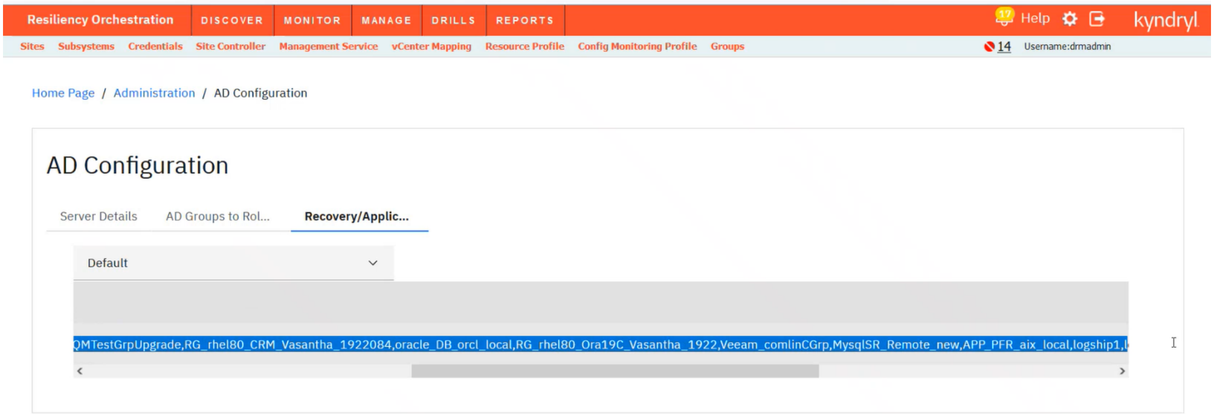
Recovery/Application Group Assigning to AD Groups

The functionality to assign Resiliency Orchestration Recovery Groups (RG) or Application Groups (AG) to allowed list of AD groups, is provided in **RG/AG assigning to AD Groups** page.

Follow the below procedure to assign RG/AGs to AD Groups –

1. Click **Admin**.
2. Scroll down to **Recovery/Application Group Assigning to AD Groups** section.
3. Click the **Go to Recovery/Application Group Assigning to AD Groups** link. The **RG/AG Assigning to AD Groups** page appears as shown in below figure.

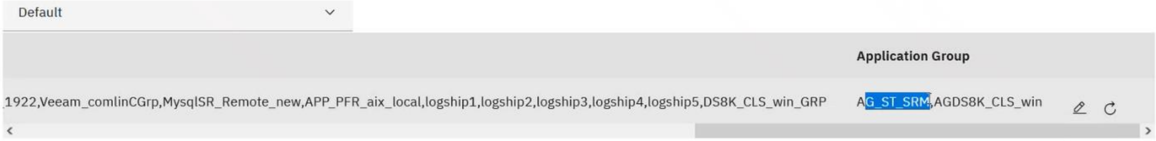
~~4.~~ Select the Organisation, from the **Subscribers** drop-down as shown in the image below.



AD Configuration

Default

QMTestGrpUpgrade,RG_rhel80_CRM_Vasantha_1922084,oracle_DB_orcl_local,RG_rhel80_Ora19C_Vasantha_1922,Veeam_comlinCGrp,MysqlSR_Remote_new,APP_PFR_aix_local,logship1,l



Default

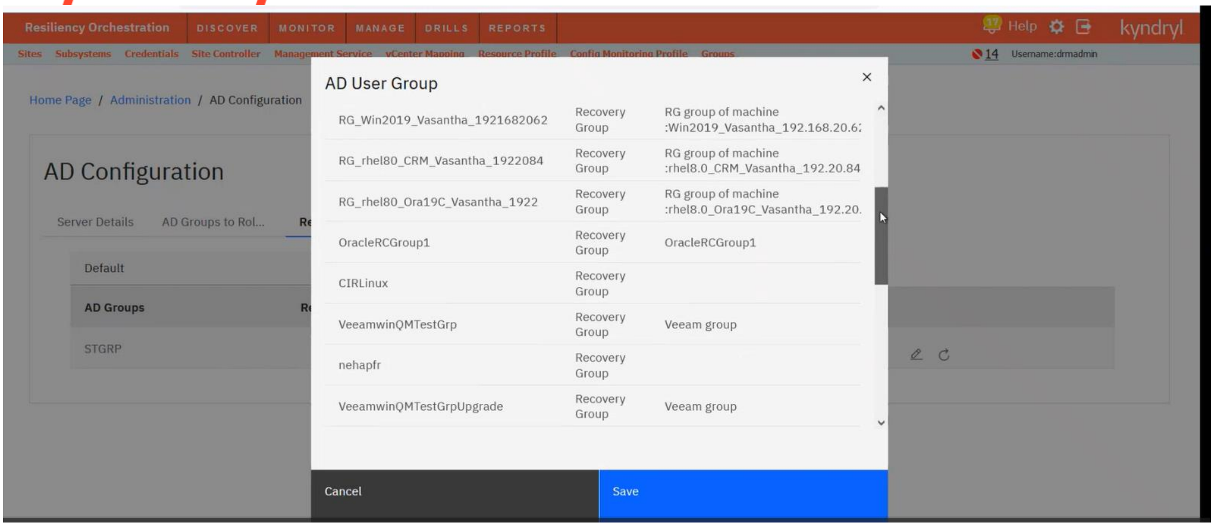
	Application Group
1922,Veeam_comlinCGrp,MysqlSR_Remote_new,APP_PFR_aix_local,logship1,logship2,logship3,logship4,logship5,DS8K_CLS_win_GRP	AG_ST_SRM,AGDS8K_CLS_win

Note -

- In the **RG/AG Assigning to AD Groups** page, displays all the AD groups for the logged in user are shown in a tabular view with assigned RGs and AGs against each AD group. The user can see and assign only those RO groups for which the user has access to.
- Each AD group has Edit and Reset actions.

- While the reset button removes the AG/RGs assigned to the AD Group, the edit button takes you to **AD User Group: <AD Group Name>** page where RG/AGs can be selected and assigned to AD groups.

~~5.~~ Click the edit button . The AD User Group: <AD Group Name> page appears as shown in below figure.



RG_Win2019_Vasantha_1921682062	Recovery Group	RG group of machine :Win2019_Vasantha_192.168.20.6:
RG_rhel80_CRM_Vasantha_1922084	Recovery Group	RG group of machine :rhel8.0_CRM_Vasantha_192.20.84
RG_rhel80_Ora19C_Vasantha_1922	Recovery Group	RG group of machine :rhel8.0_Ora19C_Vasantha_192.20.
OracleRCGroup1	Recovery Group	OracleRCGroup1
CIRLinux	Recovery Group	
VeeamwinQMTestGrp	Recovery Group	Veeam group
nehapfr	Recovery Group	
VeeamwinQMTestGrpUpgrade	Recovery Group	Veeam group

This page has a tabular view that shows list of available RGs, AGs with columns RO group name, group type, and group description.

6. Select the RG/AGs that are required using the **Action** check box provided in each row.
7. It is auto saved from selection.

The AD group to RG/AG assignment details are saved. These changes would take effect for all users (including currently logged in user) of the AD group. The change is triggered for all users if any user in the AD group logs in after the changes are saved.

If AD groups are assigned with one or more AGs, then the users of that AD groups get access to all RGs that are part of the assigned AGs.

AD Query

Role names are read using the query **(&(objectClass=Kyndryl-role))** and searching for attribute name and searching for roles in the organizational unit **ou=Roles.**

Users associated with the role are read by reading the attribute member from the role.

User login name (used for authentication in Kyndryl Resiliency Orchestration) is read using the query **(&(objectClass=user)(cn=<common name of user>))**. The common name of user is obtained from the role as mentioned previously.

Division of the User Management System

The User Management System will use an LDAP/ Active Directory server in the back end for authentication and authorization (which includes user creation, role creation and user-role mapping management).

The following roles should be made available in the external server for authorization purposes of Kyndryl Resiliency Orchestration:

Role Name	Description
NOTIFICATION MEMBER	Only notification allowed. Login not allowed
OPERATOR	Can view everything in Monitor/Manage/Reports/Discover/Agents/Admin. The privileges on the OPERATOR can be further enhanced by the custom roles created using the feature-operation mentioned in the next table.
ADMINISTRATOR	All applicable operations on all features except Create/Edit other users.
SUPER ADMINISTRATOR	All applicable operations on all features.

Note:

> User account **support** will be provided for in Advanced User Management system also. The authentication for the user account **support** will be done against Kyndryl Resiliency Orchestration. If later the User Management system mode is modified to Basic User Management, then the **ResiliencyOrchestrationAdmin** user will also be available and will be authenticated against the Kyndryl Resiliency Orchestration.

In the LDAP/ Active Directory server, 4 roles as present in the Basic User Management System should be created. They will function as per the Basic User Management System. The difference here lies with the OPERATOR role. This role can be enhanced with other custom roles.

These custom roles will contain attributes which relate to the following feature operations:

Features/Operations	Execute [Includes Start/Stop]	Edit [Includes Create/Edit/Delete]	Additional Privileges
Switchback	X	X	Will also include REPL-EXECUTE
Switchover	X	X	Will also include REPL-EXECUTE
Failover	X	X	Will also include REPL-EXECUTE
Fallback	X	X	Will also include REPL-EXECUTE
FallbackResync	X	X	Will also include REPL-EXECUTE
NormalCopy	X	X	Will also include REPL-EXECUTE
NormalFullCopy	X	X	Will also include REPL-EXECUTE
ReverseNormalCopy	X	X	Will also include REPL-EXECUTE
Policy	X	X	-NA-

Features/Operations	Execute [Includes Start/Stop]	Edit [Includes Create/Edit/Delete]	Additional Privileges
BP	X	X	-NA-
Tests[NEWDRILL]	X	X	-NA-
Groups		X	Will also include the following: 1 SOLUTION_DETAILS-EDIT 2 GROUP_NOTIFICATION-EDIT 3 GROUP_LICENSE-EDIT 4 GROUP_EVENTS-EDIT 5 RPO-EDIT 6 RTO-EDIT 7 DATALAG-EDIT

The custom roles will have a set of attributes which correspond to a combination of the feature-operation mentioned in the table above. Assigning these attributes a value of TRUE/FALSE will create a customized role. There will be no change in the GUI for supporting role creation/customization and user management.

Note -

A user can also be assigned a custom role directly without being assigned an OPERATOR role. By default the user will be assigned OPERATOR privileges internally and will be allowed to log in and do operations pertaining to the custom role assigned.

For the **User Management System**, Kyndryl Resiliency Orchestration will not ship with an LDAP/ AD server. The server will have to configured/ provided by the customer at the site.

Testing of this module in Development and SQA environments will be done using OpenLDAP [or 389 Directory Server in Fedora] on Linux and Active Directory on Windows.

On installation of Kyndryl Resiliency Orchestration, a choice will be provided in the installer on whether the Basic or Advanced User Management System has to be used.

The **support** user provided will function as in the previous releases.

Note -

The **ResiliencyOrchestrationAdmin** user need not be created on the external server in User Management mode. The product should function even without the ResiliencyOrchestrationAdmin user account being created on the external server.

Any of the internal processes (like executing policy workflows, scheduled workflows, replication workflows etc) which are using the **ResiliencyOrchestrationAdmin** user by default will be modified to take **system** as the user. So, in the audit log/ reports the user who triggered the workflow will be shown as **system** [if audit log is applicable] which gives a better understanding to the user since this will also avoid the confusion of whether the workflow was triggered by somebody logging in as **ResiliencyOrchestrationAdmin** or automatically started by the system.

For any user that is created in the external server, a record is maintained for that user for its preferences with respect to the Kyndryl Resiliency Orchestration. If the user name is modified, the modified user name will be treated as a new user and the record for the old user name will not be accessed on login. If the user is deleted in the external system, the record for the deleted user in Kyndryl Resiliency Orchestration will still remain as there is no way to indicate back to the Resiliency Orchestration server that the user is deleted.

Features and Relevant Operations to be Handled

Features/ Operations	Create	Read	Update/ Edit	Delete	Execute	Terminate
Agents		X	X		X	X
Backup		X	X		X	
BP	X	X	X	X	X	X
Credentials	X	X	X	X	X	
Datalag		X	X		X	
Failover		X	X		X	X
Fallback		X	X		X	X
FallbackResync		X	X		X	X
Groups	X	X	X	X	X	
Group_Events		X	X		X	
Group_License		X	X		X	
LICENSE		X	X			
Logs		X				
NEWDRILL	X	X	X	X		X
NormalCopy		X	X			X
NormalFullCopy		X	X			X
Group_Notification	X	X	X	X		
Operational_History		X	X			
Policy		X	X			X
REPL		X	X			X
Reports		X				
ReverseNormalCopy		X	X			X
RPO		X	X			X
RTO		X	X			X
Server_Failover		X	X			
Sites	X	X	X	X		
Solution_Details		X	X			
Subsystems	X	X	X	X		
Switchback		X	X			X
Switchover		X	X			X
System_Events		X	X			
System_Preferences		X	X			
Users	X	X	X	X		
Directory_Server		X	X			
Server_Notification	X	X	X	X		

Note -

In User Management mode, if a user is modified/ deleted in the LDAP/ AD server, then the cache on the Server will be refreshed only if any of the following scenarios occur:

- On restart of the Resiliency Orchestration Server.
- When any user logs in successfully.

Known Limitations

1. **User Role Management:** For any changes (such as, add/ delete roles or users) made in the LDAP/ AD server, in order that these changes take effect in user roles, the user has to logout and then login to the Kyndryl Resiliency Orchestration Server.
2. **Manual deletion of entries from user role's in LDAP server:** In LDAP server, if a user having a role is deleted, then the corresponding entry from the role must also be deleted. Currently LDAP does not delete the entry in the role for the user if that user is deleted. The deletion has to be done manually.
3. **User Management mode:** If a user account is attached to an empty role (a role without any attributes or attributes set to false), the user will not be allowed to login. However other users will be able to see the empty role attached to that user in the **User listing** page.

Listing Configured Users

Users can perform specific functions based on the assigned privileges.

Kyndryl Resiliency Orchestration users are categorized at the time of user creation. Users with Super Administrator and Administrator privileges can monitor and manage the Groups, users, components, agents etc. Users with Operator privileges can only monitor the Groups.

The following table lists the types of users with the privileges:

Types of Users	Description
Super Administrator	The Super Administrator is a user who has privileges to access all aspects of the configuration and operation of the Kyndryl Resiliency Orchestration. With Super Administrator privilege, you can: ▪ Manage and monitor all the Groups under Kyndryl Resiliency Orchestration. ▪ Create, modify, and delete different types of users supported by Kyndryl Resiliency Orchestration and their passwords. ▪ Create, modify, and delete Groups. ▪ Assign Groups to the users.

Types of Users	Description
Administrator	An administrator has privileges only with respect to the Group(s) assigned to him. With Administrator privilege, you can: ▪ Cannot create, delete or modify users. ▪ Create and modify Groups. ▪ Can delete Groups that belongs to the Administrator. ▪ Not assign Groups to the users.
Operator	An Operator can only monitor the Group that has been assigned except for the test exercises. Operator can view the report list, agents list, users list etc.
Notification Member	Notification members are the point of contact for recovery at the time of disaster. The notification member does not have any login access.
Internal Support	

You can view the list of users configured to Kyndryl Resiliency Orchestration Server, by performing the following steps:

1. Click on **Admin** on the navigation bar. The **Administration** page appears.
2. Click on the **User Summary**. The **Users** page appears with the following:

Column	Description
User name	Displays the name of the user.
Login name	Displays the login name of the user.
User type	Displays the type of the user. The user types are Super Administrator, Administrator, Operator and Notification Member.
✎	Click this icon to edit the user details.
🗑	Click this icon to delete the user.

Role-Based Access Control

Role-based access control (RBAC) is a method of restricting and streaming authorization roles of individual users for Kyndryl Resiliency Orchestration application. RBAC lets users have access rights only to the features they need to perform their assigned roles and prevents them from accessing features that doesn't pertain to them.

Note: In Hybrid as well as AD mode, roles have to be assigned to individual groups and not to users defined in AD.

With this release a new "Publisher " privilege has been added. This is different from the workflow "Creator" privilege. In the create roles table a new column is available for those with "Publisher " privilege.

DRMAdmin or any other super user has this privilege to publish and can assign it to other users as required. So a segregation of "Creator" and "Publisher " privilege has been done under Role management. Now "Creator" of the Workflow and "Publisher " of the Workflow can be two different users.

Creating a Custom Role when using RO for Authorization

You can create customized roles on the Role Management page in Kyndryl Resiliency Orchestration application and assign it to a user. The roles can be created for privileges such as Create, Read, Update, Delete (CRUD) operations mapped to all available features.

Once a customized role is assigned to a user, all privileges defined in this user role will be available to the user. To create a customized user role, follow the steps below.

Note:

- ROLE_MANAGER feature has been introduced to create, edit and delete custom roles. Only super administrator is authorized for these operations.
- By default, the create custom role page does not list the role manager feature for super administration. This is to prevent creation/update of custom roles with super administration any custom role needs to be created with this access, then replace content of CreateCustomRole.json with CreateCustomRoleWithRoleManager.json file which will be available in $EAMSROOT/templates/CUSTOMROLE path.

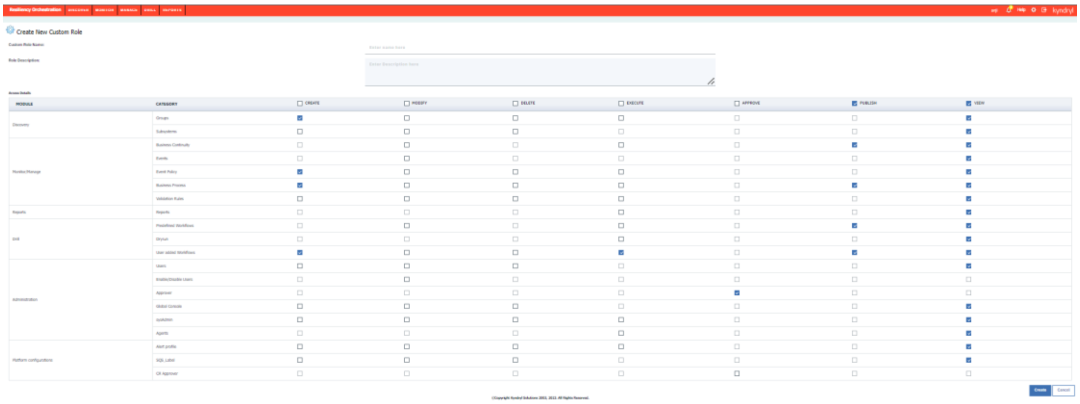
1. On the Kyndryl Resiliency Orchestration home page, click on the **Admin** link located at the right top corner to open **Administration** page.
2. On the **Administration Page**, click Go to **Custom Role Management** page. **Kyndryl Resiliency Orchestration Roles** page opens as shown below.

Note: Following are default user roles available on the page.

- SUPER ADMINISTRATOR,
- ADMINISTRATOR, OPERATOR,
- NOTIFICATION-MEMBER,
- OPERATOR

These default roles are not editable or removable. The privileges assigned to these roles are also not editable or removable.

3. Click **Add Custom Role** link. **Create New Custom Role** page appears.



Create New Custom Role

Custom Role Name: Enter name here

Role Description: Enter Description here

Access Details

MODULE	CATEGORY	☐ CREATE	☐ MODIFY	☐ DELETE	☐ EXECUTE	☐ APPROVE	☑ PUBLISH	☑ VIEW
Discovery	Groups	☑	☐	☐	☐	☐	☐	☑
	Subsystems	☐	☐	☐	☐	☐	☐	☑
Monitor/Manage	Business Continuity	☐	☐	☐	☐	☐	☑	☑
	Events	☐	☐	☐	☐	☐	☐	☑
	Event Policy	☑	☐	☐	☐	☐	☐	☑
	Business Process	☑	☐	☐	☐	☐	☑	☑
	Validation Rules	☐	☐	☐	☐	☐	☐	☑
Reports	Reports	☐	☐	☐	☐	☐	☐	☑
Drill	Predefined Workflows	☐	☐	☐	☐	☐	☑	☑
	Dryrun	☐	☐	☐	☐	☐	☐	☑
	User added Workflows	☑	☐	☐	☑	☐	☑	☑
Administration	Users	☐	☐	☐	☐	☐	☐	☑
	Enable/Disable Users	☐	☐	☐	☐	☐	☐	☐
	Approver	☐	☐	☐	☐	☑	☐	☐
	Global Console	☐	☐	☐	☐	☐	☐	☑
	sysAdmin	☐	☐	☐	☐	☐	☐	☑
	Agents	☐	☐	☐	☐	☐	☐	☑
Platform configurations	Alert profile	☐	☐	☐	☐	☐	☐	☑
	SQL Label	☐	☐	☐	☐	☐	☐	☑
	CR Approver	☐	☐	☐	☐	☐	☐	☐

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved.

By default, the Operator privileges are enabled for all roles. It can be edited based on user preferences.

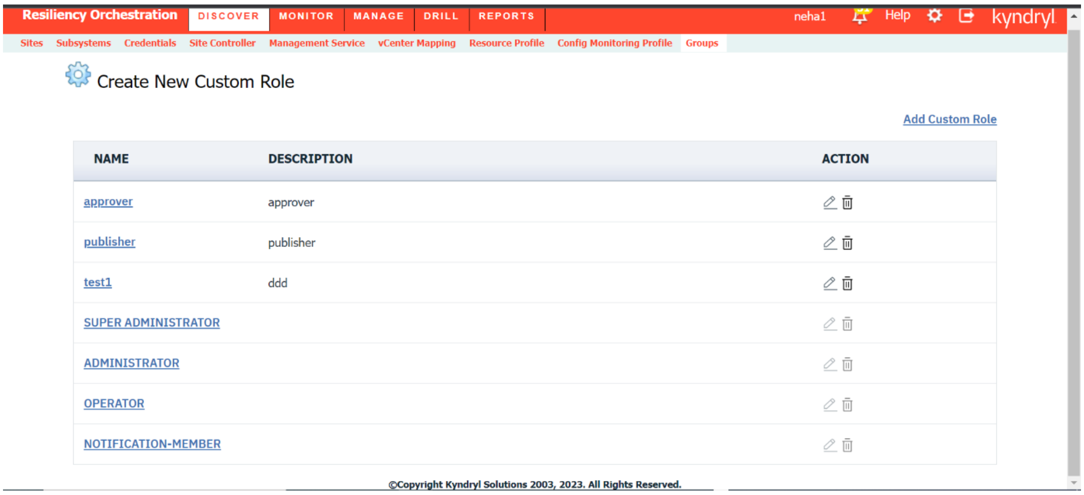
If the check box for a particular operation is grayed out, then the operation is not supported for the respective features.

Field	Description
Custom Role Name	Enter the name of the custom role you would want to create. **Note:** The role name can be 24 character long and can have underscore as special symbol.
Role Description	Enter the description of the custom role you would want to create.
CREATE	User has the following privileges: Create, Bulk Upload, Import, Export, Import Workflow, Add Action, and Insert Action for the following modules. • Discover • Monitor/Manage • Reports • Drill • Administration • Platform Configuration
MODIFY	User has the following privileges: Modify, edit, Update, Manage, Unmanage, Change Continuity, Edit name, Edit KV box, Edit, Singe Step Enable, Edit single step disable, Edit Skip Enable, Edit Skip Disable, Edit Action Properties, Edit Approver list, Edit Schedule, Enable User, and Disable User.
DELETE	The user has the privilege of deleting a custom role.
EXECUTE	User has the following privileges: Start, Stop, Terminate, Stop, on Restart, Resume on Restart, Resume , Retry, Close Event, CR Accept, CR Revert, Inprogress Event, Scannow, Trigger, and Edit Userinput.
APPROVE	User has the following privileges: Approve, Reject, and workflow and events.
PUBLISH	User can publish draft workflows
VIEW	This enabled by default for all users and allows users to view all the modules. The user has the following privileges: Read, List, and Status. **Note:** The checkbox for this field is not editable.

The following is the category/feature mapping.

Module	Category	Feature List
Discover	Groups	RPO, RTO, Datalag, Groups, Application Template, Group License, and Solution Details.
	Subsystems	Sites, Subsystems, Credentials, Common Component, vCenter Mapping, Resource Profile, and DR Profile.
Monitor/Manage	Business Continuity	NormalFullCopy, NormalCopy, ReverseNormalCopy, Failover, Fallback, FallbackResync, and Cyber DR Recovery.
	Events	Group Events, Group Notification, and SystemEvents.
	Event Policy	Policy
	Business Process	BP and REPL
	Validation Rules	Validation Task and Validation Reports.
Reports	Reports	User activity report, audit log report, Advanced_Reports, and Reports.
Drill	Predefined Workflows	Switchover, Switchback, FOTE, StartAppPR, StartAppDR, StopAppPR, and StopAppDR.
	Dryrun	PreCheck
	User added Workflows	NEWDRILL
Administration	Users	Users
	Enable/Disable Users	Enable/Disable User
	Approver	Approver
	Global Console	Global Console
	sysAdmin	Server Notification, System Preferences, Logs, Backup, Server Failover, Directory Server, Operational History, License—Mappings, and Site Ticker—Group Label/System Events/Organization/Role Manager.
	Agents	Agents
Platform configurations	Alert profile	Configuration Profile
	SQS_Label	SQS Label
	CR Approver	CR Approver

Note: After a custom role has been created, it is available in edit user and create user pages as shown in the example figure below. For more information on creating a new user refer to the topic **Adding Users**.



Create New Custom Role

NAME	DESCRIPTION	ACTION
approver	approver	✎ 🗑
publisher	publisher	✎ 🗑
test1	ddd	✎ 🗑
SUPER ADMINISTRATOR		✎ 🗑
ADMINISTRATOR		✎ 🗑
OPERATOR		✎ 🗑
NOTIFICATION-MEMBER		✎ 🗑

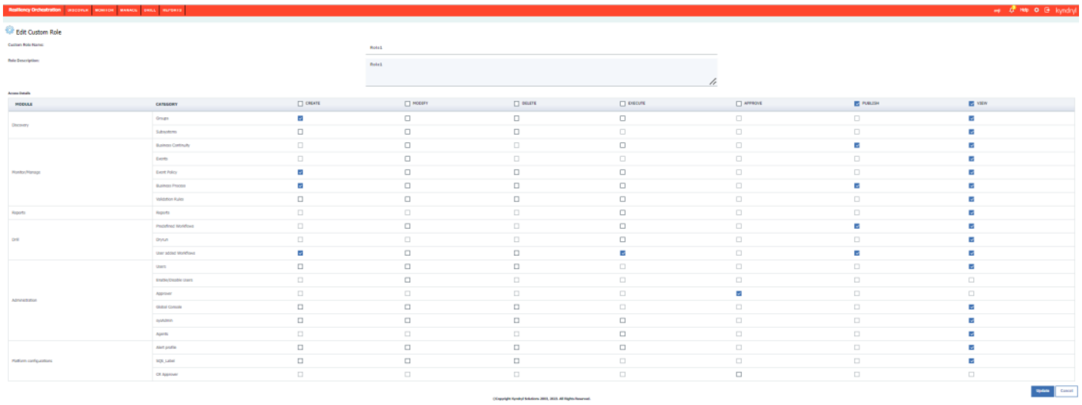
©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved.

Editing a Custom Role

To edit a custom role in Kyndryl Resiliency Orchestration application, perform the following steps.

1. On the Kyndryl Resiliency Orchestration home page, click the **Admin** link located at the right top corner to open **Administration** page.
2. On the Administration Page, click Go to **Custom Role Management** page. **Kyndryl Resiliency Orchestration Roles** page appears as shown below.

3. Click the edit icon ✎ . **Edit Custom Role** page is displayed for the selected custom role.



Edit Custom Role

Custom Role Name: Role1

Role Description: Role1

Access Details

MODULE	CATEGORY	☐ CREATE	☐ MODIFY	☐ DELETE	☐ EXECUTE	☐ APPROVE	☑ PUBLISH	☑ VIEW
Discovery	Groups	☑	☐	☐	☐	☐	☐	☑
	Subsystems	☐	☐	☐	☐	☐	☐	☑
Monitor/Manage	Business Continuity	☐	☐	☐	☐	☐	☑	☑
	Events	☐	☐	☐	☐	☐	☐	☑
	Event Policy	☑	☐	☐	☐	☐	☐	☑
	Business Process	☑	☐	☐	☐	☐	☑	☑
	Validation Rules	☐	☐	☐	☐	☐	☐	☑
Reports	Reports	☐	☐	☐	☐	☐	☐	☑
Drill	Predefined Workflows	☐	☐	☐	☐	☐	☑	☑
	Dryrun	☐	☐	☐	☐	☐	☐	☑
	User added Workflows	☑	☐	☐	☑	☐	☑	☑
Administration	Users	☐	☐	☐	☐	☐	☐	☑
	Enable/Disable Users	☐	☐	☐	☐	☐	☐	☐
	Approver	☐	☐	☐	☐	☑	☐	☐
	Global Console	☐	☐	☐	☐	☐	☐	☑
	sysAdmin	☐	☐	☐	☐	☐	☐	☑
	Agents	☐	☐	☐	☐	☐	☐	☑
Platform configurations	Alert profile	☐	☐	☐	☐	☐	☐	☑
	SQL_Label	☐	☐	☐	☐	☐	☐	☑
	CR Approver	☐	☐	☐	☐	☐	☐	☐

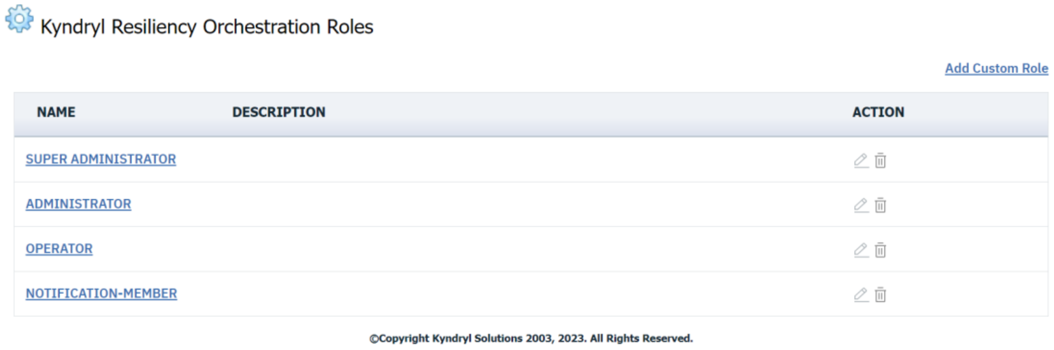
©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved.

4. Make the required changes and click **Update** button.

Deleting a Custom User Role

To delete a custom role in Kyndryl Resiliency Orchestration application, perform the following steps.

1. On the Kyndryl Resiliency Orchestration home page, click the **Admin** link located at the right top corner to open **Administration** page.
2. On the Administration Page, click Go to **Custom Role Management** page. Kyndryl Resiliency Orchestration Roles page opens as shown below.



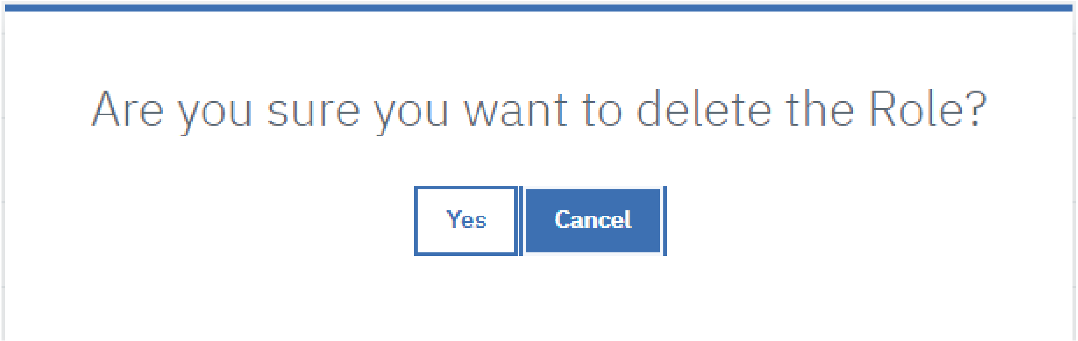
Kyndryl Resiliency Orchestration Roles

Add Custom Role

NAME	DESCRIPTION	ACTION
SUPER ADMINISTRATOR		✎ 🗑
ADMINISTRATOR		✎ 🗑
OPERATOR		✎ 🗑
NOTIFICATION-MEMBER		✎ 🗑

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved.

3. Click the delete icon 🗑. Confirmation dialog box appears as show below.



Are you sure you want to delete the Role?

4. Click **Yes** button to confirm the deletion or click **Cancel** to abort.

Appendix

Installing the schmmgmt tool on Active Directory machine

It applies to:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2003 with SP1
- Windows Server 2003 with SP2

The steps followed to install the Active Directory Schema snap-in are:

1. Open Command Prompt.
2. Type regsvr32 schmmgmt.dll

This command will register **Schmmgmt.dll** on your computer. For more information on using regsvr32, see Related Documents.

3. Click **Start** > **Run**, type **mmc /a**, and click **OK**.
4. On the File menu, click **Add/Remove Snap-in**, and then click **Add**.
5. Under Available Standalone Snap-ins, double-click **Active Directory Schema.** Click **Close** and click **OK**.
6. To save this console, on the File menu, click **Save**.
7. In Save in, point to the systemroot\system32 directory.
8. In File name, type **schmmgmt.msc**, and then click **Save**.
9. To create a shortcut on your Start menu:
    - Right-click **Start** and click **Open All Users**. Double-click the programs folder and then double-click the **Administrative Tools** folder.
    - On the File menu, point to New, and then click **Shortcut**.
    - In the Create Shortcut Wizard, in Type the location of the item, type **schmmgmt.msc**, and then click **Next**.
    - On the Select a Title for the program page, in Type a name for this shortcut, type Active Directory Schema, and then click **Finish**.

    Caution:

    Modifying the schema is an advanced operation best performed by experienced programmers and system administrators. For detailed information about modifying the schema, see the Active Directory programmer's Guide at the Microsoft Web site.

    Note:

    To perform this procedure, you must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority. As a security best practice, consider using Run as to perform this procedure. For more information, see Default local groups, Default groups, and Using Run as.

You can also run the Active Directory Schema snap-in from a computer running Windows XP Professional. Simply install the Windows Server 2003 Administration Tools Pack on the computer, and then complete step 9 above.

The Windows Server 2003 Administration Tools Pack cannot be installed on computers running Windows 2000 Professional or Windows 2000 Server.

Installing the ADSI Edit tool on Active Directory machine

It applies to:

- Windows SBS 2008
- Windows Server 2003

- Windows Server 2003 R2
- Windows Server 2003 with SP1
- Windows Server 2003 with SP2
- Windows Server 2008
- Windows Server 2008 R2

Active Directory® Service Interfaces Editor (ADSI Edit) is a Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory. ADSI Edit (adsiedit.msc) provides a view of every object and attribute in an Active Directory forest. You can use ADSI Edit to query, view, and edit attributes that are not exposed through other Active Directory Microsoft Management Console (MMC) snap-ins: Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and Active Directory Schema.

This topic includes the following sections:

- Installing ADSI Edit
- Using ADSI Edit

Installing ADSI Edit

To install ADSI Edit on computers running Windows Server® 2003 or Windows® XP operating systems, install Windows Server 2003 Support Tools from the Windows Server 2003 product CD or from the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=100114). For more information about how to install Windows Support Tools from the product CD, see Install Windows Support Tools (http://go.microsoft.com/fwlink/?LinkId=62270).

On servers running Windows Server 2008 or Windows Server 2008 R2, ADSI Edit is installed when you install the Active Directory Domain Services (AD DS) role to make a server a domain controller. You can also install Windows Server 2008 Remote Server Administration Tools (RSAT) on domain member servers or stand-alone servers. For specific instructions, see Installing or Removing the Remote Server Administration Tools Pack (http://go.microsoft.com/fwlink/?LinkId=143345).

To install ADSI Edit on computers running Windows Vista® with Service Pack 1 (SP1) or Windows 7, you must install RSAT. For more information and to download RSAT, see article 941314 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkID=116179).

Note -

- **Adsiedit.msc** will not run unless the **Adsiedit.dll** file is registered. This happens automatically if the support tools are installed. However, if the support tool files are copied instead of installed, you must run the **regsvr32** command to register **Adsiedit.dll** before you run the **Adsiedit.msc** snap-in. To register **adsiedit.dll**, type the following command (you must navigate to the directory containing the **adsiedit.dll** file): **regsvr32 adsiedit.dll**
- You can run ADSI Edit from a client computer or server. The computer does not have to be a member of a domain. However, to see domain objects using **Adsiedit.msc**, you must have the rights to view the Active Directory domain that you connect to. By default, members of the Domain Users group have these rights.

To modify objects using **ADSIEdit**, you must have at least the Edit permission on the Active Directory objects that you want to change. By default, members of the Domain **Admins** group have this permission.

Using ADSI Edit

ADSI Edit (**Adsiedit.msc**) is an MMC snap-in. You can add the snap-in to any .msc file through the Add/Remove Snap-in menu option in MMC, or just open the **Adsiedit.msc** file from Windows Explorer. The following figure illustrates the ADSI Edit interface. In the console tree on the left, you can see the major partitions Domain, Configuration, and Schema. The figure shows the Built-in container of the Contoso.com domain selected. In the details pane on the right, you can see the Built-in groups of Active Directory.

Note:

- **Adsiedit.msc** automatically attempts to load the current domain to which the user is logged on. If the computer is installed in a workgroup or otherwise not logged on to a domain, the message "The specified domain does not exist" displays repeatedly. To resolve this issue, you may want to open an MMC, add the ADSI Edit snap-in, make connections as appropriate, and then save the console file.

Notifications

Configuring Notifications

Notifications lists the users categorized under various notification names. You can configure notifications to be sent to a selected set of users on occurrence of an event. These users can only receive the notifications, but, cannot login into Kyndryl Resiliency Orchestration.

Note – In case of multitenant users, the Alert Notification related features in Resiliency Orchestration are visible/available for configuration only to certain users based on their roles. Refer the table below for information regarding the notification features and the visibility/availability for multitenant users based on their roles.

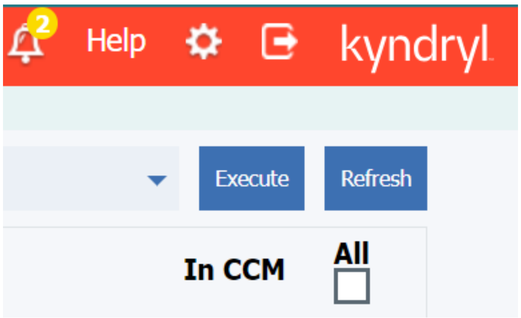
Feature	Service Provider(SP) Admin	Service Provider(SP) Operator	Tenant Admin	Tenant Operator
Admin Page				
Go to Notification Link	✓	✓	✓	✗
Summary - Mail Server	✓	✓	✗	✗
Summary - Total Number Of Notification Lists	✓ Sum of all tenants incl. its own	✓ Sum of all tenants incl. its own	✓ Sum of tenant specific notifications	✓ Sum of tenant specific notifications

Summary - SNMP Trap Forwarder not Configured	✓	✓	✗	✗
Notification Details Page				
Email Server Details	✓	✓	✗	✗
Notification List	✓ Lists all	✓ Lists all	✓ Lists only tenant specific	a Lists only tenant specific
Notifications - Right side panel	✓	✗	Only the Add Notification List link is visible	✗
Notification List - Click on List Name	✓ Lists all names	✓ Lists all names	✓ Lists only tenant specific names	✓ Lists only tenant specific names
Notification List - Edit	✓ Edit all lists	✗	✓ Edit only tenant specific lists	✗
Notification List - Delete	✓ Delete all lists	✗	✓ Delete only tenant specific lists	✗
SNMP Trap Forwarder List	✓	✓	✗	✗
SNMP Trap Forwarder List - Click on Name	✓ Opens in Edit mode	✓ Opens in View mode	✗	✗
SNMP Trap Forwarder List - Edit	✓ Opens in Edit mode	✗	✗	✗
SNMP Trap Forwarder List - Delete	✓ Delete all	✗	✗	✗
Configure Email Server	✓	✗	✗	✗
Add Notification List	✓ Lists all Organizations	✗	✓ Lists only tenant specific	✗

			organizations, and should be able to create	
Add Notification List - Right panel	✓ Lists all Organizations	✓ Lists all Organizations	✓ Lists only tenant specific notifications	✓ Lists only tenant specific notifications
Add SNMP Trap Forwarder	✓	✗	✗	✗
Add SNMP Trap Forwarder - Right panel Create/view/edit/delete	✓ Lists all	✓ Lists all	✗	✗
Add Notification List - Listing Organization	✓ Lists all	✗	✓ Lists only tenant specific organizations	✓ Read-only access
Add Notification List - Users Listing	✓ Lists all users of selected organization	✗	✓ Lists all users of logged in user's organization	✓ Lists all users of logged in user's organization
SNMP Trap Forwarder - Select Groups	✓ Lists all groups	✓ Lists all groups	✗	✗
Access to Notification page	✓	✓	✓	✓
Alert Notifications				
Feature	**Service Provider(SP) Admin**	**Service Provider(SP) Operator**	**Tenant Admin**	**Tenant Operator**
Alert Count	✓ Lists all the RGs	✓ Lists all the RGs	✓ Lists RGs belonging to tenant and assigned to it	✓ Of RGs belonging to tenant and assigned to it
Alert Group Filter	✓ Lists all the RGs	✓ Lists all the RGs	✓ Lists RGs belonging to tenant and	✓ Lists RGs belonging to tenant

			assigned to it	and assigned to it
Listing Alert Notification	✓ Alerts of all RGs	✓ Alerts of all RGs	✓ Alerts of RGs belonging to its tenant and assigned to it	✓ Alerts of RGs belonging to its tenant and assigned to it
Execute Button	✓ *	✗	✗	✗
Select Drop-down	✓ *	✗	✗	✗
Alert Selection	✓ *	✗	✗	✗

* Requires *System_Event* update RBAC privilege. This privilege exists with SP Admin by default.



In the above image, click on the Bell icon to see Config Exposures option which will post the sum of all the alerts, based on the RGs the user has access to.

For Service Provider Admin the number will be the total number of alerts, of all the RGs that are discovered, and Service Provider has access to.

Note:

- The Tenant can view the total number of alerts, of all the RGs that belong to the tenant and the tenant user has access to.
- **Only the Service Provider Admin can execute the actions on these Alerts.**
- **The alerts are listed only for the RGs that the user has access to.**

The notifications are sent to the users through three modes of communications. They are:

- **Email Notifications**
- **SMS Notifications**

- **SNMP Notifications**

To view the list of members included in the notification list, perform the following steps:

1. Click **Admin** on the navigation bar. The **Administration** page appears.
2. Click on the **Notification Summary**. The **Notification Summary** section displays the following information –
    a. **Email Server Details**: Details of E-mail server configuration for sending and receiving E-mails.

    b. **Notification List:** Provides information on configured list and its members with options to edit or delete respective notification list.

    The notification lists belonging to/associated with the Organization to which the logged in user belongs to are displayed.

    c. **SNMP Trap Forwarder List**: Provides information on configured SNMP Trap Forwarder list with an option to delete respective SNMP Trap Forwarder list.

Note – In a multiple organization mode (multitenant mode), the Service Provider and Tenant organization admin users (SPAdmin and TenantAdmin) will be able to create/edit/view/delete Notification lists. The Service Provider and Tenant organization operator users (SPOperator and TenantOperator) will be able to view the Notification lists, they cannot create/edit/delete Notification lists.

There is no access or visibility of E-mail server and SNMP Trap Forwarder configuration for Tenants. Tenants can see only notification list details.

E-mail Notification

Each event is associated with a member or group of members. The notification regarding the event is automatically sent to the e-mail address of the user. Email notification is set up through e-mail server configuration.

When a BCO is initiated on an AG, notifications are sent to users in the notification list of the AG. Following is a sample notification sent to the users configured to an AG and its associated RG's.

Subject:

Resiliency Orchestration: testAG1: Failover started at 2005-05-10 21:10:49.74

Notification:

Notification List: Test_NL1,

Group Details:

…Name: testAG1

Description: this is testAG1

Type: APPLICATION GROUP

Current Status: MANAGED, INACTIVE

Operational Details:

Continuity Operation: Failover

Status: Failover started

Start Time: 2005-05-10 21:10:49.74

End Time: -

Actions to be performed by User: None

SMS Notification

SMS notification process is similar to the E-mail notification except for the notification method. Here, you will be notified through SMS regarding an event. The SMS is sent to your cell phone.

The information regarding the failure or success of Application Events, Infrastructure events and Replication events is escalated to the respective users through Notifications.

SNMP Notification

SNMP notification provides the ability to receive notifications in the form of SNMP traps through SNMP Trap forwarder.

Users with Administrator and Super Administrator privileges can use this type of notification. Events of 'critical' and 'serious' types alone are notified through SNMP Trap Forwarder.

Note -

Kyndryl Resiliency Orchestration supports SNMPV1 version for sending and receiving SNMP traps. Ensure that third-party software installed on the client computers support SNMP management.

The Management Information Base (MIB) file which is bundled along with Kyndryl Resiliency Orchestration software stores the details on how to read and interpret the Trap Forwarder message. The notification list members can use this file for specific purposes like displaying the events information in a particular format, etc. Contact Kyndryl Resiliency Orchestration support for loading the MIB file prior to using this feature.

Notification List

Configuring Notifications

This chapter describes how to setup and configure notifications.

In this section:

Adding Notification List

Modifying Notification List

Deleting Notification List

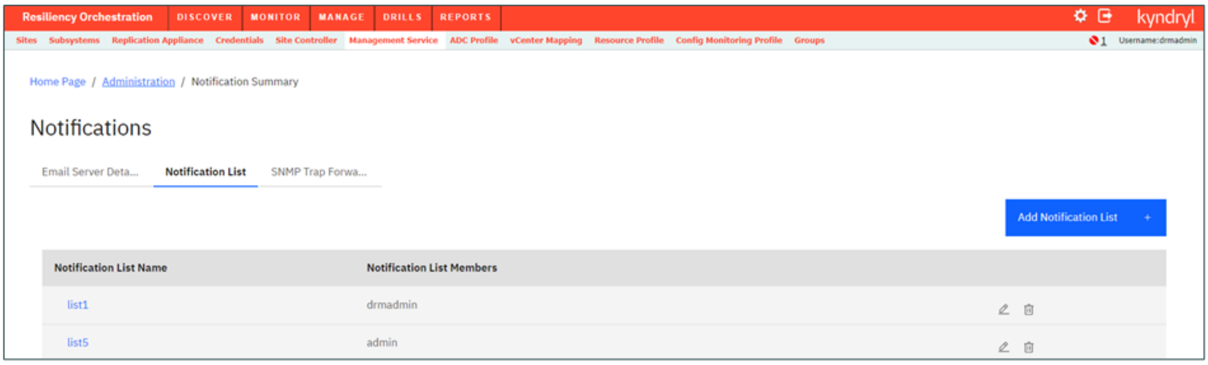
Adding Notification List

A notification list can be created to group users based on notifications to be sent. A user with administrator privilege only can create notification lists. While adding Notification List, the existing users are categorized to escalate events in the form of notifications.

Refer Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To add a notification list perform following steps:

1. Click **Admin** on the navigation bar. The **Administration** page appears. Scroll down to the **Notification Summary**. The **Notifications** page appears.



Notification List Name	Notification List Members
list1	drmadmin
list5	admin

2. Go to **Notification List** tab and click on the **Add Notification List** link in the right pane.
3. Enter name for the notification list in the **Notification List Name** field.
4. Select an organization from the **Organization** drop-down.

   Note – Leave as **Default** if you are a single tenant user. In case of multiple organization mode, select the appropriate Organization to which the Notification List being created should belong.

   Based on the Organization selected, the usernames (users part of the selected/default organization) are listed in the **User Name** field.

   Note:

   > The notification list name is mandatory and can accept alphanumeric characters, spaces and underscores only. This field should start with an alphabet and accepts only 30 characters. Select at least one user name from the list.

5. Click **Save** to save the changes and click **OK** in the pop-up message box to return to the Notifications window.
   OR
   Click **Cancel** to quit the current window without saving changes.

Modifying Notification List

Refer Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To modify the properties of a notification list, perform the following steps:

1. Click **Admin** on the navigation bar. The **Administration** page appears. Scroll down to the **Notification Summary**. The **Notifications** page appears.
2. Click ✎ icon corresponding to the notification list that you want to modify. The **Edit Notifications List** section appears.
3. You can change the **Organization** field value. Select the appropriate organization to which the notification list has to be associated with.
4. You can change the list of notification members. To do this:
   - Select a user of your choice from the Users list and click >> to add the user to the right side box. This associates the user with the notification list name.

     OR
   - Deselect users by highlighting a user from the selected member list on the right side list box and clicking << button. This removes the user from being associated with the notification list name
5. Click **Save** to save the changes and click **OK** in the pop-up message box to return to the Notifications window.
   OR
   Click **Cancel** to quit the current window without saving changes.

   Note:

   The notification list name should have at least one user associated with it.

You can modify the Notification List in the Group Setup page also.

Deleting Notification List

Refer Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To delete a notification list perform following steps:

1. Click **Admin** on the navigation bar. The **Administration** page appears. Scroll down to the **Notification Summary**. The **Notifications** page appears.
2. Click 🗑 corresponding to the notification list that you want to delete. A message box is displayed confirming the deletion.
3. Click **OK** in the message box.

Configuring SNMP Trap Forwarder

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To configure SNMP Trap Forwarder console to Kyndryl Resiliency Orchestration server to receive the notification in the form of a SNMP Trap, perform the following:

Note that in a multitenant mode, there is no access or visibility of SNMP Trap Forwarder configuration for Tenants.

1. Click **Admin** on the navigation bar. The **Administration** page appears.
2. Scroll down to the Notification Summary. The Notifications page appears.

3. Go to **SNMP TRAP Forwarder List** tab and click the **Add SNMP TRAP Forwarder** link in the right pane. The **SNMP Trap Forwarder** page appears.

Provide the necessary information in the following fields:

Field	Description
SNMP Forwarder Name	Enter a name for the SNMP Trap. This field is mandatory.
SNMP Trap Destination IP	Enter the IP address of the trap destination. This field is mandatory.
UDP Port	Enter the UDP (User Datagram Protocol) port number of the trap destination. The default is port 162. This field is mandatory.
SNMP Version	This is a non-editable field. Kyndryl Resiliency Orchestration supports SNMPV1 version for sending and receiving SNMP traps.
Community String	Enter the community string. It is a password that allows access to a network device. It defines which category of people can access the SNMP information on the device. The person responsible for the network device typically sets the community strings.
Groups	Select the groups for which you want to send the notification from the list box. You can select more than one group by using the Ctrl key.

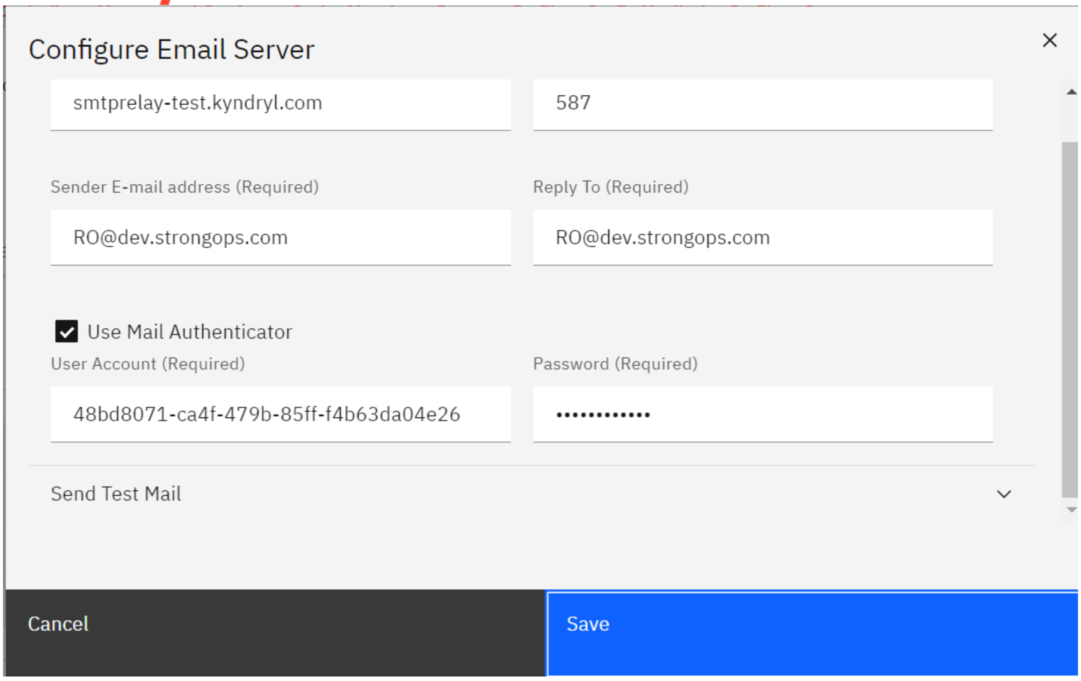
4. Click **Save** to save the changes and click **OK** in the pop-up message box to return to the Notifications window.
   OR
5. Click **Cancel** to quit the current window without saving changes.

Configuring E-mail Server

This page allows the user to configure the e-mail server. The e-mail server configuration handles all the e-mail communication to the users of the notification list.

Note that in a multitenant mode, there is no access or visibility of E-mail server configuration for Tenants.

1. Click **Admin** on the navigation bar. The **Administration** page appears. Scroll down to the **Notification Summary**. The **Notifications** page appears.
2. Go to **Email Server Details** tab and click on **Configure Email Server** on the right pane to modify the required information. The **Configuring Email Server** page appears as shown in figure below.



Configure Email Server

smtprelay-test.kyndryl.com

587

Sender E-mail address (Required): RO@dev.strongops.com

Reply To (Required): RO@dev.strongops.com

☑ Use Mail Authenticator

User Account (Required): 48bd8071-ca4f-479b-85ff-f4b63da04e26

Password (Required): ••••••••••••

Note: When user wants to check Email Server Configuration status with an valid password ,then user first needs to enter SMTP Password and check , it will not fetch SMTP password from existing DB for security reason.

The table below details the fields in the Notifications – Email Server page.

Field	Description
SMTP Server Name	This field identifies the name of the mail server. This field is mandatory. **Note-** The server name can refer to the name of server machine (For example, smtp.abc.com) or its IP address. If the server name is referred by IP address, then this field can accept only numbers and should fall within the following range and format: i.e. 0.0.0.0 to 255.255.255.255 If the server is referred by its name, then the field can accept only alphabet and period marks.
SMTP Port No	This field accepts the SMTP mail server port number. This field is mandatory.
Sender E-mail address	This displays a valid sender E-mail address. This field is mandatory.
Reply To	This displays the valid E-mail address to which the user should reply. This field is mandatory.

Use Mail Authenticator	Select this check box and provide the username and password of the SMTP mail server for authentication. This field is optional.

3. Click the **Send Test Mail** link. The **Send Test Mail** section appears.
4. Enter the e-mail address to which you want to send the notification in the **To** field and the subject of notification in the **Subject** field.
5. Click **Send Test Mail**. If it is a valid e-mail address, the message "Test mail has been sent successfully" is displayed. Otherwise the corresponding error message is displayed.
6. Click **Save** to save the changes and click **OK** in the pop-up message box to return to the Notifications window.
   OR
   Click **Cancel** to quit the current window without saving changes.

   Panaces services restart is required after changing the E-mail configuration/SMTP server configuration. For steps, refer the section **Starting and Stopping Kyndryl Resiliency Orchestration Server Services**.

Configuring E-mail Templates

This feature enables Resiliency Orchestration to customize outgoing e-mail.

(This feature is optional, to disable templates, just remove the respective e-mail from the email.properties file located under $EAMSROOT/installconfig)

Follow the below steps to enable e-mail templates on Resiliency Orchestration :

1. Add the e-mail ID and template name to the email.properties file at $EAMSROOT/installconfig as described in the below **example**.

   vivek.ganesh@kyndryl.com=sample.tmpl

NOTE: Template name can be anything with any extension.

2. Create the template which is mentioned in the above step at $EAMSROOT/installconfig/sample.tmpl as described in the below **example**.

```
Schema: HPD:IncidentInterface_Create
Server: abc.domain.com
Login: Vivek
Password: password
Action: Submit
Format: Short
!z1D_Action!: CREATE
Last Name* !1000000018!: Vivek
First Name* !1000000019!: Ganesh
Service Type !1000000099!: User Service Request
Status ! 7!: New
Reported Source !1000000215!: Email
Service Categorization Tier 1 !1000000063!: Functionality
Product Categorization Tier 1 ! 200000003!: Applications
Product Categorization Tier 2 ! 200000004!: $occured on$
Impact* !1000000163!: 1-Extensive/Widespread
```

Urgency* !1000000162!: 1-Critical
Description !1000000000!: $description$
Details !1000000151!: $event$ - $event id$ - $time occurred$

3. Navigate to this path $EAMSROOT/installconfig/email.properties

   Check the value if it is "tls" then set it to "tls1.2".

   MAIL_COMMUNICATION_TYPE=tls1.2

NOTE

> The values specified within $ will be replaced with the actual values send by Resiliency Orchestration . Text within $ should be in lower case (case sensitive), but make sure the names are as it is from the original Kyndryl Resiliency Orchestration notification e-mail.

3. Create Resiliency Orchestration user with the respective e-mail used for templates and add to the notification list. Make sure to have a separate notification list for these users and attach the same to the group.

Business Process Integration

Some business processes that may or may not related to your DR environment need to co-exist along with the processes monitored and managed by Kyndryl Resiliency Orchestration. Business Process Integration (BPI) allows you to incorporate such processes into Kyndryl Resiliency Orchestration workflow and therefore into DR environment.

Examples of such processes are daily back-ups of your database servers and the end of the day operations that may impact BCOs.

Once configured, one or more such BPIs can run on Production or on the DR at the same time. They can be configured to run only once or on periodic basis. These BPIs are associated with the Functional Groups.

BPIs are configured and incorporated into Kyndryl Resiliency Orchestration using workflows defined in XML files. These XML files are then imported to include a BPI. XML files are validated before letting them integrated in Kyndryl Resiliency Orchestration environment. Once validated and imported, Kyndryl Resiliency Orchestration system saves the timestamp of import, name of the XML file, and the version. They can be exported for archiving or editing. Exported workflow is also saved in XML format.

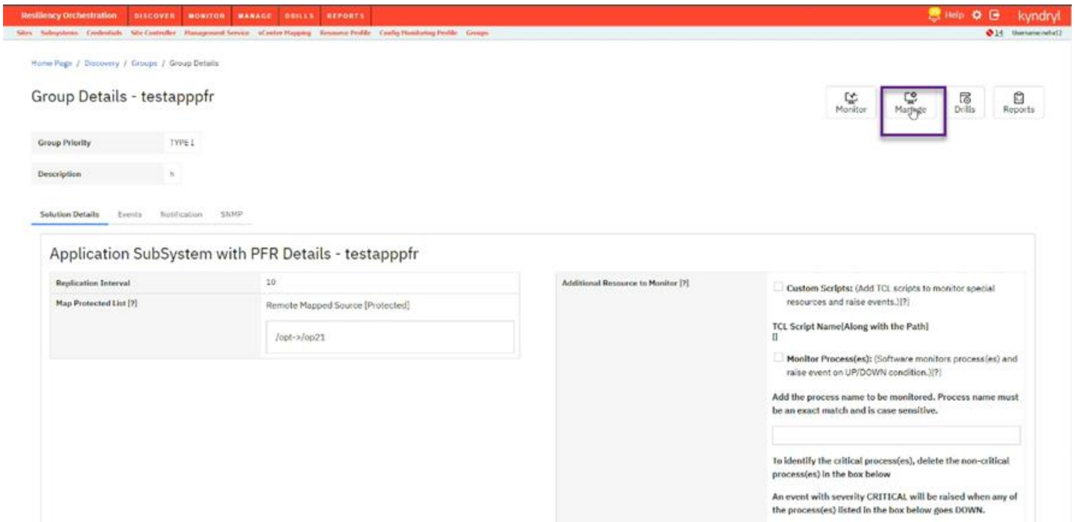
Listing Business Process Schedules

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To list the schedules of all the business processes configured for a Recovery Group, perform the steps given below:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click the **Recovery Groups** tab, the respective **Group Listing** page appears.
3. Click the required group from the **Group Name** column. The **Group Details** Page appears.

4. Click on any of the group from the Group Name column.
5. Click the **Manage tab** > **View all workflows** to list the business processes of the Group.



Group Details - testapppfr

Group Priority	TYPE 1
Description	h

Application SubSystem with PFR Details - testapppfr

Replication Interval	10
Map Protected List [?]	Remote Mapped Source [Protected] /opt->/op21

Additional Resource to Monitor [?]

□ Custom Scripts: (Add TCL scripts to monitor special resources and raise events.)[?]

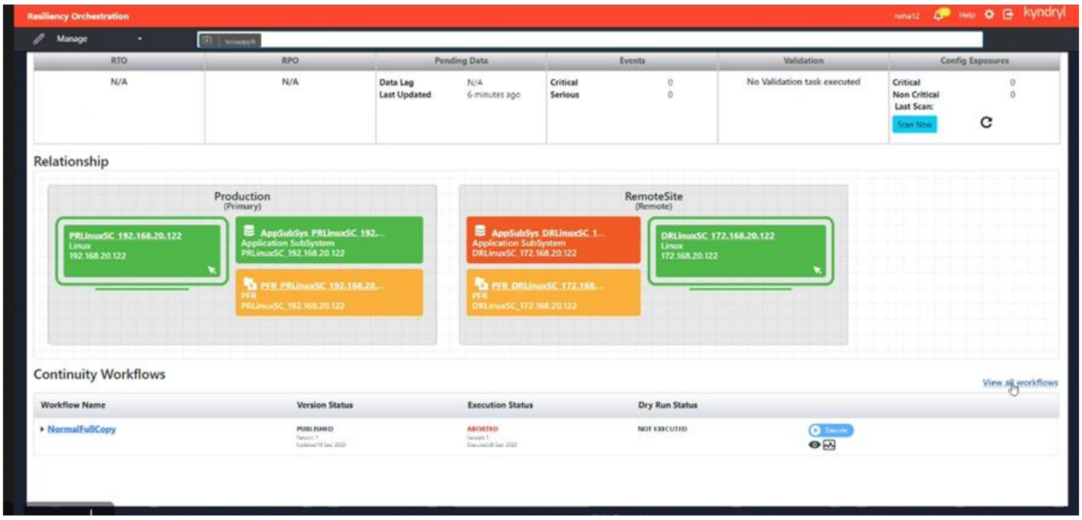
TCL Script Name[Along with the Path]
[]

□ Monitor Process(es): (Software monitors process(es) and raise event on UP/DOWN condition.)[?]

Add the process name to be monitored. Process name must be an exact match and is case sensitive.

To identify the critical process(es), delete the non-critical process(es) in the box below

An event with severity CRITICAL will be raised when any of the process(es) listed in the box below goes DOWN.



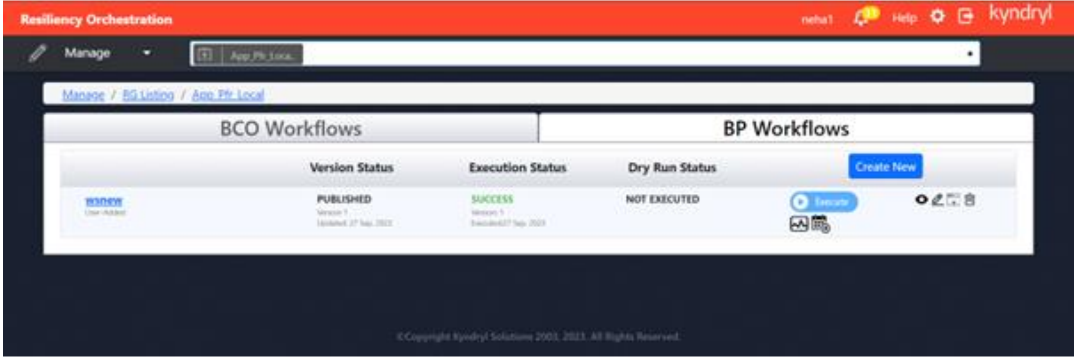
RTO	RPO	Pending Data	Events	Validation	Config Exposures
N/A	N/A	Data Lag N/A Last Updated 6 minutes ago	Critical 0 Serious 0	No Validation task executed	Critical 0 Non Critical 0 Last Scan:

Continuity Workflows

View all workflows

Workflow Name	Version Status	Execution Status	Dry Run Status
NormalFullCopy	PUBLISHED	ABORTED	NOT EXECUTED

This lists all the configured business processes, if any, for the Group with the following details.



	Version Status	Execution Status	Dry Run Status
wsnew User-Added	PUBLISHED Version 1 Updated 27 Sep 2023	SUCCESS Version 1 Executed 27 Sep 2023	NOT EXECUTED

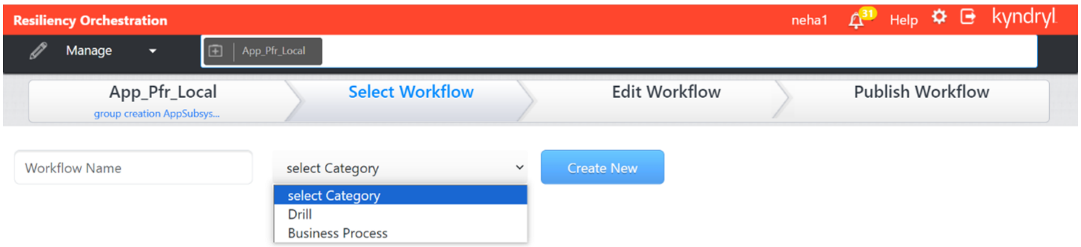
Adding Business Process

Refer Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

You can add a business process to a Recovery Group or an Application Group.

To add a Business Process, follow the steps given below:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column for which you want to add business process. The **Group Details** page appears.
4. **Click Manage tab** > View all workflows to list the business processes of the Group.
5. Under the Business Process Workflow, click the Create new.



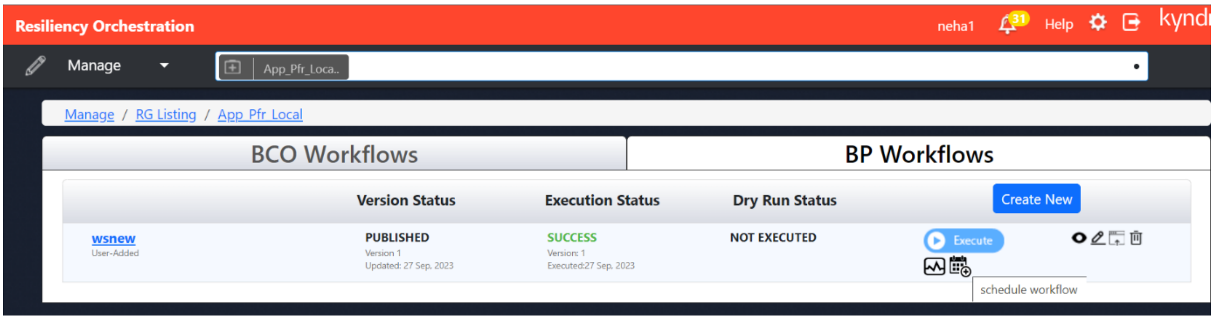
Configuring Business Process

Click *Kyndryl Resiliency Orchestration Server User Role Management* to see the privileges.

To configure the new business process:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.

2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the **GROUP NAME** column for which you want to configure the business process. The **Group Details** Page appears.
4. Click **Manage tab** > View all workflows to list the business processes of the Group
5. Click on the Calendar icon to configure and schedule it.



	Version Status	Execution Status	Dry Run Status
wsnew User-Added	PUBLISHED Version 1 Updated: 27 Sep, 2023	SUCCESS Version: 1 Executed:27 Sep, 2023	NOT EXECUTED

Custom Event

Custom events are those events that are not already available in Kyndryl Resiliency Orchestration; but they are required in your DR related business processes. You can configure to raise customized events in Kyndryl Resiliency Orchestration. This is done using a shell script that can be imported into Kyndryl Resiliency Orchestration at command line. You need to write this script to suit to your needs.

The script takes values such as event name, description, severity, and impact, policy window name, policy workflow details, and Group name. This script sends configured events to the Kyndryl Resiliency Orchestration server. However, such scripts need to be validated before importing or exporting for any possible errors.

The imported customized events, if raised, can be seen by clicking **Events** in the navigation bar. To view the custom events and their policies listed navigate as mentioned in the following section.

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow. The **Group Details** Page appears.
4. Click Group Details > Events tab.

Note:

Do not import the same event with the same name into the Kyndryl Resiliency Orchestration. This overwrites the earlier instance of that event. If you need to import the same event, use different name.

You can associate a policy workflow along with an event. This policy can be a customized or an already available policy in Kyndryl Resiliency Orchestration. Event script is imported or exported at command line using the shell scripts installed along with Kyndryl Resiliency Orchestration.

Importing Custom Event

1 Open command prompt.
2 Go to the directory where you want to import the custom event script.
3 Run following command at the command line:

```
import-event.sh importEvent <groupname> <custom event-xml-filename>
```

Exporting Custom Event Script

1 Open command prompt.
2 Go to the directory where the custom event XML file you want to export resides.
3 Run following command at the command line:

```
export-event.sh exportEvent <groupname> <eventName> <custom event-
xml-filename>
```

Importing / Exporting Custom Event Policy Workflow

Once a custom event is imported into Enterprise DR Manager, use **Workflow Manager** interface to import or export related policy workflow.

Examples

- Custom event without workflow

```
<?xml version="1.0" encoding="UTF-8"?>
<wf:custom-event xmlns:wf="/panaces/workflow/" >
  <name>MyCustomEvent</name>
  <description>description</description>
  <severity>WARNING</severity>
  <impact>impact</impact>
</wf:custom-event>
```

- Custom event with workflow

```
<?xml version="1.0" encoding="UTF-8"?>
<wf:custom-event xmlns:wf="/panaces/workflow/" >
  <name>MyCustomEvent</name>
  <description>description</description>
  <severity>WARNING</severity>
  <impact>impact</impact>
  <policy>
    <execMode>auto</execMode>
    <wf:workflow>
      <name>some workflow name</name>
      <description>some workflow description</description>
      <action-list firstActionId="c1">
        <action id="c1">
          <registeredName>Custom</registeredName>
          <name>custom action 1</name>
          <description>Description</description>
          <privateProperties>
            <wf:scriptAction type="cmd"
etcComputationType="userDefined" componentType="dynamic" >
              <serverName>Production Server</serverName>
              <command>Some command</command>
              <etcValue>10</etcValue>
            </wf:scriptAction>
```

```
                                </privateProperties>
                            </action>
                        </action-list>
                    </wf:workflow>
                </policy>
            </wf:custom-event>
```

Scheduling

You can schedule a business process workflow for one of the following schedules:

- Schedule to run once on a particular day and time.
- Schedule to run daily at a particular time or at a recurring interval.
- Schedule to run weekly on a particular day and time.
- Schedule to run monthly on a particular day and time.

To view the procedure involved in Scheduling a Business Process Workflow, refer **Scheduling Business Process Workflow**.

Managing Business Process

Refer Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

Business Processes can be managed by navigating to **Business Processes** tab of the group as follows:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow. The **Group Details** Page appears.
4. Click **Manage tab** > View all workflows to list the business processes of the Group

This page lists all the Business Processes of the group. It contains the following columns:

Field	Description
Business Process Name	Displays the name of the business process.

Field	**Description**
Status	Displays the current status of the business process. It can be one of the following: ▪ **Never Executed** -has the status indicated that the Business Process is not executed. ▪ **Executing** - The status indicates that the workflow is executing. ▪ **Awaiting Input** - The status indicates that the workflow requires user input to proceed. ▪ **Success** - The status indicates that the workflow is completed successfully. ▪ **Failed** - The status indicates that the workflow execution has failed. ▪ **Aborted** - The status indicates that the workflow has been aborted. ▪ **Crashed** - The status indicates that the Kyndryl Resiliency Orchestration has shut down during execution.
Last Execution Time	Time when the business process was executed last time.
Action	Actions can be one of the following: ▪ **Start** - To start the business process ▪ **Stop** - To stop the business process. This option is available only when business process is in progress. ▪ **Resume** - To resume the business process. This option is available only when business process has crashed earlier.

Deleting Business Process

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

A business process can be deleted from the Group Details page of a Recovery Group.

To delete a business process, perform the following steps:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click **Manage tab** > View all workflows to list the business processes of the Group
5. In the business processes list, click 🗑 corresponding to the process that you want to delete.

Continuity Workflows

To view the business process workflows:

1. Click Monitor > AG/ RG > Application Group / Recovery Group Name.
2. The **AG Details** / **RG Details** page is displayed.
3. Click **View All Workflows** if it is a RG. All the BCO and BP workflows are displayed for the RG.

- Click the BCO Workflows tab, all BCO workflows are displayed for the RG
- Click the BP Workflows tab, all BP workflows are displayed for the RG.

The following details are displayed:

Field	Description
Workflow Name	Displays the name of the workflow. Displays the group name for which you want to add the business process.
Version status	Displays the group name for which you want to add the business process.
Execution status	Displays information if the execution was success, crashed aborted or is awaiting input.
Dry Run Status	Displays information if the workflow was a success, crashed, not executed or failed

- Click 👁 to preview the workflow.

Note

The user can perform the following manage tasks in addition to viewing when the navigation is from the Manage page.

- Click ✎ to edit the workflow.
- Click 🗑 to delete the workflow.
- Click ▶ Execute to execute the workflow.
- Click 📈 to DryRun the workflow
- Click 📅 to schedule the workflow execution.
- Click **Create New** to create a new workflow

Note

- If the group is in switchover or switchback, then the current DR state of the group does not permit any continuity operations.
- To change the state of the group, go to Discover > groups page.

To view the execution history and the version history, click on the workflow name.

The E**xecution History** displays the following information:

Field	**Description**
Date	Displays the date of execution
Time Taken	Displays the time taken in seconds for execution
status	Workflow execution status
Version	Displays the version number

The **Version History** displays the following information:

Field	**Description**
Version	Displays the version number
Created On	Displays the workflow created time
Created By	Displays the User name

Workflow Manager

Workflow is a sequence of steps/tasks performed to complete a business process. The business process could be a Business Continuity Operation or DR Drill or EOD operation.

Actions and workflows are a set of procedures that are configured to act against an event in the DR environment. You cannot add or delete an Action from a Workflow when it is being executed.

Workflow manager enables you to design the workflow logic, execute and view the execution status.

Configuring the workflow involves:

- Design the workflow logic.

- Insert/delete actions to be performed
- Provide/alter inputs to the actions
  - Flow control
- Conditions to quit/abort workflow
- Handle failure conditions
- Recursion (execute an action periodically)
  - Scheduling the workflow

Executing the workflow involves:

- Execute (start/stop) workflow
- Schedule workflow

Execution Status:

- Show execution status

Working with Actions

Adding Actions/ Action Groups/ Fork and Join

A user can add actions, or an action group to customize or build a workflow. The pre-built actions are available in **Recovery Automation Library (RAL)** to insert in the workflow.

> Note:
>
> You cannot add an action/action group during workflow execution. If you attempt to do so, an alert message "Could not insert Action/Action Group. Reason:<workflowname> workflow is executing" will be displayed.

To insert an action:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow.
4. Click **Manage** **> View all workflows** or **Drills** or **Events** tab depending upon the workflow type you want to configure.
5. Click on **Edit** icon against the workflow to edit it. The **Workflow Editor** page appears.
6. Click the **Add** button. The **Add** window appears.

Field	Description
Category	Select a category from the drop-down list. Note: To add an action:

Field	Description
	1. Select an action category under **Action Category**. A list of actions under the selected action category appears. 2. Click + icon to add an action. This icon appears against each action. To add an Action Group: i. Click on ⧉ to add an action group. It will add the default action group. To add Workflows: i.Select from the Select Signature Solution from the drop-down list. i.Click Import Workflow. To add fork and join: i. Click on icon to add a **fork** node. It is used to execute actions in parallel. ii. Click on icon to add a **join** node. It is used to wait for executed forked actions.
Inserted Action Destinations	
Success Path	Drag the green bubble to the next destination action.
Failure Path	Drag the red bubble to the next destination action.

8. Click **Save now** to add an action.

Configuring Actions

An action is configured only when properties are attached to it. Both generic and advanced properties have to be configured for every action. Configuration of actions can be done one at a time in the Action Properties section. The generic properties are the same for all actions, but you can configure them depending on the action. The advanced properties vary depending on the action.

Note:

You cannot configure an action in a workflow when the workflow execution is in progress.

To open the **Action Properties** section:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click **Manage** > View all workflows or **Drills** or **Events** tab depending upon the workflow type you want to configure.
5. Click on Edit icon against the workflow to edit it. The **Workflow Editor** page appears.

Note:

You can change the existing properties by clicking on any Action or Action group in the Action graph.

To **edit** generic properties of Action or Action group:

1. Click the ⓘ icon or double click on an action.

The following table describes the run time properties of the actions:

Field	Description
Name	Specifies the name of the action. You can modify if required.
Description	Displays the description for the action. You can modify if required.
Execution Mode	This property indicates your intervention preference in action execution. It is either **Manual** or **Auto**. Default setting for each action is Auto. ▪ Manual specifies that there is some user intervention to execute the action. To enable the action to raise an Input Required event, set it to Manual execution mode. ▪ Auto specifies that no user intervention is required to execute the action. In case the **Retry on Failure** checkbox is selected and the **Execution Mode** is set as **Manual**, then action is executed without manual intervention.
Inform Upon	This property indicates whether to notify after the Action execution completes. Notification is done based on the value of this property. The available options are: ▪ No Inform ▪ Inform on Success ▪ Inform on Failure ▪ Inform All If the property is set to **Inform on Success**, notification is done only after successful execution of the action. If Inform Upon is set to **Inform All** or **Inform on Failure** and **Retry on Failure** is also configured: ▪ Notification is done only once after the execution of the action ▪ In case, the action fails during first execution instance, then **Retry on Failure** will try to execute the action again without notification. ▪ If the action fails on all attempts, the user is notified and has the control to continue/quit/retry etc.

Field	Description
Skip this Action	Select the checkbox to skip a particular action in the workflow. The skip action property can be configured even when the workflow is being executed. If any action is skipped in the workflow, the skipping action takes the success path for that action. Any skipped action will have the status displayed as 'Skipped' for that action.

Field	Description
Sync Name	Provide the name of the ***Sync point***. A name that can be used to have the consistency across the RGs of an AG. You can achieve the consistency of an AG by providing the sync points to an action in a Business Process of the respective RGs. For example: Split Mount Apply Unmount Establish

Retrying Actions

Retry On Failure	Select the checkbox to automatically retry the action on failure.
Retry Count	Enter the retry count. It is the maximum number of attempts to execute the action after the failure. Minimum value for this field is 1. This field is displayed only when you select the **Retry On Failure** checkbox.
Retry Wait Time	Enter the time in seconds to wait before retrying after the failure. Minimum value for this field is 1. This field is displayed only when you select the **Retry On Failure** checkbox.
Is Retryable	This property can be used to set the action for retrying. It can be set to **Yes** or **No**. If set to **Yes** , the **Retry** button is enabled when the action fails. If you set it to **No**, the button appears disabled.

Note:

- In case the **Retry on Failure** checkbox is selected and the **Execution Mode** is set as **Manual**, then action is re-executed without asking the user again.
- If the Retry on Failure checkbox is selected and Inform Upon is set to Inform All or Inform on Failure:
- Notification is done only once after the execution of the action.
- If the action fails during first execution instance, then **Retry on Failure** will try to execute the action again without notification.
- If the action fails on all attempts, the user is notified and has the option to continue or quit or retry.
- If the Retry on Failure checkbox is selected and Abort Upon is set to Abort All or Abort on Failure:
- If the action fails during first execution instance, then **Retry on Failure** will try to execute the action again without aborting.
- If the action fails on all attempts, the action is aborted
- When the **Retry on Failure** checkbox is selected, **is Retryable** will be set to **Yes**.

Field	Description
Abort Upon	Execution of a Workflow can be aborted upon a particular action's success or failure condition. This property can be enabled with four options. They are: ▪ Abort All ▪ No Abort ▪ Abort on Success ▪ Abort on Failure If **Abort on Success** is enabled for an action in Workflow and if the execution of that action was successful then the Workflow execution is aborted. Otherwise, the Workflow execution continues. If the Retry on Failure checkbox is selected and Abort Upon is set to Abort All or Abort on Failure : ▪ In case, the action fails during first execution instance, then **Retry on Failure** will try to execute the action again without aborting. ▪ If the action fails on all attempts, the action is aborted.
Recurrence Interval	The value specified here executes the action in a loop with the specified sleep interval. Within a Workflow, if an action is set with this property then the next action execution is controlled by Time To Execute.
Time to wait before executing this Action	Represents the current action execution to be kicked-off after x seconds, just after the previous action has been started to execute. So if x=0 for an action in a Workflow, then that action will be executed after 0 seconds just after the previous action has been started to execute. That means the current action execution and the previous action execution are in parallel. Since this property is dependent on previous action, it is not applicable for an independent action and also for the first action within a top level Workflow.
Severity for User Input Event	Provides the options to set the severity of events requiring your inputs. It can be set to: ▪ WARNING ▪ SERIOUS ▪ CRITICAL ▪ INFO

Field	Description
Severity for Action Failure Event	Provides the options to set the severity of Action failure events. It can be set to: ▪ WARNING ▪ SERIOUS ▪ CRITICAL ▪ INFO
Action Operation Type	This field displays the category to which the action belongs. Some of the Available action categories are: ▪ Replication ▪ Kyndryl ▪ Oracle ▪ PFR ▪ File ▪ SQL Server ▪ Process This is a non- editable property for all actions except for the Custom Action. For Custom action, **Action Operation Type** should be set by the user based on the operation that the custom action is configured to perform. In addition to the above RAL action category, the following Action Operation Types are also available for the user to select. ▪ Network ▪ Application ▪ Business Process ▪ Other Note: Changing the type of the Custom action will not change the type in the status/analysis for the already executed instances of the workflow.
Raise event when User Input on Failure is not configured	Select the check box to raise an event when User Input on Failure is not configured.
Override ETC	Select this check box to override the expected time to complete.
ETC	Enter the expected time to complete the task. By default, it is 10 seconds. You can give any value greater than zero.

2. The generic configuration is common for all actions.

    3. Click **Save now**, to save the configured generic properties, if modifications are done after actions are configured.

To edit advanced properties of an action:

1. Click the Action Properties tab.
2. Enter the appropriate values in the relevant fields. The advanced properties vary depending on the action. To view the Advanced Properties configuration for RAL Actions, **click here**.
3. Click **Save now** to save the changes. This displays a message saying "Workflow saved successfully."

Configuring Action Groups

An action Group is considered as configured only when its properties and its actions are configured. Only generic properties have to be configured for action group. Configuration of action group can be done one at a time in the Action Properties section.

Note:

You cannot configure an action group in a workflow when the workflow execution is in progress.

For Action Groups, only "recurrence" property can be set and rest of the properties are not applicable.

To open the **Action Properties** section:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click **Manage** > View all workflows or **Drills** or **Events** tab depending upon the workflow type you want to configure.
5. Click on **Edit** icon against the workflow to edit it . The **Workflow Editor** page appears.

    Note:

    You can change the existing properties by clicking on any Action group in the Action graph.

To edit generic properties of Action group:

1. Click the ⓘ icon or double click on an action group.
2. To edit the run time settings, refer to **Configuring Action**.
3. Enter the appropriate values in the relevant fields. The generic configuration is common for all action group.
4. Click on ✏ icon to edit the action group.
5. Make the required changes in the relevant field.

6. Click **Save now** , to save the configured properties, if modifications are done after actions are configured.

Configuring Fork and Join

A fork is considered as configured only when its properties and its actions are configured. Only generic properties have to be configured for a fork node. Configuration of a fork node can be done one at a time in the Action Properties section.

> **Note**:
>
> You cannot configure a fork and join in a workflow when the workflow execution is in progress.

To open the **Action Properties** section:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click **Manage** > View all workflows or Drills or Events tab depending upon the workflow type you want to configure.
5. Click on **Edit** icon against the workflow to edit it. The Workflow Editor page appears.
6. Click icon to add a fork, then add an action in between a fork and join.

Note

- Start of an action is connected to a fork and the end of an action is connected to a join.
- You can change the existing properties by clicking on any Fork node in the workflow.

To edit generic properties of a fork node:

1. Click the ⓘ icon or double click on a fork node.
2. To edit the run time settings, refer to **Configuring Action**.
3. Enter the appropriate values in the relevant fields. The generic configuration is common for all action group.
4. Click on ✎ icon to edit the fork node.
5. Make the required changes in the relevant field.
6. Click **Save now**, to save the configured properties, if modifications are done after actions are configured.

Deleting Actions/ Action Groups/Fork and Join

You can delete one or more actions, action groups and fork and a join from a workflow. Some of the actions in a workflow are pre-defined. Such actions cannot be deleted and the delete button will be disabled for them.

> **Note**:

You cannot delete an action during a workflow execution. If you attempt to do so, a pop up with message "PAN-SACM-4302: Could not configure Workflow as Workflow execution is in progress" is displayed.

For a workflow, if you delete the last action in an Action Group, the Action Group also gets deleted. However, the last action in a workflow cannot be deleted. If you want to delete the last action, add a new action to the workflow and then delete the action.

To delete an action:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click **Manage > View all workflows** or **Drills** or **Events** tab depending upon the workflow type you want to configure.
5. click on Edit icon against the workflow to edit it. The **Workflow Editor** page appears.
6. Click the Action/Action Group/Fork and join in the **workflow editor** that you want to delete and click 🗑 icon**.** A message box is displayed.
7. Click **OK** on the message box to delete the selected action/ action group/ fork and join.

Copy Workflow/ Copy Action

This a new feature added in Workflow manager to copy a workflow from any other group with similar signature**.** This process is executed in series and will has a Wizard based execution**.**

To copy an existing workflow, perform the following steps:

1. Click **Drills** > **Workflow list** > Select Create New Workflow.
2. Select a group from the Group listing page.

Field	Description
Name	Provide the workflow name
Category	Select one of the following category from the drop-down list: ▪ Drills ▪ Business Process

3. Click Create new.
4. Click on **Add** to add the workflows.
5. Select the **Workflow** tab from the **Add** Window

Field	Description
Solution Signature	Select one of the solution signature from the drop-down list.
Group	Select a group from the list.

6. Select the workflow to be copied and click on ✚ icon from the list.
   A message box is displayed confirming the copy action "Copying the workflow on canvas will replace all the existing items on the canvas. Do you wish to continue?"
7. Click **OK** in the message box to replace the workflow with a new workflow.

Copy Action

This a new feature added in Workflow manager, which is used to copy an action from Workflow.

1. Click Drills > Workflow list > Select Create New Workflow.
2. Select a group from the Group listing page.

Field	Description
Name	Provide the workflow name
Category	Select one of the following category from the drop-down list: ▪ Drills ▪ Business Process

3. Click **Create** new.
4. In Workflow Editor page, select an action.
5. Click on ⎘ icon to copy the selected action.

Zoom in and Zoom Out Workflow

To zoom in and out of the workflow, perform the following steps:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow. The **Group Details** Page appears.

4. Click Group Configuration tab.
5. Click **Business Processes** or **Drills** or **Continuity** or **Events** tab depending upon the workflow type you want to configure.
6. Click on Edit icon against the workflow to edit it. The **Workflow Editor** page appears.

To Zoom in:

Click ⊕ icon to Zoom in to the workflow.

To Zoom out:

Click ⊖ icon to Zoom out of the workflow.

Creating new workflow

To create a workflow in a group, perform the following steps:

1. Click Drills > Summary tab.
2. Select a group from the **Drills** page.
3. Click on **Create new** button or Click **Create new** workflow. The user is directed to the **Select Workflow** tab.

Field	**Description**
Workflow Name	Provide the workflow name
Category	Select category from the drop-down list- Drill or Business Process

4. Click Create New.

OR

- Click Manage> RG Listing > Group Name
- Click View All Workflows in Continuity Workflows
- Click BP Workflows > Create New Workflows.
- The user is directed to the **Select Workflow** tab.

To create a new **Business Process** workflow:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click Group Configuration > Business Process.

Field	Description
Name	Provide the workflow name
Category	Select Business Process category from the drop-down list

Deleting Workflow

To delete an action, perform the following steps:

1. In the navigation bar, click **Drills > Summary** tab
2. Select the group.
3. Click the workflow name > click Delete Button 🗑icon. A message box is displayed.
4. Click **OK** on the message box to delete the workflow.

Importing or Exporting a Workflow

You can import or export a workflow in the XML file format. This is possible only for the workflows which are generic and are not pre-defined in Kyndryl Resiliency Orchestration. The XML files of the workflows contain complete configuration of all the actions in the workflow. As a result, once the XML file is imported, parameter settings for all actions are automatically populated. On the other hand, by exporting, you can take backup of a workflow in XML format.

You may like to export a workflow of an existing Group and import it for a newly created Group. However, while doing this, caution must be taken to change the Production and DR components specified in the XML file before importing it for the new Group.

Import/ Export functionality can be accessed in the **Workflow Details** page.

To access Import/ Export functionality...

1 Click ***Discover*** > **Groups** on the navigation bar. The **Groups** page appears.
2 Click **Recovery Group** or **Application Group** tab, the respective **Group Listing** page appears.
3 Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4 Click the **Group Configuration** tab.
5 Click **Business Processes** or **Tests** or **Continuity** or **Events** tab depending upon the workflow which you want to import/export.
6 Click the link for the desired operation. The **Workflow editor** page appears.

To Import Workflow

1 Click on Add button.
2 Click on the workflow tab.
3 Click the **Import Workflow** button and import the file.

To Export Workflow

Click on the Export button at the footer.

To import a XML file for a workflow:

Importing a workflow will overwrite the existing workflow. Make sure that you have specified the right components in the XML file for the desired Group.

For the import to be successful, the workflow must not be running.

1 Open the **Workflow Editor** page.
2 Click on Add button.
3 Click on the workflow tab.
4 Click the **Import Workflow** button and import the file.
5 Click **Browse** to open the **Choose file** dialog box.
6 Select the desired XML file and click **Open** in the **Choose file** dialog box.

To export workflow for a Group:

1 Open the **Workflow Editor** page.
2 Click the **Export** button.
3 A pop up message is displayed as "Will export the last published workflow?"
4 Click **Yes** to open **File Download** dialog box.
5 Click **Save** to open the **Save as** dialog box to save the XML file at the desired location.

Note

- While exporting a workflow with Skip property 'Disabled', the XML file will not contain any tags with respect to skip for that action. However, when the workflow is exported with Skip property 'Enabled', the XML file will have skip tag for that action. The case is similar for 'Single step'.
- When importing a workflow from a file, the version number of the imported workflow goes through a validation check of supported RAL versions. If the version of the imported workflow is not supported, the following message is displayed.

  "Import Failed!
  The Current Recovery Automation Library (RAL) Version is <*ral_version*>
  The version of the workflow that you are trying to import is <*version*>
  This is not compatible with the current RAL Version.
  The versions of the following actions are not compatible with current RAL Version.
  Action Name = <*action_name*>, Version = <*action_version*>
  Action Name = <*action_name*>, Version = <*action_version*>
  Action Name = <*action_name*>, Version = <*action_version*>
  Action Name = <*action_name*>, Version = <*action_version*>
  Action Name = <*action_name*>, Version = <*action_version*>

  Please consult the Kyndryl Resiliency Orchestration Workflow Version Compatibility Matrix/User Manual before importing the Workflow"
- While exporting a workflow, you have two options. One is to open it in the browser directly without saving it and the other is to save it onto a local disk. The Open option does not work. Use only Save button to save a workflow onto the disk and open later with an editor of your choice.

Scheduling Business Process Workflow / Drills

You can schedule a business process workflow for one of the following:

- Schedule to run just once.
- Schedule to run daily at a particular time or at recurring intervals.
- Schedule to run weekly on a particular day and time.
- Schedule to run monthly on a particular day and time.

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow. The **Group Details** Page appears.
4. Click Group Configuration tab.
5. Click **Business Processes** or **Drills** tab depending upon the workflow type you want to configure.
6. Click on **Edit** icon against the workflow to edit it . The **Workflow Editor** page appears.
7. Click **Publish**.
8. Again click Publish Workflow.

The **Workflow Listing** page appears.

9. Click the Scheduler icon 📅 for the published Workflow accordingly. The Schedule Workflow pop-up appears with the Group name and Workflow name.
10. Click on the Enable schedule checkbox to schedule the Workflow.

Field	Description
Recurrence Frequency	
Just Once	Select this option to run the workflow once on a particular date and time. Click 📅 and select the date from the displayed calendar.
Daily	Select this option to run the workflow daily at a particular time or at recurring intervals. In the **For Duration** drop-down list: ▪ Select **Forever** to run the workflow daily forever (or) ▪ Select **Custom Range** to run the workflow daily for the desired duration. Click 📅 and select the dates between which you want to run the workflow. The scheduled dates should not be less than the current date.

Field	Description
	Set the hourly frequency of the execution and the end time from the drop-down lists under **Start Executing this Process at** option.
Weekly	Select this option to run the workflow weekly on a particular day and time. Select the checkboxes corresponding to the days on which you want to run the workflow. In the **For Duration** drop-down list: ▪ Select **Forever** to run the workflow weekly at the specified day and time forever (or) ▪ Select **Custom Range** to run the workflow weekly at the specified day and time for the desired duration. Click 📅 and select the dates between which you want to run the workflow. The scheduled dates should not be less than the current date.
Monthly	Select this option to run the workflow monthly on a particular day and time. Select **Day of every month** option to run the workflow on a particular date of every month. Select **Every** option to run the workflow on every nth week and particular day of every month. In the **For Duration** drop-down list: ▪ Select **Forever** to run the workflow monthly at the specified day and time forever (or) ▪ Select **Custom Range** to run the workflow monthly at the specified day and time for the desired duration. Click 📅 and select the dates between which you want to run the workflow. The scheduled dates should not be less than the current date.
Start Executing this Process at	Set the start time to execute the workflow from the drop-down list. The time format is HH:MM:AM/PM.

11. Enter the appropriate values in the relevant fields and click **Done**.

    Note

You can also view the **Workflow listing** page, by clicking **Drills >Drills list view** in the navigation bar. Select the group, the **Workflow Listing** page appears.

You can view all the scheduled workflows by clicking on the **Workflow Calendar** in the right hand side of Workflow **listing** page.

For **Drills:** Only lists all the scheduled workflows, as drills won't be executed.
For **Business Processes**: Lists all the workflow scheduled after the current minute.

- Just Once: Once the workflow is executed, it will not be listed in the Workflow calendar list.
- Daily, Weekly, Monthly: Once executed, the list will be updated with the date and time as per schedule.

Automatic Retry on Failure

Kyndryl Resiliency Orchestration allows automatic retry of an action if it fails. Action is executed until it succeeds or for a specific number of times, whichever comes first.

To configure Automatic Retry on Failure through UI

1. Open the ***Workflow editor*** page.
2. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
3. Click Recovery Group or Application Group tab, the respective Group listing page appears.
4. Click the required group from the **GROUP NAME** column for which you want to configure the workflow. The **Group Details** page appears.
5. Click Group Configuration tab.
6. Click **Business Processes** or **Tests** or **Continuity** or **Events** tab depending upon the operation you want to configure.
7. Click the link for the desired operation to which you want to configure actions. The Workflow Editor page appears.
8. Click the **Properties** tab for the action you want to configure.
9. Set the following fields.

Field	**Description**
Retry On Failure	Select this check box to automatically retry the action on failure.
Retry Count	Enter the retry count. It is the maximum number of attempts to re-execute the action if and only if it fails. This field can have integer values greater than zero.
Retry Wait Time	Enter the time in seconds to wait before a retry after failure. This field can have integer values greater than zero.

Note

- In case the **Retry on Failure** checkbox is selected and the **Execution Mode** is set as **Manual**, then action is re-executed without asking the user again.
- If the **Retry on Failure** checkbox is selected and **Inform Upon** is set to **Inform All** or **Inform on Failure**:
  - Notification is done only once after the execution of the action.
  - If the action fails during first execution instance, then **Retry on Failure** will try to execute the action again without notification.
  - If the action fails on all attempts, the user is notified and has the option to continue or quit or retry.
- If the Retry on Failure checkbox is selected and Abort Upon is set to Abort All or Abort on Failure:
  - If the action fails during first execution instance, then **Retry on Failure** will try to execute the action again without aborting.
  - If the action fails on all attempts, the action is aborted.
- When the **Retry on Failure** checkbox is selected, **is Retryable** will be set to "Yes".

Single Stepping Actions in Workflows

Enabling single step will wait for user confirmation while executing each action in the workflow. Single step specifies that there is some user intervention to execute the action. Use **Enable Single Step** to raise an Input Required event.

To enable this feature, perform the following:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow. The **Group Details** Page appears.
4. Click the Group Configuration tab.
5. Click the **Business Processes** or **Drills** or **Continuity** or **Events** tab depending upon the operation you want to configure.
6. Click the link for the desired workflow. The **Workflow Editor** page appears.
7. Click Publish.
8. Click the **Enable Single Step** button to enabling single stepping.

To **disable** single stepping, follow the steps from 1 to 6 and click the **Disable Single Step** button.

Note

- In case the **Skip** checkbox is selected and the **Single Step is Enabled**, then action is skipped without manual intervention.
- In case the **Execution Mode** is set as **Auto** and the **Single Step is Enabled**, the workflow will wait for user confirmation to execute.

- In case the **Execution Mode** is set as **Manual** and the **Single Step is Enabled**, the workflow will wait for user confirmation only once to execute.

Synchronizing Workflow with RPO/RTO

It is possible that the Workflow being executed is also being considered for RPO/RTO calculation. To avoid this conflict, you can synchronize the Workflow with RPO/RTO calculation mechanism.

To do the synchronization, perform the following steps:

1. Identify the Action/Action Group that can probably conflict with RPO/RTO mechanism.
2. Insert Group Lock action at the start and end of the Action/Action Group. Refer **Adding Actions/ Action Groups** for procedural details.
3. In the Action graph, click the **Group Lock** action at the start of the Action/Action Group.
4. Click the **Advanced** tab in the **Action Properties** section.
5. Select the **Acquire Lock** option to associate lock acquisition action to the Group Lock action.
6. Click **Finish**.
7. In the Action graph, click the **Group Lock** action at the end of the Action/Action Group.
8. Click the **Advanced** tab in the **Action Properties** section.
9. Select the **Release Lock** radio button to associate lock removal action to the Group Lock action.
10. Click **Finish**.

This synchronization is performed on first-come-first-serve basis. Only after release of the Group Lock, the conflicting action can resume.

Create/ Save as a Draft/Publish

A user with “Create” privilege is able to create a draft and save it. From Kyndryl RO 8.1.3.2 onwards Create is segregated to Create and Publish privilege’s.

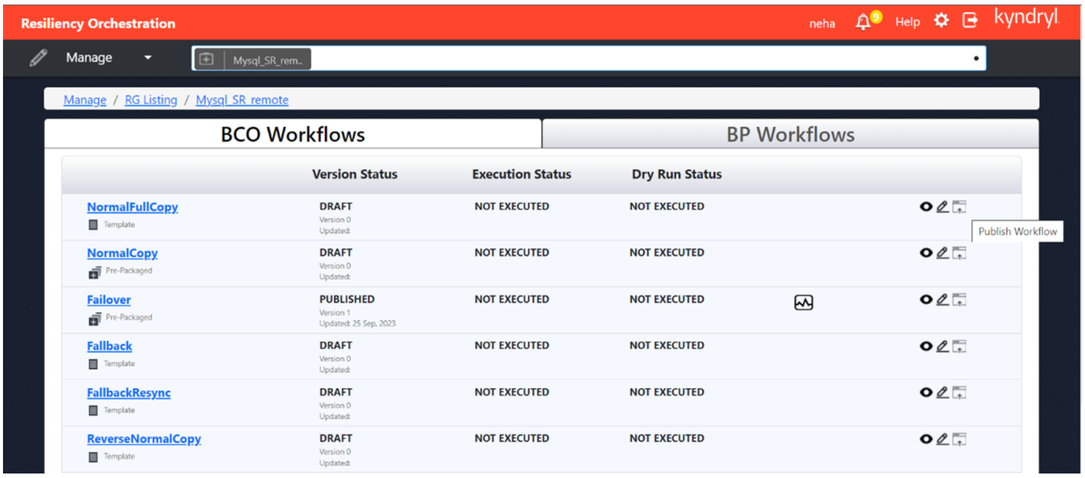
Save as a Draft (by “Create” privilege user)

This feature is added in Workflow manager to provide the user with an option to save the workflow created as a draft. To start the execution, the workflow should be published.

To save the workflow in draft state, perform the following steps:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow.
4. Click Group Configuration tab.

5. Click **Business Processes** or **Drills** or **Continuity** or **Events** tab depending upon the workflow type you want to configure.
6. Click on **Edit** icon against the workflow to edit it. The **Workflow Editor** page appears.
7. Click **Next**.
8. Click Save as a draft in the Publish Workflow page.

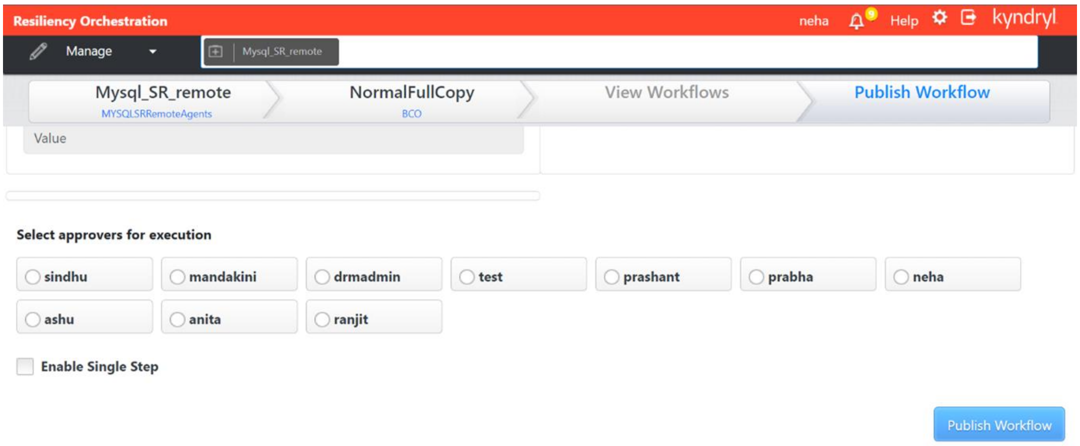


	Version Status	Execution Status	Dry Run Status
NormalFullCopy Template	DRAFT Version 0 Updated:	NOT EXECUTED	NOT EXECUTED
NormalCopy Pre-Packaged	DRAFT Version 0 Updated:	NOT EXECUTED	NOT EXECUTED
Failover Pre-Packaged	PUBLISHED Version 1 Updated: 25 Sep, 2023	NOT EXECUTED	NOT EXECUTED
Fallback Template	DRAFT Version 0 Updated:	NOT EXECUTED	NOT EXECUTED
FallbackResync Template	DRAFT Version 0 Updated:	NOT EXECUTED	NOT EXECUTED
ReverseNormalCopy Template	DRAFT Version 0 Updated:	NOT EXECUTED	NOT EXECUTED

Previewing Workflow

To preview a workflow, perform the following steps:

1. Click **Drills** > View Workflow Dashboard > Select Create New Workflow.
2. Select a group from the Group listing page.



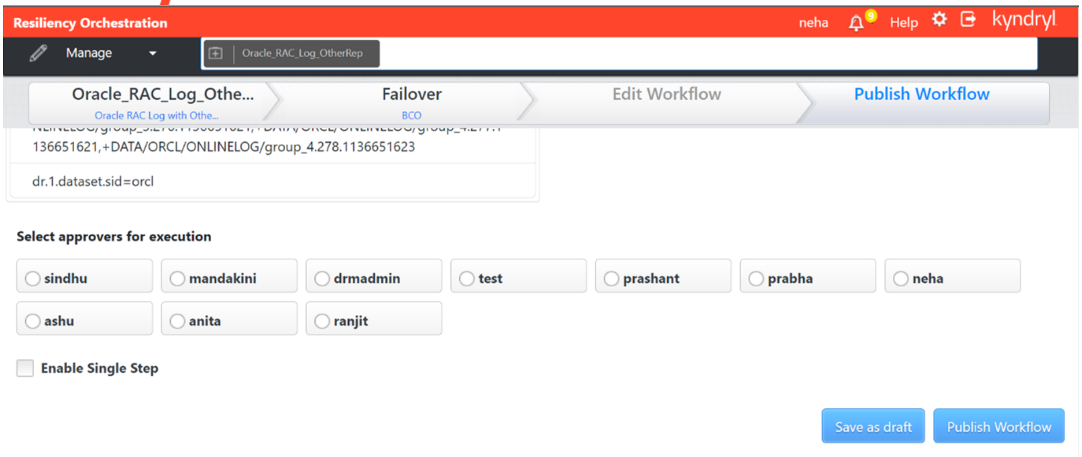
Select approvers for execution

○ sindhu ○ mandakini ○ drmadmin ○ test ○ prashant ○ prabha ○ neha

○ ashu ○ anita ○ ranjit

□ Enable Single Step

Publish Workflow



136651621,+DATA/ORCL/ONLINELOG/group_4.278.1136651623

dr.1.dataset.sid=orcl

Select approvers for execution

○ sindhu ○ mandakini ○ drmadmin ○ test ○ prashant ○ prabha ○ neha

○ ashu ○ anita ○ ranjit

□ Enable Single Step

Workflow Version History/ Rollback

- Workflow Version History is a new features added in Workflow Manager, the goal is to track the workflow level changes such as adding/deleting actions, updating workflow properties, also to track the action level changes within a workflow. Action level changes like action basic/advanced properties configuration, property values. Also to track any changes to the custom script by using the checksum compare feature between workflow versions.
- Every time a workflow is published, the workflow version is saved.
- Rollback is a new feature added to the Workflow Manager, is used to roll back the previous workflow configured.

To view the published workflow versions, perform the following procedure:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click Group Configuration tab.
5. Click **Business Processes** or **Drills** or **Continuity** or **Events** tab depending upon the workflow type you want to configure.
6. Click on **Edit** icon against the workflow to edit it . The **Workflow Editor** page appears.
7. Click on the **Version** button at the footer.

Field	Description
Version	Displays the version number of the corresponding published workflow.
Created on	Displays the timestamp of the corresponding published workflow.

Field	Description
By	Displays the user's name for the corresponding published workflow.
Rollback	This button is used to rollback a particular version.

Workflow Key Value List

Key-Value Pair

A Key-Value Pair (KVP) is a set of two linked data items: a key and its associated value.

A key-Value box (KVB) is a lookup table containing KV pairs. This can be configured through workflow configuration UI or through import of workflow XML.

KV pair can be used to provide inputs to RAL actions. Each RAL action publish their keys. During execution, if action finds its published key, then the action uses the associated value. For example, File Delete Operation Action defines PANFO_DELETE_FILE as the key to identify the file to be deleted. So during execution, the file identified by the key will be deleted.

Adding Key Value Pair

To add a key value pair to the Key Value List:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** page appears.
4. In the **Group Details** page, click **Group Configuration** tab. It further displays a list of tabs. The **Business Process**, **Drills**, **Continuity** and **Events** tabs allows to add a key value pair.
5. Click the desired tab and select any name (**BCO Name**, **Drill Name**, **Event ID**, **BUSINESS PROCESS NAME** column) in the group.
6. In the **Workflow Editor** page that opens, click the **Key Value Pairs** link. The **Workflow Key Value List** window opens.

   OR

   Click **Publish**, Publish workflow page appears. The **Workflow Key Value List** window opens.

Field	Description
Key	A key is a string that uniquely identifies a specific property of an object/entity. This field can contain only string datatype. Keys must begin with an alphabet, and must not contain whitespace.

Field	Description
Value	A Value is the data/property that is identified by its Key. This field can contain only string datatype. Click **Add** to enter the key and value to the Key Value List.
Key Value List	A Key Value List is a set of two linked data items: a Key, and its Value.

6. Enter the appropriate information in the relevant fields.
7. Click **Add key value** button to save the changes.

Group level Key Value configuration

Group level KV are the global key value at group level which will be available to all the Workflows in Test Exercise, Business Process and BCOs.

CLI to Add/Update/Delete group key value are available under $EAMSROOT/bin/ag_agent_test_client.zip

steps to add global kv (Add - operation)

1. Execute AGTestClient.sh script and type "groupkv".
2. It prompt you to enter operation 'Enter Add, Update, Delete operation of global KV', enter Add.
3. Enter the Enter Group Name under which you want to create global KV
4. Enter Key Name, e.g. MountPointList_DR_Redo and then Enter Values Name, e.g. /findb_redo1, /findb_redo2, /findb_redo3, click enter.
5. Your global KV will be saved.

Following are the steps to **update global key value** (Update - operation)

1. Execute AGTestClient.sh script and type "groupkv".
2. It prompt you to enter operation 'Enter Add, Update, Delete operation of global KV', enter Update
3. Enter the Enter Group Name under which you want to update global KV
4. Enter Key Name, e.g. MountPointList_DR_Redo and then Enter Values Name to be update, e.g. /findb_redo1, /findb_redo4, /findb_redo8, click enter.
5. Your global KV will be updated.

Following are the Steps to **delete global key value** (Delete - operation)

1. Execute AGTestClient.sh script and type "groupkv".
2. It prompt you to enter operation 'Enter Add, Update, Delete operation of global KV', enter Delete
3. Enter the Enter Group Name under which you want to delete global KV
4. Enter Key Name, e.g. MountPointList_DR_Redo and then for Enter Values Name, enter nothing , click enter.
5. Your global KV will be deleted.

Modifying Key Value Pair

To modify a key value pair:

1. Open the **Workflow Key Value List** window. For more information, refer to **Adding Key Value Pair**.
2. Select the key value pair you want to edit from the **Key Value List** field and click **Edit**.
3. Modify the key name in the **Key** field.
4. Modify the value for the key in the **Value** field.
5. Click **Add** to add the modified key value pair to the Key Value List.
6. Click **Add key value** to save the changes.

Removing Key Value Pair

To remove a key value pair from the Key Value List:

1. Open the Workflow Key Value List window. For more information, refer to Adding Key Value Pair.
2. Select the key value pair you want to delete from the **Key Value List** field.
3. Click 🗑icon to delete the key value pair from the Key Value List.
4. Click on Save now to save the changes

Note

Currently, removing all the key-value pairs associated with a workflow using the above procedure submits and empties the key-value list to the back-end, which will overwrite the existing values associated with a workflow.

Applying the Key Value

You can apply the user defined or pre-defined keys through UI or XML file.

Through UI:

1. Open the Workflow details page.
2. Click the **Action properties** tab of the relevant RAL action.
3. Use the pre-defined or user defined key.
4. Save the action.

Through XML:

1. Export the current workflow. The exported workflow is saved in XML format.
2. Open the XML file in text editor.
3. Write the XML tags using pre-defined or user defined keys.
4. Save the XML file.
5. Import the saved XML file.

Workflow Configuration Limitations

Following are the invalid/unsupported workflow configurations:

- A recurring action should not be configured with "Time to wait before executing this Action". The behavior is unpredictable if configured.
- An action within a recurring action group should not be configured with "recurrence interval". The behaviour is unpredictable if configured.
- In a workflow, an action group can contain only RAL actions, not another Action Group.
- Workflow should not be created where the success path and failure path of Actions/Action Groups forms loop/cycle. The behaviour is unpredictable if configured and user should not try to delete action/actiongroup using UI.

  For example, assume a workflow is being created with three actions (say A1, A2, A3). If A1's next action is A2 and A2's next action is A3 and A3's next action is either A1 or A2 then it forms a cycle/loop among the actions. Such configuration results in unpredictable behaviour like high CPU utilization resulting in software/system crash. If any workflow has cycle/loop then the only workaround is to import a new workflow without cycles/loops.
- From the UI, the maximum characters allowed in a workflow name are 24.

Configuring Approver List

To view the Workflow Details, go to **Adding Key Value List**.

The following steps can be performed to configure the Approver list.

1. In the Workflow Editor page, Click **Next.**
2. In Publish workflow page, select the checkbox to select the approvers for execution.
3. Click on Publish Workflow.

Note

- A user having privilege to create/modify a workflow can configure the list of 0 or more approvers. Only one of the approvers from the approver list can approve the workflow.
- Approvers selected will be user accounts who are associated with the concerned group.
- Any change made to the approver list of a workflow will be audit logged, mentioning the list of users who are approvers also.

Configuration

Configuring RPO/ RTO

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To configure RPO and RTO values for a Group, do the following:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.

2. Click Recovery Group tab, the Recovery Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click on Monitor / Manage icons to view the RTO and RPO tabs.
5. To configure **RPO/ RTO,** refer to Group Creation section in Resiliency Orchestration AD2C Service User Guide.

Configure the RPO/ RTO by providing following information:

Field	Description
Desired RPO	Enter the RPO goal for the application. **Note:** This field is mandatory and accepts numerals. The value is entered either in seconds, minutes or hours and maximum value that can be entered is calculated for a month (i.e. maximum value for seconds is 24 (hours in a day)*60*60*30 (per month)).
RPO compute Interval	Enter the time interval at which the RPO is computed by the system automatically. It is recommended that you have RPO compute interval value less than or equal to "Apply Log Interval" (as specified in the NormalCopy operation of the respective DR Solution supported). The RPO value is computed at an interval of not less than 5 minutes. **Note:** This field is mandatory and accepts numerals. The value is entered either in seconds, minutes or hours and the maximum value that can be entered is calculated for a month (i.e. maximum value for seconds is 24 (hours in a day)*60*60*30 (per month)). The value should always be greater than zero. This value differs according to the DR Solution type.

Field	Description
RPO deviation Threshold	Enter the RPO deviation value from the desired value by which an alert and an event is to be raised. **Note:** When RPO deviation percentage is greater than the configured value, an event is raised.

The properties of RTO are given below:

Desired RTO	Enter the RTO goal for the application. **Note** This field is mandatory and accepts numerals. The value is entered either in seconds, minutes or hours and maximum value that can be entered is calculated for a month (i.e. maximum value for seconds is 24 (hours in a day)*60*60*30 (per month)). Value should be always greater than zero.
RTO deviation Threshold	Enter the RTO deviation value from the desired value by which an alert and an event is to be raised. **Note** Valid range of values is 1-99 only. When RTO deviation percentage is greater than the configured value, an event is raised.

Uses Block based Replication	This field indicates that solution needs workflows for RTO Computation. By default, it is not checked. If the replication technology used for this group is block based, then user needs to check this. Any configuration where there is a setup requirement (like mounting volumes) before we can compute RTO, user needs to check this field and configure the RTO workflows. In such cases, a workflow is executed before and after RTO computation logic (Depending on value of "Start using RTO Computation Workflows" checkbox). For the customer environment where there is no necessity to run RTO workflow for computing RTO (For e.g. there is device provided that is always mounted on DR side), then user can leave this field unchecked. When checked, user gets option to configure the RTO workflows and option to start using workflows.
Start using RTO Computation Workflows	Checkbox indicates if RTO workflows are configured and ready to use. When checked, RTO workflows will be called before and after the RTO Computation logic. When it is not checked, then RTO calculation will use cached value of ETC (Expected time to complete) of some of the action that needs RTO workflows to be executed for ETC computation.

RTO computation is done at the same time when RPO is computed.

Configure the Data Lag Objective by providing following information:

Field	**Description**
Desired Data Lag Objective	Enter the Data Lag goal for the application. **Note** This field is mandatory and accepts numerals. The value is entered either in KB/ MB/ number of files.
Data Lag deviation Threshold	Enter the Data Lag deviation value from the desired value by which an alert and an event is to be raised. **Note** When Data Lag deviation percentage is greater than the configured value, an event is raised.

Note:

The minimum configurable value of RPO is 15 minutes.

Replication interval should be equal to or more than the dump log interval. Apply log interval should be equal to or more than the replication interval. Configured RPO should be more than dump log interval. Typically RPO should be double the dump log interval.

6. Click **SAVE** to save the configured properties of RPO and RTO.

RTO Workflow Support

Some of the solutions that need RTO workflow support, additional fields, 'Uses Block based Replication' and 'Start using RTO Computation Workflows' are shown, that user needs to configure. These are shown for following solutions.

- For all log based Solutions and application subsystems with Block based replication (like Hitachi Replication)
- DR Solution with Other Replicator
- DR Solution with Custom Replicator

User also needs to configure RTO workflows. Following are guidelines to configure the RTO workflows.

1. We recommend user to use 'no inform' for all actions. This is required so that workflow failure does not stop further execution of workflow during next RTO cycle. On failure, an event is raised that can alert user about failures.
2. User should not use GroupLock RAL Action in RTO workflows.
3. Success of workflow is based on availability of key 'PRE_RTO_STATUS'/'POST_RTO_STATUS' with value of 'SUCCESS'. If the key is not available or available with some other value, it is considered as failure. User implementing this workflow can insert an 'Assignment Action' at the end of success path to indicate workflow is successful.
4. Whenever Pre/Post workflow fails, a WARNING event is raised (BCSMGR_RPORTO4). If the event is not closed, then further failures of workflow would not raise BCSMGR_RPORTO4 event. Instead EVENTMGR02 is raised at regular interval.
5. PostRTO workflow is always executed if preRTO workflow is executed. This is irrespective of success or failure of preRTO workflow.
6. If pre RTO workflow fails, RTO would include cached value/default value for some of the actions that are dependent on RTO workflows.
7. While computing RTO, some of the actions are going to returned cached value for ETC. That means, these value would have collected at different timestamps. In such cases, RTO as of time is shown to be timestamp of ETC computed having oldest compute time. For e.g. If there are 2 actions in FO workflow, action1 has cached value collected at time 10 AM, action2 has ETC computed at current time (for eg. say 10:30 AM), then 'RTO as of time' value would be 10AM.
8. RTO workflows are 'system workflows' and would NOT be shown under 'Workflowlist' tab.
9. In reports page, these workflows are shown if 'Show System Workflow' checkbox is checked.

In addition to the above configuration, RPO and RTO values are specific to solutions. These specific values are configured depending on the type of the solution supported.

Configuring Notification Regarding Events

Click *Kyndryl Resiliency Orchestration Server User Role Management* to see the privileges.

To configure Notification regarding Events, perform the following:

1 Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.

2 Click **Recovery Group** tab, the **Recovery Group Listing** page appears.

3 Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.

4 Click the **Group Configuration** tab.

5 Click the **Events** tab.

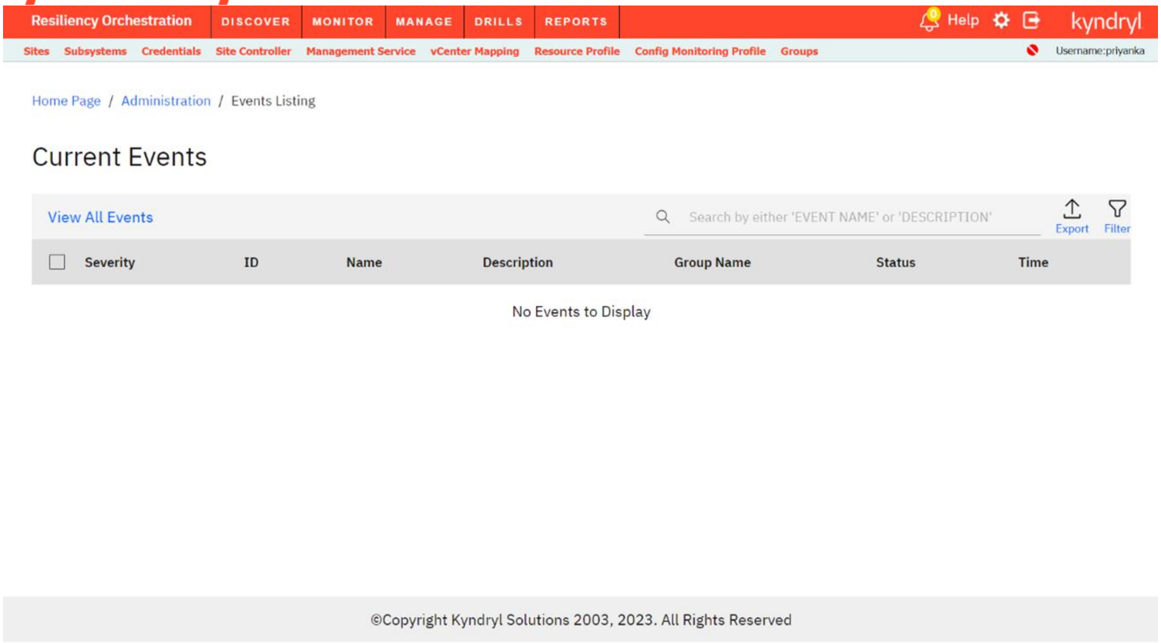
Field	Description
Event ID	Displays the respective Event ID which identifies each event.
Event Description	Provides a brief description of the respective event.
Event Severity	Displays the level of severity of the respective event.
Event Impact	Provides information on affect/effects about the event.
Notify	Allows you to send notification regarding the event to the user. By default, SERIOUS and CRITICAL events are notified.

6 Select the check boxes corresponding to the Events for which you want to notify the user on occurrence of it.

Note:

To receive notification regarding the event, at least one notification list must be associated with the group. For more information on creating the notification list, refer to Adding Notification List.

7 Click **Update Selection** button.



Current Events

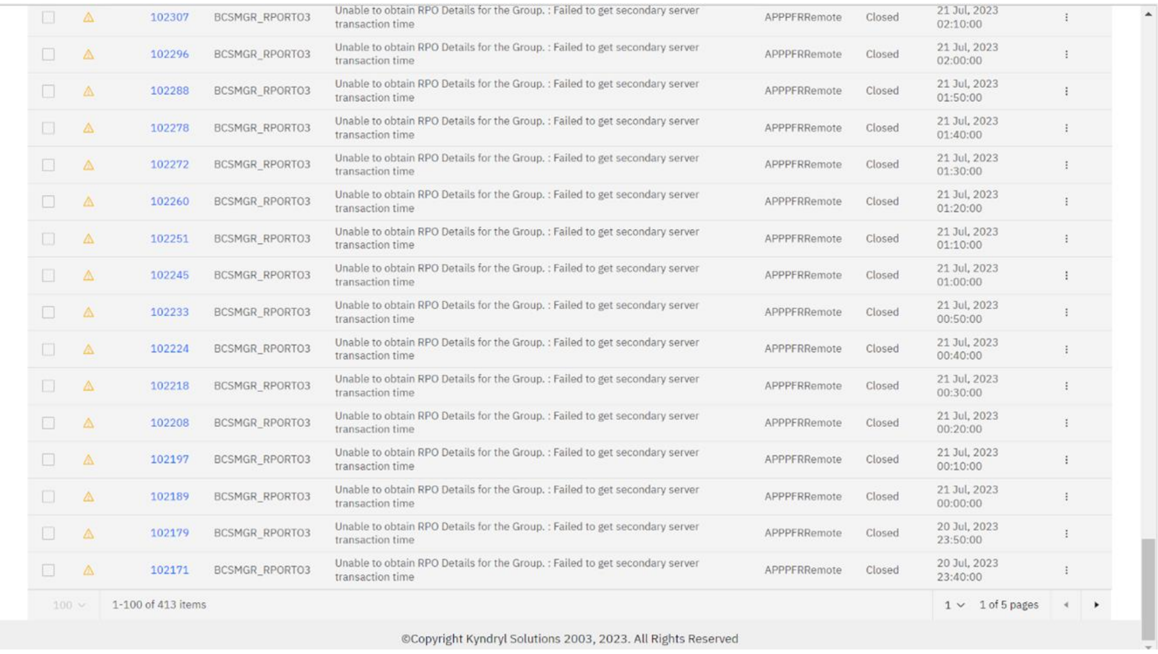
View All Events

Search by either 'EVENT NAME' or 'DESCRIPTION'

□ Severity	ID	Name	Description	Group Name	Status	Time

No Events to Display

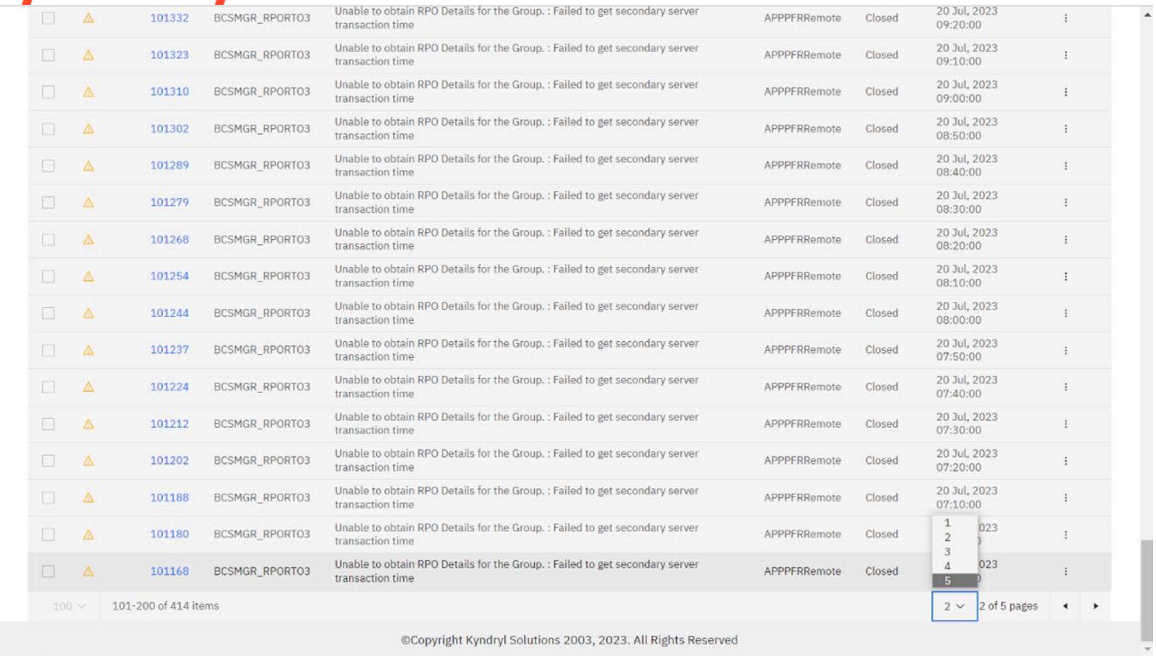
©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved



□	⚠	102307	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 02:10:00
□	⚠	102296	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 02:00:00
□	⚠	102288	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 01:50:00
□	⚠	102278	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 01:40:00
□	⚠	102272	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 01:30:00
□	⚠	102260	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 01:20:00
□	⚠	102251	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 01:10:00
□	⚠	102245	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 01:00:00
□	⚠	102233	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 00:50:00
□	⚠	102224	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 00:40:00
□	⚠	102218	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 00:30:00
□	⚠	102208	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 00:20:00
□	⚠	102197	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 00:10:00
□	⚠	102189	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	21 Jul, 2023 00:00:00
□	⚠	102179	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 23:50:00
□	⚠	102171	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 23:40:00

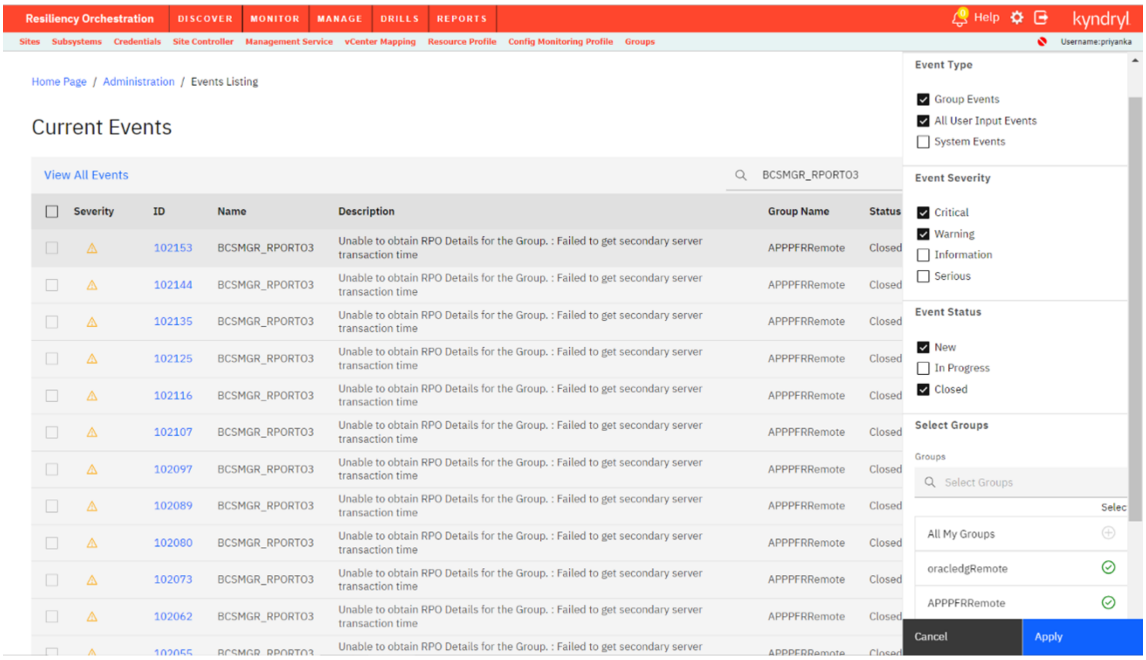
100 1-100 of 413 items 1 1 of 5 pages

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved



□	⚠	101332	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 09:20:00	⋮
□	⚠	101323	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 09:10:00	⋮
□	⚠	101310	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 09:00:00	⋮
□	⚠	101302	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 08:50:00	⋮
□	⚠	101289	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 08:40:00	⋮
□	⚠	101279	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 08:30:00	⋮
□	⚠	101268	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 08:20:00	⋮
□	⚠	101254	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 08:10:00	⋮
□	⚠	101244	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 08:00:00	⋮
□	⚠	101237	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 07:50:00	⋮
□	⚠	101224	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 07:40:00	⋮
□	⚠	101212	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 07:30:00	⋮
□	⚠	101202	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 07:20:00	⋮
□	⚠	101188	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	20 Jul, 2023 07:10:00	⋮
□	⚠	101180	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	023	⋮
□	⚠	101168	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed	023	⋮

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved



Current Events

View All Events

BCSMGR_RPORTO3

□	Severity	ID	Name	Description	Group Name	Status
□	⚠	102153	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102144	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102135	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102125	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102116	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102107	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102097	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102089	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102080	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102073	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102062	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server transaction time	APPPFRRemote	Closed
□	⚠	102055	BCSMGR_RPORTO3	Unable to obtain RPO Details for the Group. : Failed to get secondary server	APPPFRRemote	Closed

Event Type

- ☑ Group Events
- ☑ All User Input Events
- □ System Events

Event Severity

- ☑ Critical
- ☑ Warning
- □ Information
- □ Serious

Event Status

- ☑ New
- □ In Progress
- ☑ Closed

Select Groups

Groups

Select Groups

All My Groups	⊕
oracledgRemote	✓
APPPFRRemote	✓

Configuring Event Policy

Events or Incidents occur as a consequence of a problem with Components, Datasets or Protection Schemes. A Group is configured with all possible Events/Incidents depending up on the solution type.

Click *Kyndryl Resiliency Orchestration Server User Role Management* to see the privileges.

General Definitions:

Field	Description
Event	A casualty resulting in production data down. An incident is an event with the highest severity level (threat level).
Incident	Consequences as a result of something happened on an object.

To configure Events, perform the following:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click the **Recovery Group** tab, the **Recovery Group Listing** page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** page appears.
4. Click the **Group Configuration** > **Events** tab.

This tabbed page lists the Event ID, it's description, severity and impact. You can select the check boxes corresponding to the events for which you want to send notification to the user.

5. Click the Event ID link corresponding to the Event you want to configure. The **Event Configuration Details** page is displayed providing information on the Event's configuration along with the Policy Set Details as given below:

Field	Description
Configuration for Event	
Group Name	Displays the Group name.
Event ID	Displays the respective Event ID which identifies each event.
Severity	Displays the level of severity of the respective event.
Is_ Alertable	Events whose alertable is true will be displayed in the UI
Description	Provides a brief description of the respective event.
Event Impact	Provides information on affect/effects about the event.
Impact_group status	Displays the impact of the event on the group status.
Notify Update Selection	Select the checkbox to notify the updates

A Policy Set is defined as a combination of actions with respect to both day and night policy. The **Policy Set Details** displays the following information:

Field	Description
POLICY	Displays the policy name Note: There can be multiple instances of same Event raised for a Group that require execution of same policy. However, only one instance of a policy can run at a time. In such cases, the later instances of the event are put to FAILED status. For example, there are three instances of Event E- E1, E2, and E3, raised for Group G, requiring the execution of policy P. If P is being executed for E1, its execution for E2 and E3 will be put to FAILED status. Once the policy execution for an Event is put to FAILED status, it cannot be initiated again. Instances of same event for different Group do not affect each other.
TIME OF DAY	Gives time of day when this policy will be effective. (Currently, the time of day is always 24 hours). For example, the policy page shows a timing gap of '00:00 to 23:59' hours, which ultimately mean that the workflow, will get executed when the incident occurs at any time with in the given range of a day.
WORKFLOW NAME	Displays the workflow name which is always associated to the policy.
POLICY EXECUTION MODE	You can set this field to **Manual** or **Auto**. Manual selection requires your intervention to execute a policy.

6. Click workflow name link under **WORKFLOW NAME** column to configure the workflow associated to the policy.

Adding Polar Event Script

This tool is used to manually add the polar cancellation to the events for which polar cancellation is not implemented.

The key features of this tool are:

- Group Status is based for events from 7.0 and we need to have polar cancellation for all the events that are raised.
- For events which do not have polar cancellation add them manually.

The line of code to execute this tool in cancellation is:

```
EAMSROOT/bin/ AddPolarEventsMapping.sh
```

The typical output on execution of this code is :

```
./AddPolarEventsMapping.sh -e BCSSybaseLogEvent021 -c
BCSSybaseLogEvent014
configFile::: /opt/panaces/installconfig/PanacesAgent.cfg
logFileName::: AddPolarEventsMappingCLI
result::: null
level::: 7
eventName=BCSSybaseLogEvent021 polarEvent=BCSSybaseLogEvent014
Polar Mapping Added Successfully...
```

Note:

When BCSSybaseLogEvent014 is raised it will close BCSSybaseLogEvent021.

Site Ticker

To view the Site Ticker page information, perform the following steps:

- Click **Admin** on the navigation bar. The **Administration** page appears. Scroll down to the **Site Ticker** and click **Go to Site Ticker**. The **Site Ticker** page appears.
- The Site Ticker page displays the following table:

Field	Description
Name	Select the Site name from the dropdown list
Description	Displays the information of the Site
From	The Ticker will be enabled from that time
To	The Ticker will be disabled after that time
Updated by	Updated user
Updated on	Updated time

Show Expired Ticker

On clicking the **Show Expired Ticker**, the Expired Site Ticker table is displayed.

Add Site Ticker

To add a Site Ticker, click on the **Add Site Ticker** button. A table is displayed.

Field	Description
Name	Select the Site name from the drop-down list

Field	Description
Description	Provide the description
To	Select the date from the Calendar
From	Select the date from the Calendar

Click **Create** to create the new site.

Click **Close** to cancel the current operation.

Note

The Site ticker count can be viewed for the DR, PR and SCC sites by clicking **Monitor** OR **Manage** on the Navigation bar and then clicking the **Sites** tab.

Vault Framework

Introduction

About Vault Framework

Vault is a password management software and its goal is to help organizations secure, manage and track credentials for sensitive data and critical systems. Centralized management of passwords at different levels, such as the operating system, database and application level makes this highly effective and efficient.

The Vault Framework is a high-level framework that provides reusable business logic for clients to integrate their applications, GUI controls and workflows with different Vault algorithms. Extensive vault components enable seamless integration with the client's applications. The Framework provides enough flexibility to the clients to design an approach that suits their requirements.

The next section provides Vault components, providers and functionalities common to any Vault.

Vault Artefacts: Vault artefacts are essential for Kyndryl Resiliency Orchestration to communicate with any vendor specific Vault.

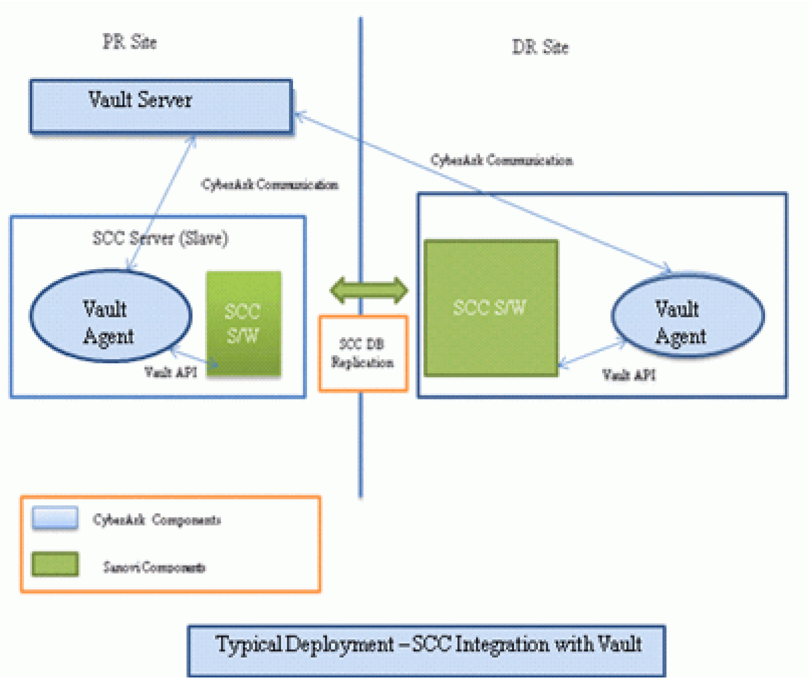
- Connection Parameter: Connection parameters are static for a specific vault. They must be configured and can be seen in the Kyndryl Resiliency Orchestration GUI, under **Discover > Credentials > ConfigureVault.**
- Query Parameter: Query parameters are different for every subsystem. They must be configured and can be seen in the Kyndryl Resiliency Orchestration GUI, under **Discover > Subsystems > Components, Discover > Subsystem > Datasets** and **Discover > Subsystem > Protection Schemes**, when you select the Vault Type and select the **'Fetch from Vault'** option.

Vault Providers: Vault providers are the APIs, JARs and Binaries that need to be configured on the server and are specific to the Vault**.**

Vault Features: The following features are common to every vendor specific Vault software. For more information on vault features refer to Vault Features

- Password Management and Password Caching: With password management, the Vault agent encrypts the password for Kyndryl Resiliency Orchestration and decrypts the password just before making a call to the underlying system. The passwords are cached at regular intervals and also get updated every time there is an inconsistency of password in the Vault and the cache.
- Locking Agents Mechanism: The locking mechanism is applicable for subsystems configured with Vault. The locking mechanism. The locking mechanism is designed such that the agent locks all the calls to the underlying subsystem the moment a cred fail is encountered. This avoids locking the underlying subsystem user to a great extent.

Integration with Kyndryl Resiliency Orchestration



Typical Deployment – SCC Integration with Vault

With minimal configuration, Kyndryl Resiliency Orchestration integrates with vendor specific Vault for clients who have implemented Vault password management software. Kyndryl Resiliency Orchestration passes the connection parameters and query parameters to the Vault Agent. The agent executes the **tcl** script. This script acts like a medium between the Vault agent and the Vault. All the required parameters to make request to the vendor specific Vault are available with the **tcl** file. The TCL script will call the relevant Vault APIs, establish communication (connection to the configured Vault server), and serve the (password) requests from the Vault agent.

This integration has the following benefits:

1. It ensures that the user does not have to manually enter the username and password to login to the Kyndryl Resiliency Orchestration GUI.
2. Change in password in any of the Vault integrated client systems does not have an impact on the Resiliency Orchestration Application as these changes are recognized by Vault and the latest correct password is pushed to Kyndryl Resiliency Orchestration GUI.

Configuring Vault

This section provides steps to integrate any Vault algorithm with Kyndryl Resiliency Orchestration. The following table provides references to sample files and folders required to complete the integration smoothly. The reference files are available at.

File Name in the Document	Reference File Name
PanacesAgentGeneric.cfg	PanacesAgentGeneric.cfg

Panaces.Properties	panaces.properties
TestVault_config.xml	cyberark_config.xml
TestVault.tcl	cyberark_vault_connector.tcl

Vault Properties

Provisioning from the Customer

- Vault software should be installed and configured at the customer datacenter. This includes installing **Providers**, which are software modules from Vault for Application integration with Vault. The Customer needs to install Vault providers on Resiliency Orchestration Server (This is the server where Resiliency Orchestration Management application is running). If there are two Kyndryl Resiliency Orchestration Servers for High Availability, then Vault providers need to be installed on both the Resiliency Orchestration servers.
- Customer needs to provision the vault such that the providers that are installed on Resiliency Orchestration server have access to the vault where passwords are stored and have access to all the passwords that are required Resiliency Orchestration software.
- Kyndryl Resiliency Orchestration software should be qualified for Vault 7.1 release.
- Customer should have Vault 'provider software' licenses for RHEL 5.0.
- Customer should export the Vault installation path in the current user profile to establish communication between the Vault **Provider** and the Kyndryl Resiliency Orchestration Server. For Eg.: If the CyberArk is installed at /opt/CARKaim then the end user should export the path in the user profile as 'CARKAIM_HOME=/opt/CARKaim'.

Other Prerequisites

- Version, 7.1 must be installed.
- Set parameter IS_SERIALCALL_ENABLED=true in <EAMSROOT>/installconfig/PanacesAgentGeneric.cfg. By default it is false. Make this change for local agents as well.
- Set parameter Kyndryl.vault.agent.onstartup = true in <EAMSROOT>/installconfig/panaces.properties. By default it is false.

Configuring Vault Properties

1. Login to the Kyndryl Resiliency Orchestration Server and open folder $EAMSROOT/installconfig. You will see the Panaces.Properties file.
2. Update the values for the properties in the file as mentioned in the following table. The values mentioned in the table are default values and can be changed by the user.

Property Name	Default Value	Description
sanovi.vault.cred.refetch	10 minutes	This is the time interval in minutes to fetch the password from vault. This is the time interval in minutes between password fetches from vault. The passwords from Vault for the vault supported subsystems are encrypted and cached in Resiliency Orchestration server at regular configured time intervals. This is the default value.
sanovi.vault.lock.waittime	2 minutes	This is the wait timeout in minutes at the agent side. If the agent does not get new password in 2 minutes, the agent throws an exception that it did not receive new password and still continues to wait. This is the default value.
sanovi.vault.credcache.firstUpdateWaitTime	60 seconds	During the server start up, passwords for subsystems that are vault supported are fetched from vault and cached in memory. This is the wait time, where EAMS server pauses for this wait time before the passwords are fetched from vault and cached. At Panaces Server startup, the Panaces server is paused for a configured period of time. The Vault Agent gets the passwords of all the configured subsystems that are vault supported from Vault and the encrypted passwords are cached in Resiliency Orchestration. This is the default value.
sanovi.vault.credcache.updatecred	true	This is a Boolean property, when set to true, Password caching is enabled. Passwords for subsystems that are vault configured are fetched from vault and cached in memory. DB caching is removed. None of the passwords fetched from vault are saved in DB. By default, password caching is enabled. This needs to be turned off if vault is not configured. The cache always has encrypted passwords. If this property is set, all subsystems (when required) will look for passwords from cache first and then from vault if not found in cache. This is the default value.

Property Name	Default Value	Description
sanovi.vault.credcache.cacheUpdateInterval	3600 seconds	This is the interval in seconds, where a cron job runs to fetch passwords for vault supported subsystems and caches in the memory. This cron job runs only if password caching is enabled. Default interval is kept as 1 hr (3600 sec). This interval ideally should be more than 1 hr (ex: 24 hrs). Also, should be more than the interval mentioned in other properties, Kyndryl.vault.cred.refetch and Kyndryl.vault.lock.waittime.
sanovi.vault.enableEncryption	true	This property is used to enable password encryption in Resiliency Orchestration. Default is set to 'true'. When enabled, Kyndryl Resiliency Orchestration encrypts all the passwords received from Vault and the same are cached in Resiliency Orchestration if caching is enabled. This is the default value.
sanovi.vault.agent.onstartup	false	This property enables Vault agent to be started before other remote agents start. If this is set to true, the Panaces server is paused for some time, till the Vault Agent starts. If this is set to false, the Panaces server will not be paused till the Vault Agent starts, and the Vault agent gets started along with all other remote agents. By default, this property is set to false. This property needs to be set to true if the client is using Vault. Note: This property was introduced in Vault Version 2.0
network.disconnect.threshold	2 minutes	This property enables Vault to raise the network down event after the specified time has lapsed after the network has gone down.

Configuring New Vault

This section provides instructions on configuring a new vault.

Note: To configure a new Vault, for example 'TestVault' in Kyndryl Resiliency Orchestration Server using TCL, create a new folder 'TestVault' under $EAMSROOT/agent/vault/ and follow the steps below.

1. Login to the Kyndryl Resiliency Orchestration Server

2. Create the following sub-folders under **<EAMSROOT>/agents/vault/TestVault** folder.

   1. /config/
   2. /lib/
   3. /script/

3. Create a new vault configuration xml called **TestVault_config.xml (the name of the xml can be anything) and place it under <EAMSROOT>/agents/vault/TestVault /config/ TestVault_config.xml**

   Note: Refer to the cyberark_config.xml file in the attachment.

4. The parameter 'VaultType': This is the name of the Vault. This should be same as the folder name. Here the Folder name is TestVault so the vault type inside the TestVault_config.xml must be 'TestVault'.

   For Example: <VaultType>TestVault</VaultType>

5. The parameter '**ConnectionParameter's**: Add each connection parameter required to connect to the Vault. Provide '**Name'**, '**Unique Id**' and '**Description'** for each connection parameter. **'Type'** is not being used currently.**Sensitive** is a new XML (optional) element if not defined,content is plain text by default. All the connection parameters configured here appear as mandatory fields while configuring a Vault.

   For Example:

   <Name>: 'Provider Port', 'Application ID' and 'Provider Timeout' are the query parameters provided by Cyberark.

   <UniqueId>: Unique alias needs to be provided for each query parameter

   <Description>: Description for each parameter

   <Type>: It is currently not being used

   <Sensitive>: if value is true the data(in the UI) needs to be masked.

```
<ConnectionParameter>

                <Parameter>

                        <Name>Provider Port</Name>

                        <UniqueId>CYBERARK_PROVIDER_PORT</UniqueId>

                        <Description>CyberArk Provider Port</Description>

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


                </Parameter>
                <Parameter>

                        <Name> Application ID</Name>

                        <UniqueId>CYBERARK_APPLICATION_ID</UniqueId>

                        <Description>CyberArk Application ID</Description>

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

                            <Sensitive> true </Sensitive>

                </Parameter>



            <Parameter>

                        <Name> Provider Timeout</Name>
        <UniqueId>CYBERARK_PROVIDER_TIMEOUT</UniqueId>

                        <Description>CyberArk Provider Timeout</Description>

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

        </Parameter>

        </ConnectionParameter>
```

Note: Connection parameters are the parameters required to connect to a vault and provide unique id to each parameter. These parameters are specific to specific Vaults. The Vault Vendor must provide these parameter names.

6. The parameter '**QueryParameter'**: Add each query parameter required to fetch password form Vault. Provide '**Name'**, '**Unique Id'** and '**Description'** for each query parameter. '**Type'** is not being used currently. All the query parameters configured here appear as mandatory fields while configuring a subsystem to use Vault.

    Example:

<Name>: 'Safe Name' and 'Object Name' are the query parameters provided by Cyberark.

<UniqueId>: Unique alias needs to be provided for each query parameter

<Description>: Description for each parameter

<Type>: It is currently not being used

```
<QueryParameter>
```

```
        <Parameter>
                <Name>Safe Name</Name>
                <UniqueId>CYBERARK_SAFE_NAME</UniqueId>
                <Description>CyberArk Safe Name</Description>
                <Type>String</Type> <!-- Number/Text -->
        </Parameter>
        <Parameter>
                <Name>Object Name</Name>
                <UniqueId>CYBERARK_OBJECT_NAME</UniqueId>
                <Description>CyberArk Object Name</Description>
                <Type>String</Type> <!-- Number/Text -->
        </Parameter>
</QueryParameter>
```

Note: Query parameters are the parameters required to fetch password from vault and provide unique id to each parameter. These parameters are specific to specific Vaults. The Vault Vendor must provide these parameter names.

7. Verify that the parameter <**Connector**> in the **TestVault_config.xml** is **<Connector>panaces.agents.vault.vaultagent.vaulttclconnector.VaultTclExecutor</Connector>**
8. Create a new **tcl** file, **TestVault.tcl** under **<EAMSROOT>/agents/vault/Arcos/script/**

   Note: Refer to the sample cyberark_vault connector.tcl file

9. Modify the parameter **<args>** in the **TestVault_config.xml** to point to the newly created **tcl** file. This absolute path must be mentioned.

For Example:

<args>/agents/vault/TestVault/script/TestVault.tcl</args>.

Note: Also, refer to sample cyberark_config.xml file

args tag should be relative path starting from /agents

Refer to the sample cyberark_vault connector.tcl file

To get the configured parameter in Kyndryl Resiliency Orchestration in your TCL

Call set parameter = [getKeyValue "UniqueID configured in xml "]

For Example:

set providerPort [getKeyValue "CYBERARK_PROVIDER_PORT"]

Note: Please refer set sample cyberark_vault connector.tcl file

10. Add all vault specific libraries required to connect to vault to be kept under <EAMSROOT>/agents/vault/TestVault/lib

    Note: Refer to the attached zipped lib folder to understand the file structure and all the files in the lib directory.

What goes in the TestVault.tcl file?

Note: If Config file has Sensitive= true for any connection parameter DO NOT print values of fields marked as sensitive in the log.

Note: Refer to sample cyberark_vault_connector.tcl file

1. Refer to the **<EAMSROOT>/agents/vault/TestVault/config/TestVault_config.xml** while creating the tcl file.
2. Create variables for each connection parameter mentioned in xml under **#Connection** parameters.
3. Create variables for each query parameter mentioned in xml under **#Query** parameters.
4. Using all parameters make vault specific API call and Set the retrieved password using the statement **setPassword $password.**

    Note:

    In case of failure, raise appropriate exception by using raiseVaultConnectionException or raiseUnableToGetPwdException method.

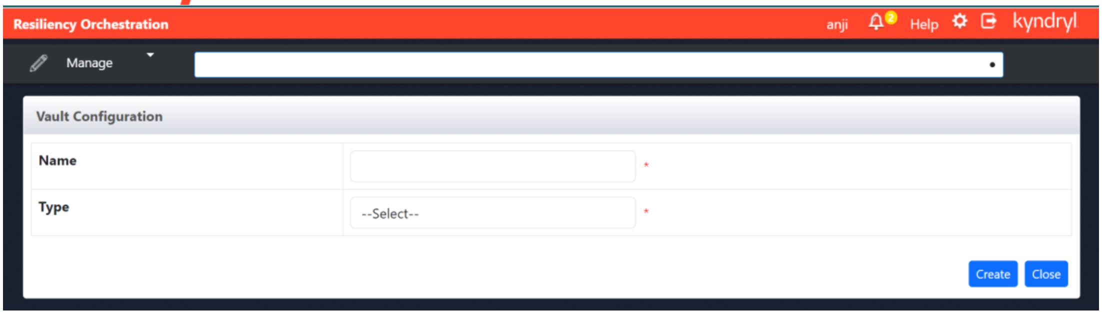
    raiseVaultConnectionException should be called when we are not able to connect to vault.

    raiseUnableToGetPwdException should be called when system is able to connect but not able to retrieve password.

    In case you are not able to distinguish the error then call raiseVaultConnectionException with proper error message.

Configuring Vault with Kyndryl Resiliency Orchestration GUI

1.Login to Kyndryl Resiliency Orchestration, go to the **Discover > Credentials** tab and click **ConfigureVault** and the following screen appears.



Vault Configuration

Name	*
Type	--Select-- *

Note: The configured Vault type will appear in the drop-box. For Example: CyberArk is shown in the above picture. The parameters shown (Provider Port, Application ID, Provider Timeout) are from the config.xml, for example : TestVault_config.xml.

2. For more information on the field values see the table below. The **Name** and **Type** are static fields. The rest of the fields depend on the type of Vault. The Vault vendor must provide information about these fields.

Field Name	Description
Name	Vault name you want to configure. This is a mandatory field. Provide a unique name.
Type	You can select the Vault type from the drop-down list. This list will display the vaults that are configured in the 'Configuring New Vault' step mentioned above. This is a mandatory field
Provider Port	This is a mandatory field. Vault Vendor to provide the value to connect to the Vault.
Application Id	This is a mandatory field. Vault Vendor to provide the value to connect to the Vault.
Provider Timeout	This is a mandatory field. Vault Vendor to provide the value to connect to the Vault.

3. Click **Create**. The system takes you to the **Credentials Listing** Page.

Configuring Subsystems to use Vault with SCC GUI

Configuring Components with Kyndryl Resiliency Orchestration GUI

Note: This step associates the subsystems to the respective Vaults. You need to define the Component.

Configuring Components

1. Click the **Discover > Subsystems** tab and the following **Subsystems Listing** Page screen appears.
2. Select a **Component Subsystem** from the **Create New** drop down list box and click **Go** and the following screen appears.
3. Enter all the field information.

   Note: Check the 'Fetch from Vault' check box and select the vault you want to associate to the component subsystem.

4. Click on **'Test Credentials'** to test the Vault Connectivity. The test credentials should pass if Vault is configured properly.
5. Click **Save**. The system takes you to the **Subsystems Listing** Page.

Configuring Datasets with Kyndryl Resiliency Orchestration GUI

Note: This step associates the subsystems to the respective Vaults. You need to define the Datasets.

Configuring Datasets

1. Click the **Discover > Subsystems** tab and the following **Subsystems Listing** Page appears.
2. Select a **Dataset Subsystem** from the **Create New** drop down list box and click **Go** and the following screen appears.
3. Enter all the field information.

   Note: Check the 'Fetch from Vault' check box and select the vault you want to associate to the dataset subsystem.

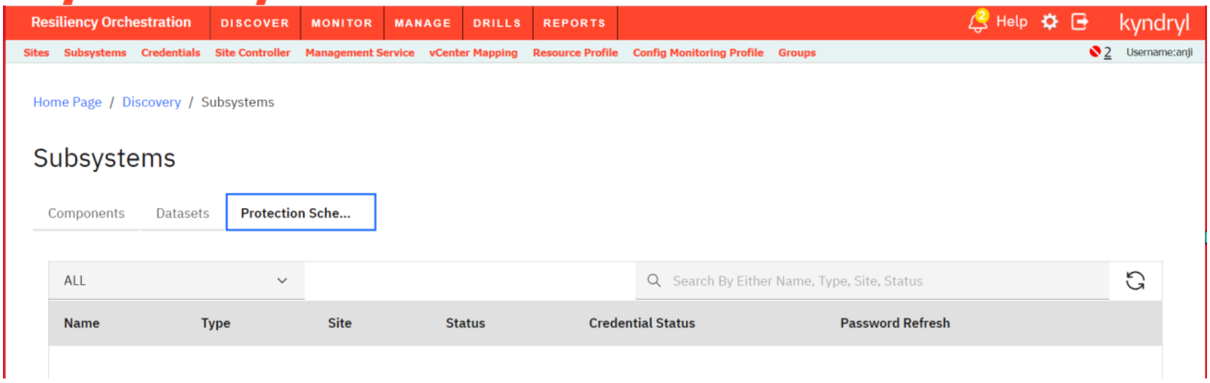
4. Click on 'Test Credentials' to test the Vault Connectivity. The test credentials should pass if Vault is configured properly.
5. Click **Save**. The system takes you to the **Subsystems Listing** Page.

Configuring Protection Schemes with Kyndryl Resiliency Orchestration GUI

Note: This step associates the subsystems to the respective Vaults. You need to define the Protection Scheme.

Configuring Protection Scheme

1. Click the **Discover > Subsystems** tab and the following **Subsystems Listing** Page appears
2. Click on the **Protection Scheme Subsystem**



Name	Type	Site	Status	Credential Status	Password Refresh

3. Enter all the field information.

   Note: Check the 'Fetch from Vault' check box and select the vault you want to associate to the protection scheme subsystem.

4. Click on '**Test Credentials'** to test the Vault Connectivity. The test credentials should pass if Vault is configured properly.

5. Click Save. The system takes you to the Subsystems Listing Page.

Vault Agent

Note: The Starting of the Agent is not necessary because the Vault Agent starts by default when Kyndryl Resiliency Orchestration Server starts as a remote agent and can be seen in the Agent Listing page in Kyndryl Resiliency Orchestration GUI. You will need to manually Start it only if the Agent does not start for some reason.

Explicit Start/Stop of Vault Agent:

- The Vault Agent can be started and stopped from the 'Agent Listing' page. If Vault Agent is stopped explicitly through 'Agent Listing' page, the subsequent Kyndryl Resiliency Orchestration Server startup will not start the Vault Agent.
- The Kyndryl Resiliency Orchestration Server pauses for a maximum of two minutes, for Vault Agent to start first. If the Vault Agent does not start during that time, Kyndryl Resiliency Orchestration server continues to start without the Vault Agent. In that case, the Vault agent needs to be started explicitly from 'Agent Listing' page.
- Alternatively, the following property in panaces.properties can be used to pause Panaces Server till all remote agents are started.**panaces.server.startupDelayForAgents = 0**

The above property can be used to pause the panaces server till all the remote agents are started and connected. A value for this property makes sure that all remote agents including the vault agent are started and connected before the panaces server starts.

Any of the following options can be used to Start or Stop the Vault Agent explicitly.

Option 1

VaultAgent Start:

```
<EAMSROOT/bin>
./VaultAgent.sh    start     <RESILIENCY_ORCHESTRATION_IP>    LINUXSERVER
```

VaultAgent Stop:

```
<EAMSROOT/bin>
./VaultAgent.sh     stop     <RESILIENCY_ORCHESTRATION_IP>    LINUXSERVER
```

VaultAgent Status:

```
<EAMSROOT/bin>
./VaultAgent.sh   status   <RESILIENCY_ORCHESTRATION_IP>  LINUXSERVER
```

Option 2

1. Login to Kyndryl Resiliency Orchestration.
2. Click ⚙icon and click **Go to Agents.**
3. Click **Stop** next to the **Vault Agent Staus** column to stop the AgentOR click **Start** next to the **Vault Agent Status** column to start the Agent.

   Note: The Status column will show the status of Vault.

Java Heap Settings for Vault Agent:

By default, Xms and Xmx are set to 64 MB each. The heap memory can be modified in the script, VaultAgent.sh.

On Vault agent crash, a dump file is created at $EAMSROOT on Resiliency Orchestration server for further analysis.

Vault Features

Locking Agents Mechanism

Note: For agent locking to work, the agents have to be upgraded to 7.0.

Agent connectivity behaviour to underlying OS or DB

The locking mechanism is designed such that the agent locks all the calls to the underlying subsystem the moment a cred fail is encountered. This avoids locking the underlying subsystem user to a great extent.

As soon as the Agent fails to connect to underlying system with invalid credentials, it will be treated as login failure and the corresponding Resiliency Orchestration or Agent Monitoring call will fail. The subsequent connection to underlying system will be blocked. A message will be issued to the server to issue the latest password from Vault.

All the calls to agents are blocked until new password is pushed.

OR

All the waiting calls automatically get timed out after the configured time set in the property. **Kyndryl.vault.lock.waittime = 2 minutes**

For more details on the various configurable properties refer Configuring Vault Properties.

There are 2 mechanisms to push passwords for only failed accounts from Vault to the agents through Resiliency Orchestration.

Auto Refresh:

In the Auto Refresh mechanism, the Resiliency Orchestration server pushes the passwords for only failed accounts at regular intervals of time.

Resiliency Orchestration server will maintain a retry interval property in panaces.properties file. Using this property Resiliency Orchestration server will issue a re-fetch password instruction to vault agent and then retry login.

This interval of time is configured in panaces.properties using the property **Kyndryl.vault.cred.refetch = 10 minutes.**

Resiliency Orchestration server fetches the passwords for the failed accounts every configured 'X' minutes of time from Vault. Resiliency Orchestration server pushes the fetched password only if the fetched password and the password with which the agents have failed are not same. If they are same, the agents continue to wait and Resiliency Orchestration server will try again after 'X' minutes of configured time.

Once the new password is pushed, all the blocked operations at the agents will resume. If the agents do not get new passwords, all the blocked operations will continue to be blocked OR will resume automatically on a time out with an exception.

Refresh Button:

When authentication failure takes place at the agent level, the Refresh button Refresh, in the **Subsystems Listing** Page against each respective subsystem is enabled and all the calls to the corresponding agent are blocked. On clicking the Refresh button, the password from Vault is sent for the failed account to the respective agents.

Use Case 1:

When the component creds are used with DataSet and Protection Scheme, the refresh button will only be enabled at the component level, however the cred will fail (✗) at component, dataset, and protection scheme.

Use Case 2:

When **'Fetch from Vault'** is used across the subsystems the refresh button will be enabled for **Component**, **Dataset** ,and **Protection Scheme**. All three must pass the test credentials.

Use Case 3:

When a **Group Credential** is configured with vault and used across **Component**, **Dataset,** and **Protection Scheme**, the Refresh button will appear for all the subsystems and must pass the respective test credentials.

User Case 4:

When the subsystem's password is changed during workflow execution, the workflow will fail with an Awaiting Input error message.

To continue the execution of the workflow, the following steps must be done.

1. Make the subsystem active – Following are 2 ways to make the subsystem active
   a. Click the 'Refresh' button against the subsystem. This will explicitly push the password from Vault to the subsystem and should make the subsystem active if the password is correct.

      Note: It is assumed here that passwords in Vault and Subsystem are in sync.

   b. Wait for AutoRefresh to happen – Auto refresh automatically pushes the password from Vault to the subsystem if there is a change in the password.
2. Wait for the subsystem to become active
3. Retry the failed workflow – Click the 'Retry' button to continue with the workflow.

Note: Clicking the Refresh button multiple times with wrong password in Vault may lock the underlying subsystem.

Once the Refresh button is clicked the password from Vault is pushed to the respective agent and the button will get disabled. If agents fail again with the pushed passwords, the button will become enabled again for failed subsystems.

FAQs:

1. When can I view the Refresh button in the UI?

The Refresh button is visible only when there is an authentication failure for the subsystem.

2. When is the Refresh button enabled?

The Refresh button is visible only when there is an authentication failure for the subsystem.

3. When will the Refresh button be disabled?

This functionality presently does not exist.

> Note: Workflows/RALs configured with TCL/Shell script which have Group Credentials/Credentials as a part of the script, which bypass the agent and connect directly, do not aid the agent to track and control the connections to the underlying subsystem, hence locking at the agent level when the credentials fail is not possible.

Password Management and Password Caching

The password exchange between the Vault Agent, Kyndryl Resiliency Orchestration and the Subsystems is encrypted. The vault agent will always return the password in an encrypted form. The Resiliency Orchestration is unaware of the actual password and does not try to interpret or decrypt it. It supplies the encrypted password to the agents. The agent decrypts the password just before making a call to the underlying system.

To enable caching, refer Vault Properties.

The passwords are cached at regular intervals. The cache is updated only when the password fetched from vault and the password in cache are different.

The logger "Schedule update: Cred cache:" shows the cached passwords (this should be encrypted) at regular intervals of time. The default is 3 minutes so the Cache Update Job will run every 3 minutes.

The logger "Placing credentials in memory for:" shows when subsystems select passwords from memory

To verify the password from cache, check the log. It should print "Fetching credentials from memory for:..."

Subsystems Kyndryl Supports

The subsystems that Kyndryl supports the Vault Framework for are listed below.

- Windows
- AIX
- HPUX
- Linux
- Solaris
- DB2
- MSSQL
- Oracle
- Sybase
- Oracle DG
- Vcenter

Dashboards

The Kyndryl Resiliency Orchestration application provides you with different types of Dashboards, where you can view details of the applications that are managed by the Kyndryl Resiliency Orchestration application. You can find details of the applications that are managed by different Kyndryl Resiliency Orchestration Servers across geographically distributed sites.

The information is captured and presented graphically as Widgets, and details are displayed for the selected application in the Dashboard.

The following types of dashboards are available for viewing that depend on the role of the user:

- **Operation Dashboard**
- **DR Manager Dashboard**
- Cyber Data Dashboard
- Cyber Platform Configuration

For details about the Cyber Platform Configuration Dashboard, refer to the Cyber Incident Recovery for Platform User Guide. For details about the Cyber Data Dashboard, refer to the Cyber Incident Recovery for Data user guide.

Operation Dashboard

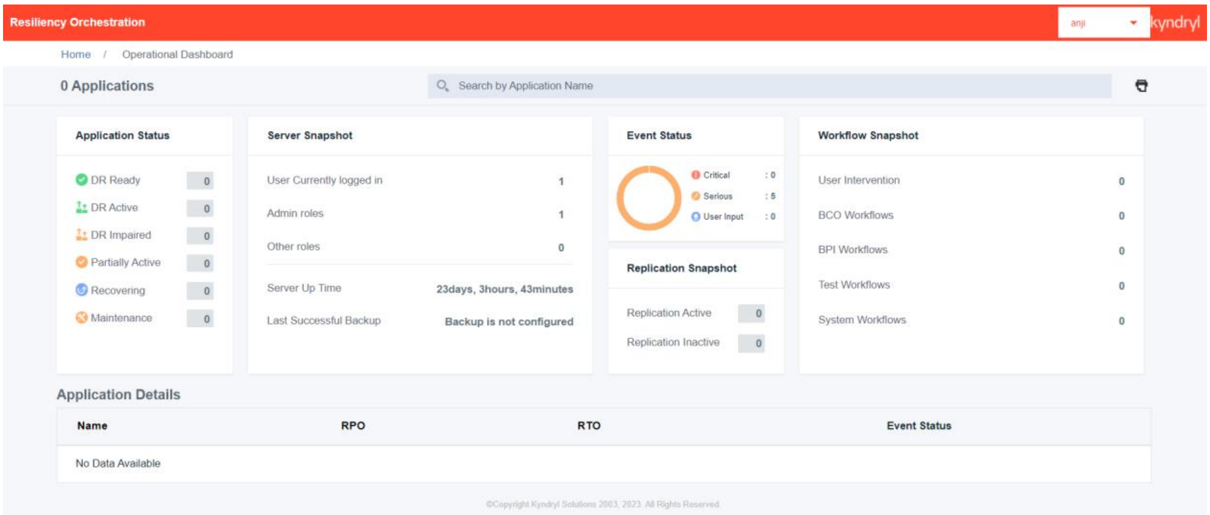
The DR Operational Dashboard can be used by the Kyndryl Resiliency Orchestration Operator to view the summaries and details of the Applications running on the Kyndryl

Resiliency Orchestration Servers. The summaries are presented as Widgets. Details about the selected application can also be viewed under the **Application Details**.

To know your privileges for your assigned role, see *Kyndryl Resiliency Orchestration Server User Role Management.*

To view the Operational Dashboard, click the **DR Operational Dashboard** button on the Kyndryl Resiliency Orchestration Home page.

To view the Kyndryl Resiliency Orchestration Home page, click the **Home** icon.



Application Status

DR Ready	0
DR Active	0
DR Impaired	0
Partially Active	0
Recovering	0
Maintenance	0

Server Snapshot

User Currently logged in	1
Admin roles	1
Other roles	0
Server Up Time	23days, 3hours, 43minutes
Last Successful Backup	Backup is not configured

Event Status

Critical	: 0
Serious	: 5
User Input	: 0

Replication Snapshot

Replication Active	0
Replication Inactive	0

Workflow Snapshot

User Intervention	0
BCO Workflows	0
BPI Workflows	0
Test Workflows	0
System Workflows	0

Application Details

Name	RPO	RTO	Event Status
No Data Available			

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

You can do the following tasks in the DR Operational Dashboard page:

- View the **summaries** of the Applications managed by the different Kyndryl Resiliency Orchestration Servers presented in the Widgets
- View **details** of the Applications
- **Print a snapshot** of the Dashboard

Application Summary

The Application Summary displays the following Widgets:

- **Application Status**

  This Widget displays the status of the Applications. The icons for each of the state along with the number of Applications, which are in that state are displayed. You can click on the number displayed for each state to find the details of that Application, which gets displayed under the **Application Details**.

  The Applications have the following states:

  - **DR Ready**

The Application Group (AG) is in the DR Ready state if all the RGs within the AG are in the DR Ready state. In the DR Ready state, the DR dataset and PR dataset are in a known replication state and the replication status is one of the following:

- Replication is not occurring between them
- Normal mode of data replication and restoration is occurring
- Normal mode of data replication and restoration failed for some reason

- **DR Active**

  The Application Group (AG) is in the DR Active state if all the RGs within the AG are in the DR Active state. In the DR Active state, the control of business is switched to the DR site when the PR dataset is down on the PR site and replication does not occur in the PR site.

- **DR Impaired**

  The Application Group (AG) is in the DR Impaired state if any of the RGs within the AG is in the DR Impaired state. The DR Impaired state is the initial state of the Group. In the DR Impaired state, the DR dataset is not in a known replication state and the DR Dataset has to be synchronized with the PR dataset for any DR activity to happen. The DR may also be impaired due to issues during the transit to Failover BCM.

- **Partially Active**

  The Application Group (AG) is in the Partially Active state if some of the RGs within the AG are in the DR Active state and the others in the same AG are in the DR Ready state.

- **Recovering**

  The Application Group (AG) is in the Recovering state if some of the RGs within the AG are in either of the following states: Failover transit, Switch over transit, Switchback transit, or Failback transit, and the other RGs within the same AG are in the DR Ready or DR Active state.

- **Server Snapshot**

  This Widget displays the following information about the users who have logged in to the Kyndryl Resiliency Orchestration application across different sites and the Kyndryl Resiliency Orchestration server.

  - Total number of users who have logged in
  - Number of users who have logged in with Administrator privileges (including users with Super Administrator and Administrator roles)
  - Number of users who have logged in with privileges other than that of an Administrator

- The Server uptime indicates the time in days, hours and minutes, that the Kyndryl Resiliency Orchestration Server has been running from the time of its installation
- The last successful backup status of the Kyndryl Resiliency Orchestration Server with the day and time of the backup

- **Event Status**

  This Widget displays the status of the cumulative events of all Applications and their associated RGs. Events are classified and the status displayed in the following types:

- Critical

  Events that require immediate attention by the Kyndryl Resiliency Orchestration Admin and must be fixed on priority

- Serious

  Events that require to be attended to immediately

- User Input

  Events that are awaiting inputs from the Kyndryl Resiliency Orchestration Users

- **Replication Snapshot**

  This Widget displays the status of the Applications based on their replication status. The applications are classified in the following types:

- Replication Active

  Lists the number of applications that have an active replication in progress

- Replication Inactive

  Lists the number of applications that do not have an active replication in progress

- **Workflow Snapshot**

  This Widget displays the number of Applications that have different workflows being executed. The following workflow types are displayed:

  - User Intervention

    Applications that require inputs from the Kyndryl Resiliency Orchestration Users to complete the workflow execution

  - BCO Workflows

    Applications that are executing the BCO workflows

- BPI Workflows

  Applications that are executing the BPI workflows

- Test Workflows

  Applications that are executing the Test workflows

- System Workflows

  Applications that are executing the System workflows

Application Details

You can find the details of the Applications displayed in the following scenarios:

- The default display is of the Applications based on the priorities you set for an Application during its creation. The applications are arranged in the descending order of their priority. Applications with the same priority are displayed in an alphabetically increasing order.
- Applications you searched for in the Search Field
- Applications you clicked in any of the Widgets

The following details about the Application are displayed:

- **Name**

  Displays the names of the Applications selected or searched for.

- **RPO**

  Displays the configured RPO for the Application along with the observed deviation in the RPO as a percent (%).

- **RTO**

  Displays the configured RTO for the Application along with the observed deviation in the RTO as a percent (%).

- **Event Status**

  Displays the event types for the Application as a bar labelled with the number of events under each type.

- **Management Server**

  Displays the IP address of the Kyndryl Resiliency Orchestration Server that is managing the Application.

Dashboard Snapshot

You can print a snapshot of the displayed DR Operational Dashboard page.

To print the displayed page using your browser configured printer controls, click the **Print** icon, and follow the instructions displayed to print.

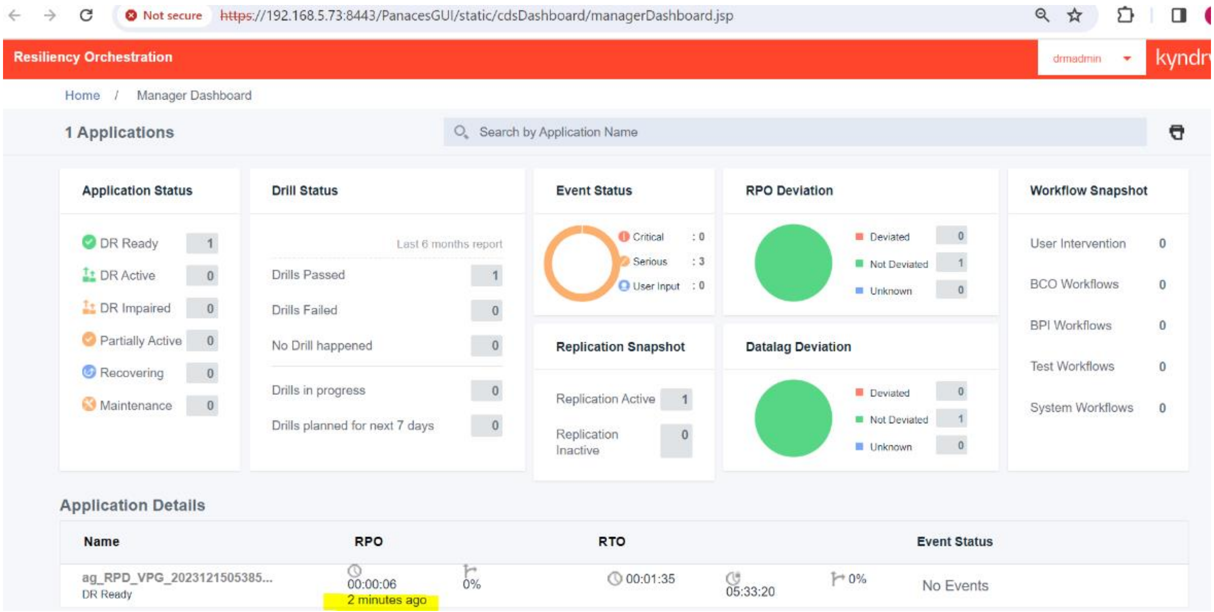
DR Manager Dashboard

The DR Manager Dashboard can be used by the Kyndryl Resiliency Orchestration user to view the summaries and details of the Applications running on the Kyndryl Resiliency Orchestration Servers. The summaries are presented as Widgets. Details about the selected application can also be viewed under the **Application Details**.

To know your privileges for your assigned role, see *Kyndryl Resiliency Orchestration Server User Role Management.*

To view the Manager Dashboard, click the **DR Manager Dashboard** button on the Kyndryl Resiliency Orchestration Home page.

To view the Kyndryl Resiliency Orchestration Home page, click the **Home** icon.



Not secure https://192.168.5.73:8443/PanacesGUI/static/cdsDashboard/managerDashboard.jsp

Resiliency Orchestration drmadmin kyndr

Home / Manager Dashboard

1 Applications

Search by Application Name

Application Status

DR Ready	1
DR Active	0
DR Impaired	0
Partially Active	0
Recovering	0
Maintenance	0

Drill Status

Last 6 months report

Drills Passed	1
Drills Failed	0
No Drill happened	0
Drills in progress	0
Drills planned for next 7 days	0

Event Status

Critical	: 0
Serious	: 3
User Input	: 0

RPO Deviation

Deviated	0
Not Deviated	1
Unknown	0

Workflow Snapshot

User Intervention	0
BCO Workflows	0
BPI Workflows	0
Test Workflows	0
System Workflows	0

Replication Snapshot

Replication Active	1
Replication Inactive	0

Datalag Deviation

Deviated	0
Not Deviated	1
Unknown	0

Application Details

Name	RPO		RTO			Event Status
ag_RPD_VPG_2023121505385... DR Ready	00:00:06 2 minutes ago	0%	00:01:35	05:33:20	0%	No Events

The following sections can be seen in the DR Manager Dashboard page:

- **Application Summary**
- **Application Details**

Application Summary

The Application Summary displays the following Widgets:

- **Application Status**

  This Widget displays the status of the Applications. The icons for each of the state along with the number of Applications, which are in that state are displayed. You can click on the number displayed for each state to find the details of that Application, which gets displayed under the **Application Details**. The Applications have the following states:

- **DR Ready**

  The Application Group (AG) is in the DR Ready state if all the RGs within the AG are in the DR Ready state. In the DR Ready state, the DR dataset and PR dataset are in a known replication state and the replication status is one of the following:

  - Replication is not occurring between them
  - Normal mode of data replication and restoration is occurring
  - Normal mode of data replication and restoration failed for some reason

- **DR Active**

  The Application Group (AG) is in the DR Active state if all the RGs within the AG are in the DR Active state. In the DR Active state, the control of business is switched to the DR site when the PR dataset is down on the PR site and replication does not occur in the PR site.

- **DR Impaired**

  The Application Group (AG) is in the DR Impaired state if any of the RGs within the AG is in the DR Impaired state. The DR Impaired state is the initial state of the Group. In the DR Impaired state, the DR dataset is not in a known replication state and the DR Dataset has to be synchronized with the PR dataset for any DR activity to happen. The DR may also be impaired due to issues during the transit to Failover BCM.

- **Partially Active**

  The Application Group (AG) is in the Partially Active state if some of the RGs within the AG are in the DR Active state and the others in the same AG are in the DR Ready state.

- **Recovering**

  The Application Group (AG) is in the Recovering state if some of the RGs within the AG are in either of the following states: Failover transit, Switch over transit, Switchback transit, or Failback transit, and the other RGs within the same AG are in the DR Ready or DR Active state.

- **Drill Status**

  This Widget displays the status of the Drills conducted by the Kyndryl Resiliency Orchestration for all Applications. Drills are the Switch Over and Switch Back operations executed for an Application.

  The count of Drills for the Applications that are under execution and those that are planned are also shown. The **Drill Status** Widget displays the following information about the Applications:

  - **Drills Passed**

The number of Applications that have passed the Drill.

- **Drills Failed**

  The number of Applications that have passed the Drill.

- **No Drill happened**

  The number of Applications that did not have any Drill executed in the last six months.

- **Drills in progress**

  The number of Applications that have Drills being executed.

- **Drills planned for next 7 days**

  The number of Applications that have Drills scheduled for executed in the next seven days.

- **Event Status**

  This Widget displays the status of the cumulative events of all Applications and their associated RGs. Events are classified and the status displayed in the following types:

- **Critical**

  Events that require immediate attention by the Kyndryl Resiliency Orchestration Admin and must be fixed on priority

- **Serious**

  Events that require to be attended to immediately

- **User Input**

  Events that are awaiting inputs from the Kyndryl Resiliency Orchestration Users

- **Replication Snapshot**

  This Widget displays the status of the Applications based on their replication status. The applications are classified in the following types:

- **Replication Active**

  Lists the number of applications that have an active replication in progress

- **Replication Inactive**

  Lists the number of applications that do not have an active replication in progress

- **RPO Deviation**

This Widget graphically displays the deviations in the RPOs set for the Applications. The RPO is set for the RGs associated with an Application and is considered as the RPO for that Application.

- Deviated

  Indicates the number of Applications that have the RPO of any associated RG that has deviated from the set RPO

- Not Deviated

  Indicates the number of Applications that have the RPO of their associated RGs with no deviation from the set RPO

- Unknown

  Indicates the number of Applications that do not have a known RPO measured at that instance.

- Time stamp for the RPO is added to the RPO (from RO 8.4.6.0 version.)

- **Datalag Deviation**

  This Widget graphically displays the deviations in the Data lag for the Applications. The Data lag is measured for the RGs associated with an Application and is considered as the Data lag for that Application.

  - **Deviated**

    Indicates the number of Applications that have the Data lag of any associated RG that has deviated from the set Data lag

  - **Not Deviated**

    Indicates the number of Applications that have the Data lag of their associated RGs with no deviation from the set Data lag

  - **Unknown**

    Indicates the number of Applications that do not have a known Data lag measured at that instance.

- **Workflow Snapshot**

  This Widget displays the number of Applications that have different workflows being executed. The following workflow types are displayed:

  - **User Intervention**

    Applications that require inputs from the Kyndryl Resiliency Orchestration Users to complete the workflow execution

  - **BCO Workflows**

    Applications that are executing the BCO workflows

  - **BPI Workflows**

    Applications that are executing the BPI workflows

- **Test Workflows**

  Applications that are executing the Test workflows

- **System Workflows**

  Applications that are executing the System workflows

Application Details

You can find the details of the Application you searched for in the Search Field displayed in columns. Details of the Application you clicked in any of the Widgets are also displayed under **Application Details**.

The following details about the Application are displayed:

- **Name**

  Displays the names of the Applications selected or searched for.

- **RPO**

  Displays the configured RPO for the Application along with the observed deviation in the RPO as a percent (%).

- **RTO**

  Displays the configured RTO for the Application along with the observed deviation in the RTO as a percent (%).

- **Event Status**

  Displays the event types for the Application as a bar labelled with the number of events under each type.

- **Management Server**

  Displays the IP address of the Kyndryl Resiliency Orchestration Server that is managing the Application.

Manage

The **Manage** page has four tabs namely:

1. Sites
2. Application Groups
3. Recovery Groups
4. Executing Workflows.

On clicking the Manage tab, the RG Listing page is displayed.

Filters

Filters help the user to set priority as per the requirements. While we can view four types of filters for an AG we can view eight types of filters for the RG. Below are the different types of filters.

Field	Description
Type I	Select this to give the RG priority I
Type II	Select this to give the RG priority II
Type III	Select this to give the RG priority III
Type IV	Select this to give the RG priority IV
DR Ready	The RG is in this continuity state if: ▪ DR sync is in progress - NC workflow is running ▪ DR sync is in progress - SLA is deviated by 12:23:45 - NC workflow is running but RPO deviation is more than 100%
DR Active	The RG is in this continuity state if: ▪ DR Resync is in Progress - RNC workflow is running ▪ DR Active - Failover of the group is successful
DR Impaired	The RG is in this continuity state if: ▪ Switchover In Progress ▪ Switchback In Progress ▪ Failover In Progress ▪ Fallback In Progress
In Transit	The RG is in this continuity state if: ▪ DR Init not started - After the group is moved to managed mode and NFC is not started ▪ DR Init is in progress - NFC workflow is running ▪ DR Init is Aborted - NFC is aborted or crashed

Field	Description
	▪ DR Sync is Aborted - NC is aborted or crashed ▪ DR Sync is Paused - Awaiting User Input for Action Create File set - SLA is deviated by 12:23:45 - NC is running but awaiting ▪ DR Sync not started - NFC is successful and the group is moved to normal inactive ▪ DR Resync is not started - After SO is successful and RNC workflow is not started ▪ DR Resync is Aborted - RNC is aborted or crashed

Note: The filter attributes are dynamic to what is configured in group labels (**Admin** > Go to **Group Labels Info**).

Group Health

Displays the Group Health for each RG with the following colors:

🟥 1 Group status is changed to Red if there are any critical events raised.

🟧 1 Group Status is changed to Amber if any warning and serious events are raised.

🟩 1 Group status is Green when there are no critical, serious, or warning events open and only info events are present.

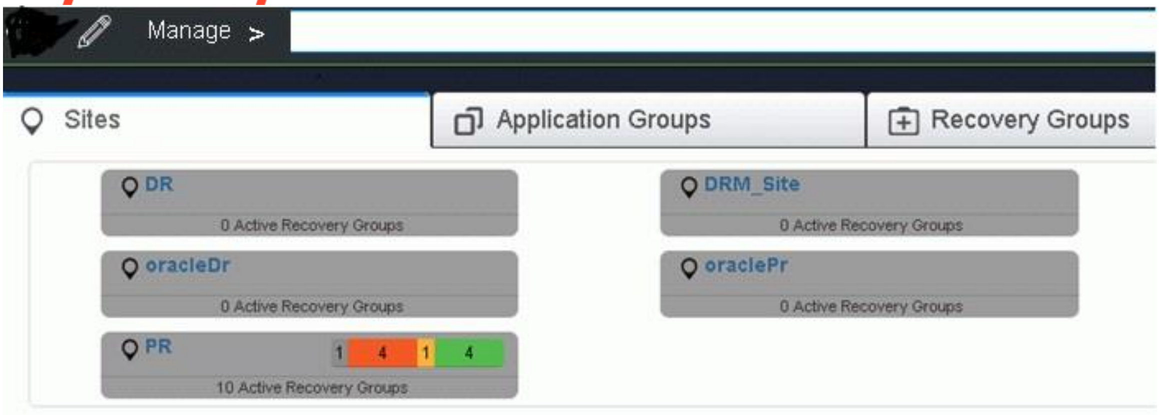
⬜ 1 Group Status is changed to Grey when no monitoring information is available.

The number displayed in each color indicates the RGs in that group's health state. The group health graph changes based on the events that are raised for the group.

Sites

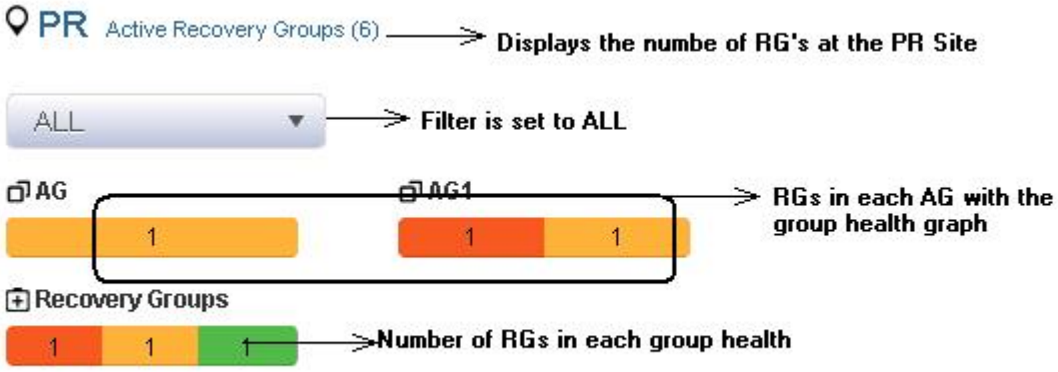
To view all the Sites, click **Manage** > **Sites.**

The Sites page displays the Site listing, PR Sites, DR sites, and the Kyndryl Resiliency Orchestration site information.



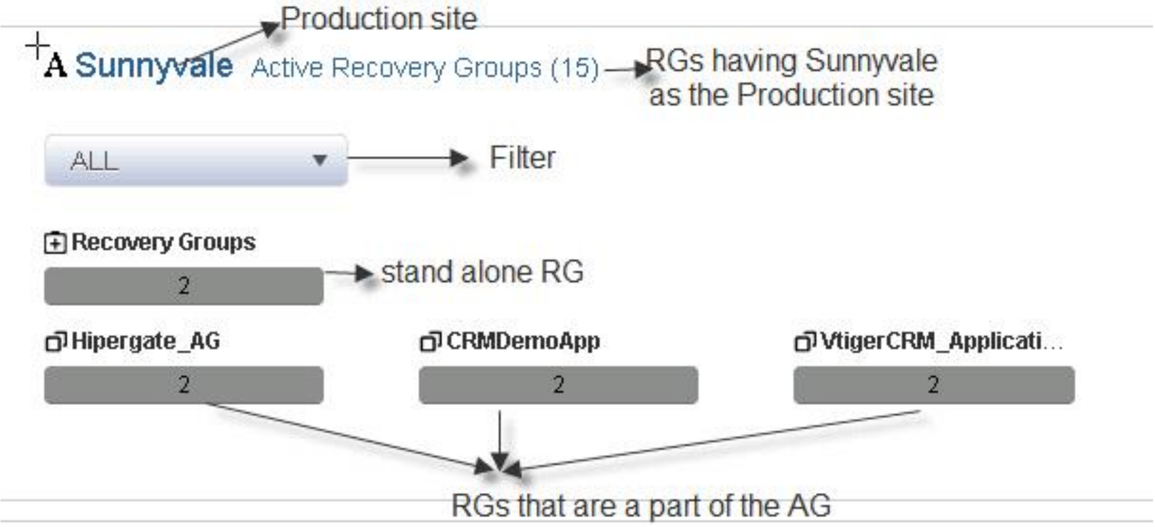
The Site Listing page gives a numerical explanation of the recovery groups in each of the PR sites, DR sites, and Resiliency Orchestration sites.

In the PR Site table, as shown in the below figure, the total number of active recovery groups is displayed in the brackets. The group label by default is set to ALL. All the application groups are displayed with the number of RGs that are a part of AG. The different colors represent the group health of the RG. The Recovery groups represent the total number of RGs which are in different health states.


PR Active Recovery Groups (6)
Displays the numbe of RG's at the PR Site
ALL
Filter is set to ALL
AG
1
AG1
1
1
RGs in each AG with the group health graph
Recovery Groups
1
1
1
Number of RGs in each group health

The **Site Listing** page is displayed. Each site displays the number of active recovery groups available at the production site.

The details of each production site are explained below.



The table displays information about the stand-alone recovery groups and recovery groups that are part of the application group.

The site information page displays the following details:

- The total number of recovery groups is displayed beside each production site.
- On selection of the required filter, the recovery groups of that filter are displayed.
- When the filter is set to **All,** all the recovery groups and application groups are displayed.

Field	Description
Type	Displays the four types of filters, by default; Type 1 Type II Type III Type IV Note: The filter attributes are dynamic to what is configured in group labels (**Admin > Group Labels Info**)
Group Name	Displays the name of the AGs. While displaying AGs, the AG and the corresponding RGs are displayed in a tree structure. The Group Health of each RG is displayed with the following colors: 🟥 1 Group status is changed to Red if there are any critical events raised. 🟧 1 Group Status is changed to Amber if any warning and serious events are raised. 🟩 1 Group status is Green when there are no critical, serious, or warning events open and only info events are present. ▨ 1 Group Status is changed to Grey when no monitoring information is available.

Field	Description
	The number displayed in each color displays the RGs in that group's health state. Note: You can view the Dashboard of the AG or RG by clicking the respective Group link.
RTO	Displays Configured RTO, Current RTO with a percentage of Deviation from the configured RTO, and the Recovery Time.
Events	Displays the events when there are undesired changes in the groups that take place. Events can either be critical or serious Events can be viewed in the Sequence of events

- The first column represents the number of standalone recovery groups at the production site.
- The second column represents the number of recovery groups in each application group at the production site.

Note: Even if one RG of an AG is a part of the production site, it will list and give a count of all RGs that are associated with the AGs.

Application Groups

An ⧉ Application Groups (AG) contains RGs. A RG cannot be part of more than one AG at a time. AGs can be considered as containers of RGs.

You can view the Application Group by clicking on the **Manage** tab on the Kyndryl Resiliency Orchestration GUI. As soon as the Groups are configured, you can view the application groups by navigating through the following path.

Click **Manage** > ⧉ **Application Groups** to view all the Application groups.

The Application Groups page displays the following information:

On clicking the link of the AG, the **AG Listing** page is displayed.

The AG listing page displays the RTO and the Events information Relationship and continuity Workflows.

By default, the AG page displays ten AGs. Click **View All** to view all the AGs on the AG listing page.

The first navigation bar displays the first level of the path, while the second navigation bar displays the navigation path in more detail.

Each AG displays the number of RG in the AG along with the group health graph.

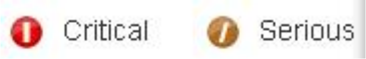
On clicking the AG, the user is directed to the **AG listing** page.

Click on **RTO** to view the RTO status. The RTO summary status is displayed in the RTO tab.

Click on **RPO** to view the RPO status. The RPO summary status is displayed in the RPO tab.

Click on **Events** to view the Sequence of Events that has occurred. The graph displays the time and the date of the event occurrence.

If it is a critical event, it is represented in red, and the serious event is represented in amber color respectively as shown below.



The Relationship section has the following two links:

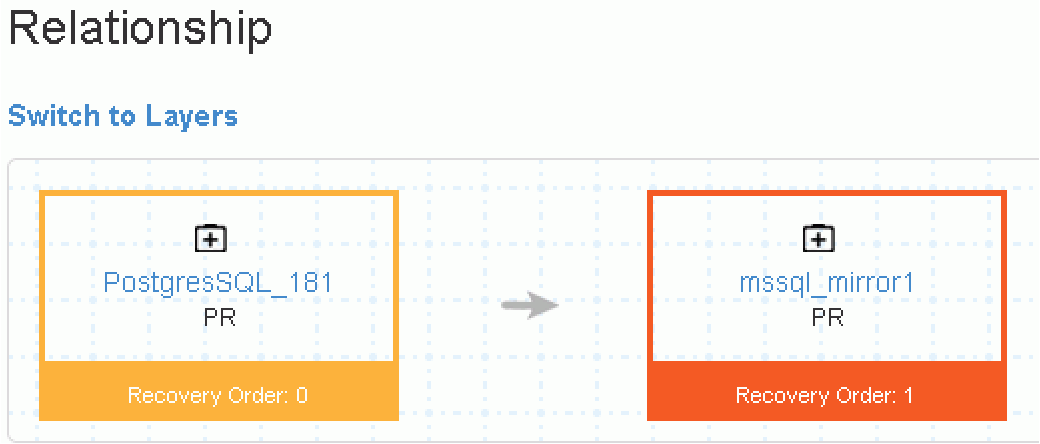
- Switch to Layers/Switch to Recovery Order
- Details

Note: The Details link appears only for Application Recovery for AWS solutions.

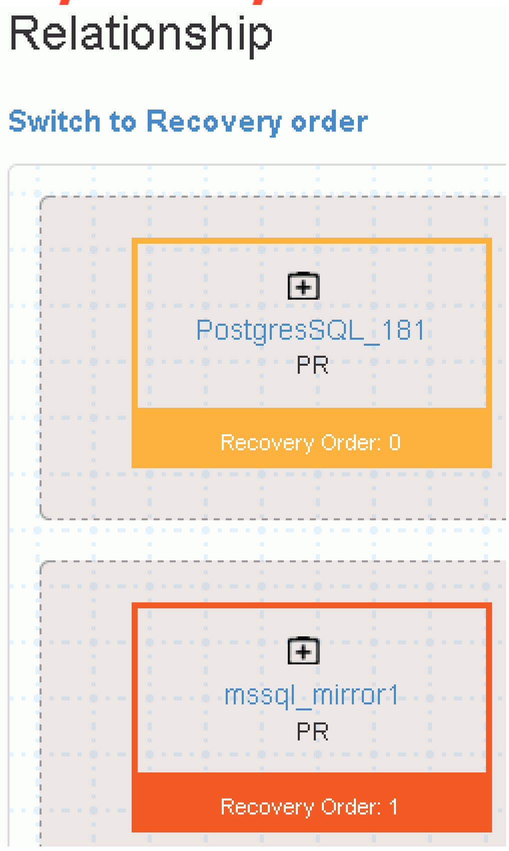
Switch to Layers and Switch to Recovery Order are the two links to view the relationship of the RGs.

On setting the relationship status to Switch to layers, the RGs are displayed one

after the other.



In setting the relationship to switch the recovery group, the RGs are one below the other as shown below:



Relationship

Switch to Recovery order

Note

- Each box represents a recovery group
- The colors of the RGs represent the group's health
- The icon ⊞ represents the recovery group and the name of the recovery group is displayed. On clicking the Recovery group name, the user is directed to the Relationship table on the RG listing page of that RG.
- The Site location is displayed. Here the site location is PR.
- Recovery Order is the position of the recovery groups and the numbering starts from 0.

The Details link provides detailed information on the application stack by displaying the configuration for primary, on-premise VMs and the AWS configuration for remote on-cloud devices and grouping the Application stack by tier.

The next table displays the Continuity workflow information:

Field	Description
Workflow Name	Displays the name of the workflow
Version status	Displays information on the version status
Execution status	Displays if the current state of execution
Dry Run Status	Displays if Dry Run has been executed or not

Click on the 👁 **View** button to view the Workflow.

Click on the ✏ edit the Workflow.

AG Listing

The AG listing page displays the RTO and the Events information Relationship and continuity Workflows.

By default, the AG page displays ten AGs. Click **View All** to view all the AGs on the AG listing page.

The search bar is automatically backfilled with the search criteria based on the page context. The breadcrumbs help navigate to the desired page.

Each AG displays the number of RGs in the AG along with the group health graph.

On clicking the AG, the user is directed to the **AG Details** page.

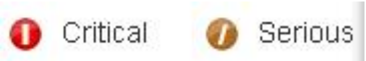
AG Details

Click **Manage > Application Groups** to get the AG Details.

Click **RTO** to view the RTO status. The RTO summary status is displayed in the RTO tab.

Click on **Events** to view the Sequence of Events that has occurred. The graph displays the time and the date of the event occurrence.

If it is a critical event, it is represented in red, and the serious event is represented in amber color respectively as shown below.



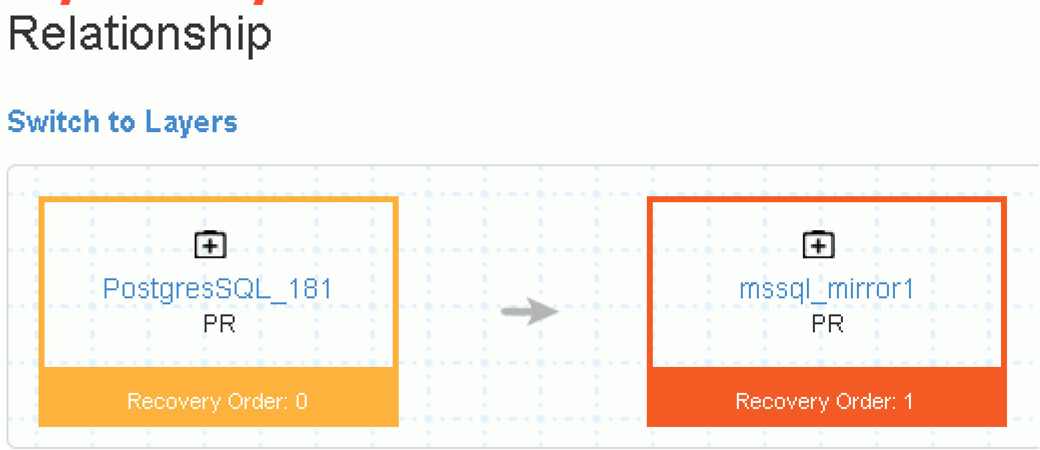
To view the relationship of RGs within the AG, click **Relationship**.

The next table displays the **Continuity Workflows**.

Relationship

The **Relationship** between the RGs within the AG is displayed. There are two ways of representing this; **Layers** and **Recovery Order.**

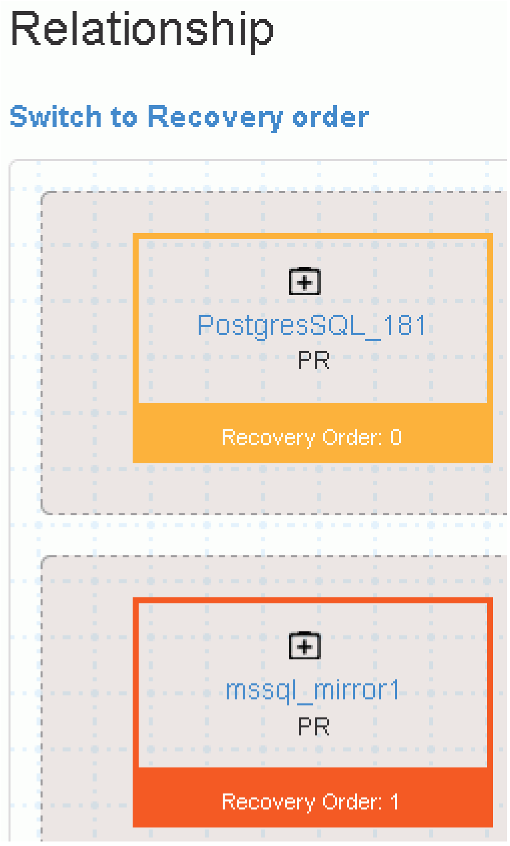
The layers will represent the relationship in the form of layers and the recovery order will represent the relationship in the order in which they will be recovered. Layers showcase the serial order and recovery order represents the parallel execution of the RGs.



Relationship

Switch to Layers

In setting the relationship to switch to the recovery group the RGs are one below the other as shown in the following figure.



Relationship

Switch to Recovery order

- Each box represents a recovery group.
- The colors of the RGs represent the group's health.
- The icon ⊞ represents the recovery group and the name of the recovery group is displayed.

- The Site location is displayed. Here the site location is PR.

Recovery Groups

Recovery Groups

Click **Manage** > ⊞ **Recovery Groups** to view the Recovery Groups. The Group Health meter on the RG page displays the number of recovery groups under each state. The RGs can be classified under these four colours which display the health of the group.

The group health graph displays the recovery groups in each group's health state. On hovering over the graph, the percentage of each group's health is displayed.

The filter by default is set as Type 1. The RG listing page displays ten recovery groups, on clicking **View All,** all the recovery groups are displayed. For each recovery group, the following information is displayed.

Field	**Description**
Recovery Groups	Displays names of the RGs
RPO	Displays the configured RPO (in minutes) of the Group **Note:** If the configured RPO and the current RPO for the Group have crossed the threshold value you can view the deviation in red (or orange). If the deviation is within the threshold value, the deviation is represented in green.
RTO	Displays the RTO status (in minutes) for the Group. The current RTO and the configured RTO are displayed. If there is any deviation, the percentage is displayed
Pending Data	Display the data lag and display when the last replication has occurred
Validation	Displays information if the validation has been executed
Config Exposures	Displays the critical and non-critical list

There are eight types of filters for an RG. See **Filters**.

On clicking the Recovery Group, the **RG Listing** page is displayed.

RG Listing

Click **Manage** > **Recovery Groups.** The group health of each recovery group is displayed beside the recovery group.

The **RG Listing** page is displayed. The RG Listing page displays the following details of each recovery group.

Note: For VM protection solutions, the RTO tab is not displayed. However, the RG Group listing page displays RTO as Workflow not published.

Field	Description
Recovery Groups	Displays names of the RG
RPO	Displays the configured RPO (in minutes) of the Group. **Note** If the configured RPO and the current RPO for the Group have crossed the threshold value you can view the deviation in red (or orange). If the deviation is within the threshold value, the deviation is represented in green.
RTO	Displays the RTO status (in minutes) for the Group. The current RTO and the configured RTO are displayed. If there is any deviation, the percentage is displayed. For more information see Viewing RTO Details
Pending Data	Display the data lag and display when the last replication has occurred
Validation	Displays information if the validation has been executed.
Config Exposures	Displays the critical and non-critical list

Click on the recovery groups to view the **RG Details** page.

RG Details

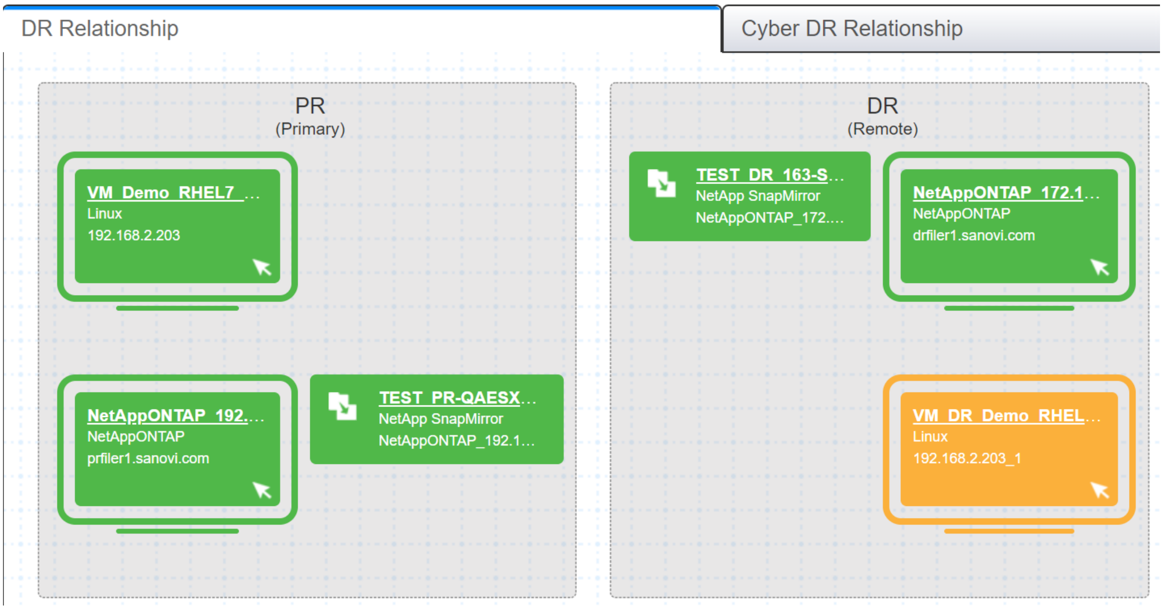
To view the details of each RG, navigate to **Manage** > **Recovery Groups,** and click on the **RG name**.

Field	Description
RTO	Displays the RTO status (in minutes) for the Group. The current RTO and the

Field	Description
	configured RTO are displayed. If there is any deviation, the percentage is displayed.
RPO	Displays the configured RPO (in minutes) of the Group. **Note** If the configured RPO and the current RPO for the Group have crossed the threshold value you can view the deviation in red (or orange). If the deviation is within the threshold value, the deviation is represented in green.
Service Details	Displays when the last replication occurred
Events	Displays the events. For more information click Sequence of Events
Validation	Displays information if the validation has been executed.
Config Exposures	Displays the critical and non-critical list

Relationship in RG

The **Relationship** image displays the relationship between the RGs within the AG in the PR and the DR site.



represents the component. Clicking on the component link will display a confirmation navigation message. Clicking Yes will take you to the respective component and allow you to view or edit the component details.

represents the database. Clicking on the database link will display a confirmation navigation message. Clicking Yes will take you to the respective database and allow you to view or edit the database details.

represents the replicator. Clicking on the replicator link will display a confirmation navigation message. Clicking Yes will take you to the respective replicator and allow you to view or edit the replicator details.

Click **View all workflows** to view the BCO and BP workflows.

The BCO and BP workflows have the following:

- NormalFullCopy
- NormalCopy
- Failover
- Fallback
- FallbackResync
- ReverseNormalcopy

The Version Status, Execution Status, and DryRun Status of each workflow are displayed.

Click on the DryRun icon to Execute Dryrun.

Click **DryRun** to execute the DryRun.

or

Click **Cancel** to cancel the DryRun execution.

Continuity Workflows

To view the business process workflows:

1. Click Manage > AG/RG > Application Group/Recovery Group Name.
2. The **AG Details**/**RG Details** page is displayed.
3. Click **View All Workflows** if it is an RG.
    1. Click the **BCO Workflows** tab and all BCO workflows are displayed for the RG.
    2. Click the **BP Workflows** tab, and all BP workflows are displayed for the RG.

The following details are displayed:

Field	Description

Workflow Name	Displays the name of the workflow. Displays the group name for which you want to add the business process.
Version status	Displays the group name for which you want to add the business process.
Execution status	Displays information if the execution was successful, crashed aborted, or is awaiting input.
Dry Run Status	Displays information if the workflow was a success, crashed, not executed, or failed

- Click ▶ Execute to execute the workflow.
- Click 📈 to DryRun the workflow.
- Click 📅 to schedule the workflow execution.
- Click 👁 to preview the workflow.
- Click ✎ to edit the workflow.
- Click 🗑 to delete the workflow.
- Click **Create New** to create a new workflow.

Note

- If the group is in switchover or switchback, then the current DR state of the group does not permit any continuity operations.
- To change the state of the group, go to **Discover** > **Groups** page.

To view the execution history and the version history, click on the workflow name.

The **Execution History** displays the following information:

Field	**Description**
Date	Displays the date of execution
Time Taken	Displays the time taken in seconds for execution
status	Workflow execution status
Version	Displays the version number

The **Version History** displays the following information:

Field	Description
Version	Displays the version number
Created On	Displays the workflow created time
Created By	Displays the username

Limitation – The execution history lists the latest 100 records. Use the following key in the panaces.properties file to increase the limit of the count.

```
panaces.action.execution.history.in.limitCount=100
```

Executing Workflows

Executing Workflow

You can view the details of the workflow that is currently executing along with the details of each action of the workflow.

To view the Workflow, do the following:

1. Click the **Manage >** **Executing Workflows** tab on the navigation bar to view the **RG listing** page.
2. For the desired Group, select the **Workflow link** from the **Workflow** details column. The **Workflow Execution** page appears.
3. Select the RG/AG from the drop-down list filter. If the selected group is RG, then the eight types of **filters** are displayed and if it is an AG, then only four types of filters are displayed namely:

- Type I
- Type II
- Type III
- Type IV

If the selected group is an RG, only then the workflow drop-down list is displayed. Select from the drop-down list.

- BCO
- BP
- Policy
- System Workflow
- All

The following details are displayed:

Field	Description

Group Name	Displays the name of the workflow.
Workflow name and Version	Displays the Workflow name and its present version.
Start Time	Displays the start time of the Workflow.
Time Elapsed	Displays the time elapsed from the process of initiation to completion of the Workflow.
Status and results of RALS	Displays the status of the Workflow and the count reflects the number of completed actions versus total actions.

On clicking the Group name, the user is directed to the RG details page or the AG details page of that group.

On clicking the **Workflow**, the Execution History and Version History are displayed.

Click the executing link, the workflow page is displayed.

Note:

- Click **Key Value Pairs** to view the Key values configured for this Workflow.
- Click **Abort** to stop workflow execution. The **Reason to Abort** pop-up appears, enter the reason, and click on **Reason to Abort**.
- Click **Export to CSV** to export the workflow details to CSV file format.
- Click the **Workflow Actions** tab to view the execution details of actions within the workflow.

Field	**Description**
Action	Displays the name of the action.
TIME INITIATED	Displays the exact start time of the action execution.
TIME ELAPSED (SEC)	Displays the time calculated from the process of initiation to completion of the action.
TYPE	Displays the type of action.
STATUS DETAILS	1. Displays the status details of the action execution. **Note:** 2. If the status is in EXECUTING mode, the user can click on the EXECUTING link to view the Continue as Success or Continue as Failure option buttons. Depending on the requirement and by giving a reason, select any one of the options. 3. If the Status is Awaiting Input, depending on the requirement, the user can select any one of the below options: 4. Continue as a Success 5. Continue as Failure 6. Retry 7. Quit

	If the user wants to know the reason for Awaiting Input, click the View action log button. 8. Click on any link corresponding to the desired action to view the following details for the action. 9. DB Logs 10. Tail Logs 11. Sys Logs

4. Click the **Go Back** link to view the **Active Workflow Listing** page.

Note:

- DB Logs: Displays the Oracle and MSSQL DB Logs. Configure the Error log path while dataset discovery of MSSQL only then we will get the DB Log link for MSSQL.
- Tail Logs: Displays the logs from the path configured in Custom Action.
- Sys Logs: Displays the Linux Operating System Logs.

In the **Workflow Actions** tab, the actions are grouped under the respective Action Groups so that you can know the action belongs to which Action Group.

Note:

The time Elapsed in the Workflow and the total time elapsed for all Custom actions in the workflow are not the same. It is dependent on multiple other factors.

Health Monitoring

The health of the group is continuously monitored, and the status is available as a **Group Health Graph** on the Recovery group page. When there is a change in the status of the health of the groups an event arises.

To navigate to the **Group Health Graph**, click **Monitor** or **Manage** on the Navigation bar. Then click ⊞ **Recovery Group.** The Group Health meter on the RG page displays the number of recovery groups under each state.

Viewing Group Relationship

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the relationship details of a Group, perform the following steps:

1. Click **Manage** on the navigation bar. The **RG Listing/ AG Listing** page appears.
2. Click the desired Group from the **Recovery Groups** column. The **Recovery Group listing** page for the respective RG or AG appears.
3. View the **Relationship** diagram.

Group Dependency

The **Group Dependency** tab under the **Application Group** displays a visual representation of all RGs dependent on the AG. Click each RG name against its box to display its **Recovery Group**. You can also view the order in which Failover will be done during disaster recovery by checking the arrow above the **Group Failover order**.

Recovery Group Relationship

You can view the relationship between the configured production and the DR in a pictorial representation by navigating to the **Recovery Group Details.** This page displays the solution-specific replication details, names, and status of the datasets, protection schemes, and components on production and DR servers.

You can expand or collapse the Replication, Component, and Dataset details by clicking **Expand All** and **Collapse All** links at the top right corner of the page.

RPO and RTO Monitoring

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the RPO and RTO details of a Group, perform the following steps:

1. Click **Manage** on the navigation bar. Click **Recovery Groups.**
2. Click the desired Group from the **Recovery Groups** column. The **Recovery Group** page for the respective RG or AG appears.
3. Click the **RTO/ RPO** tab respectively. The tabs are displayed for the Recovery Group. This displays the following information:

Note:

For VM protection solutions, the **RTO tab is not displayed**. However, the RG Group listing page displays RTO as **Workflow not published**.

Field	Description
App RPO Summary	Displays Configured RPO, Current RPO with the percentage of Deviation from the configured RPO, and the Recovery Point. For more information see Viewing App RPO Details.
Data RPO Summary	The data RPO summary table will be displayed if the solution supports Data RPO. Viewing Data RPO Details.
RTO Summary	Displays Configured RTO, Current RTO with a percentage of Deviation from the configured RTO, and the Recovery Time. For more information see Viewing RTO Details
RTO Breakup	Displays the name of the Recovery Step executed during the recovery process along with the Expected Completion Time in seconds.

Note: If the number of RG's more than 5 then follow the below instructions:
Change the value of the property '**org.quartz.threadPool.threadCount**' in the file '**$EAMSROOT/installconfig/panaces.properties**' to the number of RG's.
For example, if you have 18 RG's then the property should have 18 as below
org.quartz.threadPool.threadCount = 18

Pending Data

You can view the detailed Replication List by clicking **Manage** > **Recovery Groups** and all the RGs will be listed.

Select any Group name and click the Pending Data tab.

On the Pending data tab, you can monitor the replication process for each group by viewing the detailed replication status of the group and the protection scheme associated with the Group. Storage-related information about the monitored RG and information about data consistency i.e., whether the DR site is in sync with the Production without respect to data replication are also displayed. For example, for a Group configured under the SRDF Protection Scheme, you can view the IDs of the source and target symmetric units.

The Replication tab displays the Data log and the last updated time the files have been replicated.

Field	Description
Data Lag	Displays the data lag information for the RG
Last Updated	Displays the time when the RG was last updated

Click **Stop Replication** to stop the replication.

Click **Start Replication** to start the replication.

Click **Refresh Details** to refresh the replication page.

The replication details are displayed in the table:

Field	Description
Protection	Displays the replication type
Replication status	Displays the status of the replication, Active Inactive and Unknown
Primary-Remote service	Displays the PR and DR information

Note: This table consists of basic information for all groups. Additional information will be displayed, depending on the Replication Type.

Viewing Recovery Group Replication Details

To view the DR solution-specific replication details of the RG, perform the following steps:

1 Click **Manage > Recovery Groups. The RG Listing Page appears.**

2 Click **Group Name** in the **RG Listing Page.**

3 Click the **Pending Data** tab.

4 The Pending Data tab is displayed that lists the DR Solution-specific replication details. The Replication tab is displayed only for that Recovery Group.

Click **Stop Replication** to stop the replication process.

Click the **Refresh Details** to refresh the information.

Monitor

The Monitor page has four tabs namely:

1. Sites
2. Application Groups
3. Recovery Groups and
4. Executing Workflows.

On clicking the Monitor tab, the sites page is displayed.

Filters

Filters help the user to set priority as per the requirements. While we can view four types of filters for an AG we can view eight types of filters for the RG. Below are the different types of filters.

Field	Description
Type I	Select this to give the RG priority I

Field	Description
Type II	Select this to give the RG priority II
Type III	Select this to give the RG priority III
Type IV	Select this to give the RG priority IV
DR Ready	The RG is in this continuity state if: ▪ DR sync is in progress - NC workflow is running ▪ DR sync is in progress- SLA is deviated by 12:23:45 - NC workflow is running but RPO deviation is more than 100%
DR Active	The RG is in this continuity state if: ▪ DR Resync is in Progress - RNC workflow is running ▪ DR Active - Failover of the group is successful
DR Impaired	The RG is in this continuity state if: ▪ Switchover In Progress ▪ Switchback In Progress ▪ Failover In Progress ▪ Fallback In Progress
In Transit	The RG is in this continuity state if: ▪ DR Init not started - After the group is moved to managed mode and NFC is not started ▪ DR Init is in progress - NFC workflow is running ▪ DR Init is Aborted - NFC is aborted or crashed ▪ DR Sync is Aborted - NC is aborted or crashed ▪ DR Sync is Paused - Awaiting User Input for Action Create File set - SLA is deviated by 12:23:45 - NC is running but awaiting ▪ DR Sync not started - NFC is successful and the group is moved to normal inactive

Field	Description
	▪ DR Resync is not started - After SO is successful and RNC workflow is not started ▪ DR Resync is Aborted - RNC is aborted or crashed

Note: The filter attributes are dynamic to what is configured in group labels (**Admin** > Go to **Group Labels Info**).

Group Health

Displays the Group Health for each RG with the following colors:

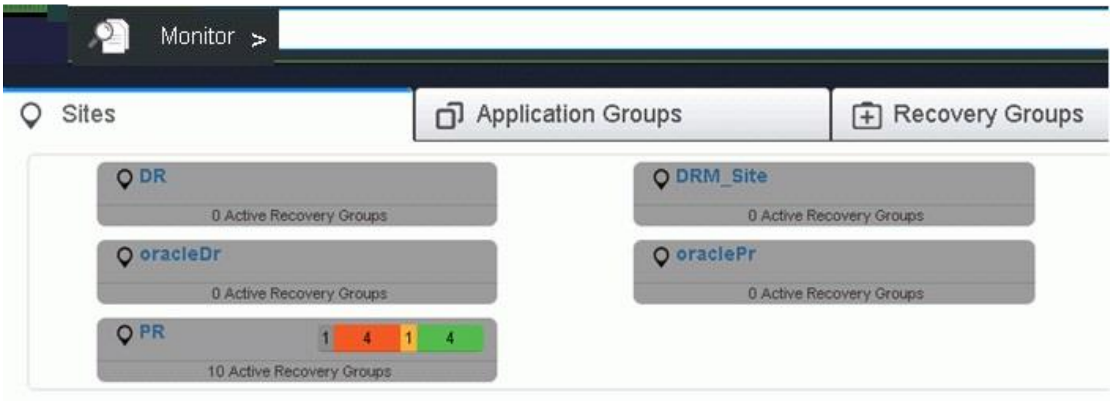
🟥 1 Group status is changed to Red if there are any critical events raised.
🟧 1 Group Status is changed to Amber if any warning and serious events are raised.
🟩 1 Group status is green when there are no critical, serious, and warning events open and only info events are present.
⬜ 1 Group Status is changed to Grey when no monitoring information is available.

The number displayed in each color indicates the RGs in that group's health state. The group health graph changes based on the events that are raised for the group.

Sites

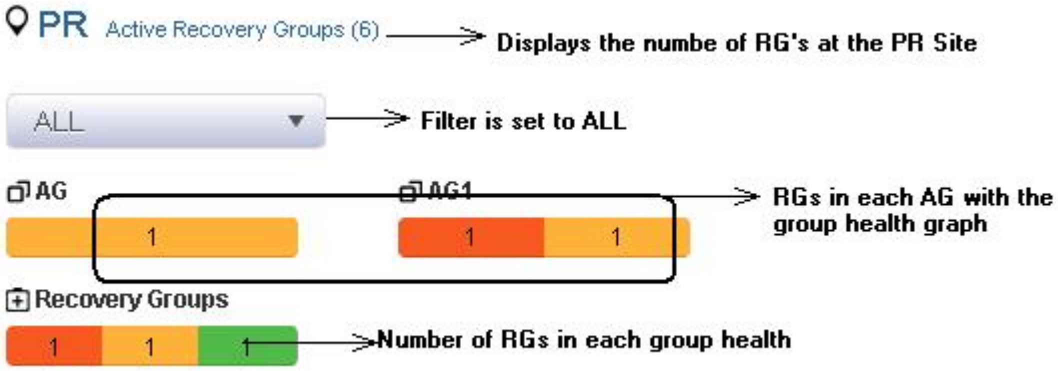
To view all the Sites**,** click **Monitor** > **Sites.**

The Sites page displays the Site listing, PR Sites, DR sites, and the Kyndryl Resiliency Orchestration site information.



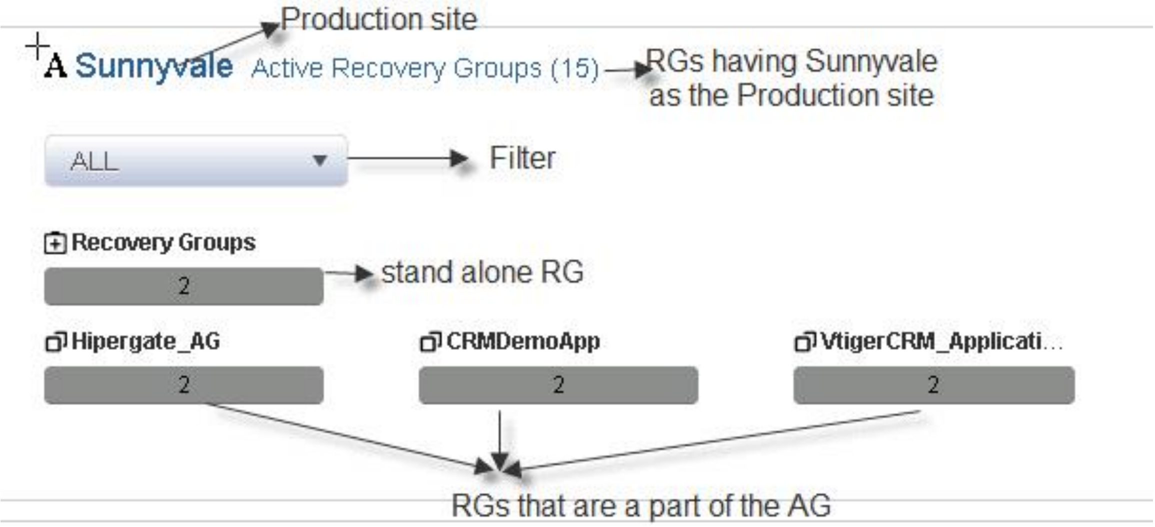
The Site Listing page gives a numerical explanation of the recovery groups in each of the PR Site, DR Site, and Resiliency Orchestration sites.

In the PR Site table, as shown in the below figure, the total number of active recovery groups is displayed in the brackets. The group label by default is set to ALL. All the application groups are displayed with the number of RGs that are a part of the AG. The different colors represent the group health of the RG. The Recovery groups represent the total number of RGs which are in different health states.


PR Active Recovery Groups (6)
Displays the numbe of RG's at the PR Site
ALL
Filter is set to ALL
AG
AG1
1
1
1
RGs in each AG with the group health graph
Recovery Groups
1
1
1
Number of RGs in each group health

The **Site Listing** page is displayed. Each site displays the number of active recovery groups available at the production site.

The details of each production site are explained below.



The table displays information about the stand-alone recovery groups and recovery groups that are a part of the application group.

The site information page displays the following details:

- The total number of recovery groups is displayed beside each production site.
- On selection of the required filter, the recovery groups of that filter are displayed.

- When the filter is set to **All,** all the recovery groups and application groups are displayed.
- The first column represents the number of standalone recovery groups at the production site.
- The second column represents the number of recovery groups in each application group at the production site.

Note: Even if one RG of an AG is a part of the production site, it will list and give a count of all RGs that are associated with the AGs.

Application Groups

Application Groups

The ⧉ Application Groups (AG) contains RGs. An RG cannot be part of more than one AG at a time. AGs can be considered as containers of RGs.

You can view the Application Groups by clicking the **Monitor** tab on the Kyndryl Resiliency Orchestration ™ GUI. As soon as the Groups are configured you can view the application groups by navigating through the following path.

Click **Monitor** > ⧉ **Application Groups** to view all the Application Groups.

The application groups page displays the following information:

Field	**Description**
Group Name	Displays names of the AGs. While displaying AGs, the AG and the corresponding RGs are displayed in a tree structure. The Group Health of each RG is displayed with the following colors: 🟥 1 Group status is changed to Red if there are any critical events raised. 🟧 1 Group Status is changed to Amber if any warning and serious events are raised. 🟩 1 Group status is green when there are no critical, serious, and warning events open and only info events are present. ⬜ 1 Group Status is changed to Grey when no monitoring information is available. The number displayed in each color displays the RGs in that group's health state. **Note:**

Field	Description
	You can view the Dashboard of the AG or RG by clicking the respective Group link.
RPO	Displays Configured RPO, Current RPO with the percentage of Deviation from the configured RPO, and the Recovery Point.
RTO	Displays Configured RTO, Current RTO with the percentage of Deviation from the configured RTO, and the Recovery Time.
Events	Displays the events when there are undesired changes in the groups that take place. Events can either be critical or serious Events can be viewed in the Sequence of events

On clicking the link of the AG, the **AG Listing** page is displayed.

The AG listing page displays the RTO and the Events information Relationship and continuity Workflows.

By default, the AG page displays ten AGs. Click **View All** to view all the AGs on the AG listing page.

The first navigation bar displays the first level of the path, while the second navigation bar displays the navigation path in more detail.

Each AG displays the number of RGs in the AG along with the group health graph.

On clicking the AG, the user is directed to the **AG listing** page.

Click on **RTO** to view the RTO status. The RTO summary status is displayed in the RTO tab.

Click on **RPO** to view the RPO status. The RPO summary status is displayed in the RPO tab.

Click on **Events** to view the Sequence of Events that has occurred. The graph displays the time and the date of the event occurrence.

If it is a critical event, it is represented in red, and the serious event is represented in amber color respectively as shown below.

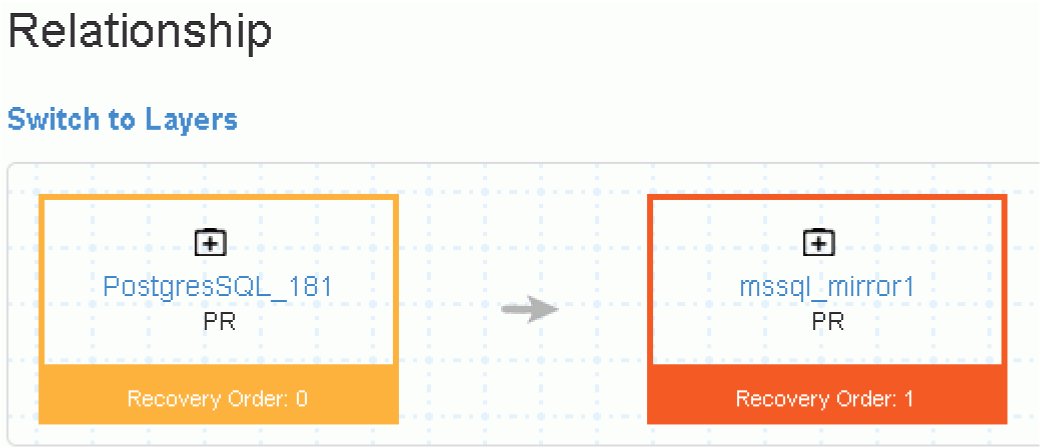
The Relationship section has the following two links:

- Switch to Layers/Switch to Recovery Order
- Details

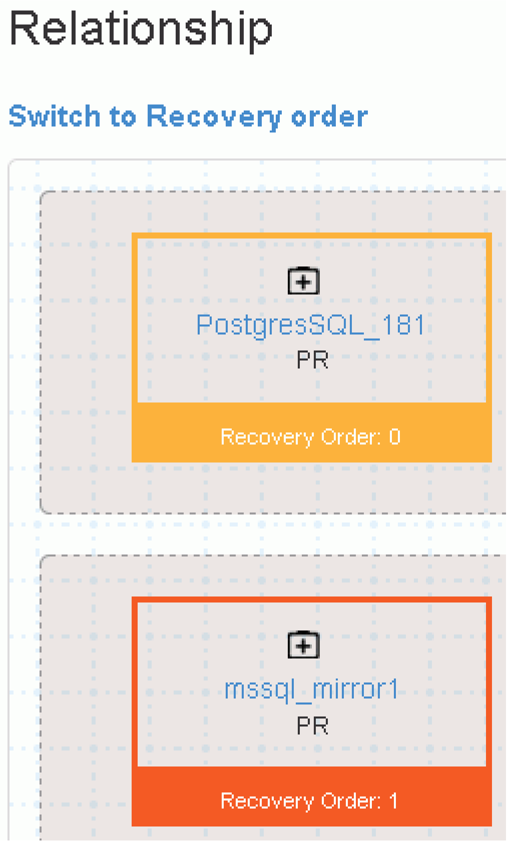
Note: The Details link appears only for Application Recovery for AWS solutions.

Switch to Layers and Switch to Recovery Order are the two links to view the relationship of the RGs.

On setting the relationship status to Switch to layers, the RGs are displayed one beside the other.



In setting the relationship to switch to the recovery group the RGs are one below the other as shown below



Note

- Each box represents a recovery group.
- The colors of the RGs represent the group's health.
- The icon ⊞ represents the recovery group and the name of the recovery group is displayed. On clicking the Recovery group name, the user is directed to the Relationship table on the RG listing page of that RG.
- The Site location is displayed. Here the site location is PR.
- Recovery Order is the position of the recovery groups, and the numbering starts from 0.

The Details link provides detailed information about the Application stack by displaying the configuration for primary, on-premise VMs and the AWS configuration for remote on-cloud devices and grouping the Application stack by Tiers.

The next table displays the Continuity workflows.

The **Continuity Workflows** information is also displayed.

Field	**Description**
Workflow Name	Displays the name of the workflow
Version status	Displays information on the version status
Execution status	Displays if the current state of execution
Dry Run Status	Displays if Dry Run has been executed or not

Click on the 👁 **View** button to view the Workflow.

Note: The user cannot edit the workflow in the View workflow page when navigating from the Monitor page.

AG Listing

The AG listing page displays the RTO and the Events information Relationship and continuity Workflows.

By default, the AG page displays ten AGs. Click **View All** to view all the AGs on the AG listing page.

The search bar is automatically backfilled with the search criteria based on the page context. The breadcrumbs help navigate to the desired page.

Each AG displays the number of RGs in the AG along with the group health graph.

On clicking the AG, the user is directed to the **AG Details** page.

AG Details

Click Monitor > Application Groups to get the AG Details.

Click **RTO** to view the RTO status. The RTO summary status is displayed in the RTO tab.

Click on **Events** to view the Sequence of Events that has occurred. The graph displays the time and the date of the event occurrence.

If it is a critical event, it is represented in red, and the serious event is represented in amber color respectively as shown below.

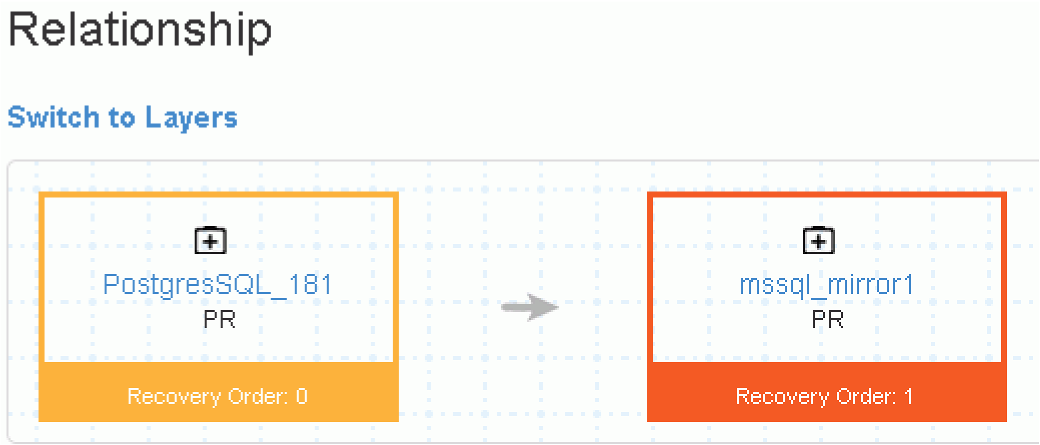
To view the relationship of RGs within the AG click **Relationship**.

The next table displays the **Continuity Workflows**.

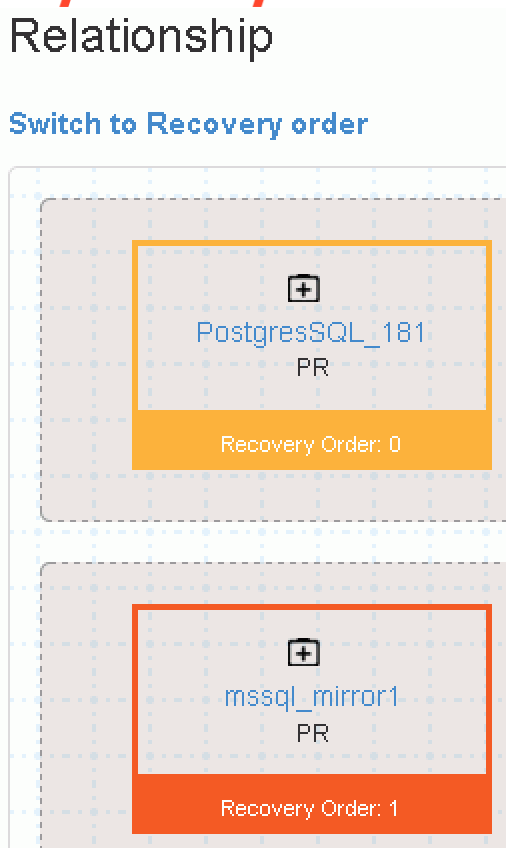
Relationship

The **Relationship** between the RGs within the AG is displayed. There are two ways of representing this; **Layers** and **Recovery Order.**

The layers will represent the relationship in the form of layers and the recovery order will represent the relationship in the order in which they will be recovered. Layers showcase the serial order and recovery order represents the parallel execution of the RGs.



In setting the relationship to switch to the recovery group the RGs are one below the other as shown below



- Each box represents a recovery group.
- The colors of the RGs represent the **group health**
- The icon ⊞ represents the recovery group and the name of the recovery group is displayed
- The Site location is displayed. Here the site location is PR.

Recovery Group

Recovery Group

Click **Monitor** > ⊞ **Recovery Groups** to view the Recovery Groups. The Group Health meter on the RG page displays the number of recovery groups under each state. The RGs can be classified under these four colors which display the health of the group.

The group health graph displays the recovery groups in each group's health state. On hovering over the graph, the percentage of each group's health is displayed.

The filter by default is set as Type 1. The RG listing page displays ten recovery groups, on clicking **View All,** all the recovery groups are displayed. For each recovery group, the following information is displayed.

Field	Description
Recovery Groups	Displays names of the RGs
RPO	Displays the configured RPO (in minutes) of the Group. **Note** If the configured RPO and the current RPO for the Group have crossed the threshold value you can view the deviation in red (or orange). If the deviation is within the threshold value, the deviation is represented in green.
RTO	Displays the RTO status (in minutes) for the Group. The 🕒 current RTO and the 🕒 configured RTO are displayed. If there is any ↱ deviation, the percentage is displayed.
Pending Data	Display the data lag and display when the last replication has occurred
Validation	Displays information if the validation has been executed.
Config Exposures	Displays the critical and non-critical list

There are eight types of filters for an RG. See **Filters**.

On clicking the Recovery Group, the **RG Listing** page is displayed.

RG Listing

Click **Monitor** > ⊞ **Recovery Groups.** The group health of each recovery group is displayed beside the recovery group.

The **RG Listing** page is displayed. The RG Listing page displays the following details of each recovery group.

Note: For VM protection solutions, the RTO tab is not displayed. However, the RG Group listing page displays RTO as Workflow not published.

Field	Description
Recovery Groups	Displays names of the RG

RPO	Displays the configured RPO (in minutes) of the Group **Note:** If the configured RPO and the current RPO for the Group have crossed the threshold value you can view the deviation in red (or orange). If the deviation is within the threshold value, the deviation is represented in green
RTO	Displays the RTO status (in minutes) for the Group. The 🕒 current RTO and the 🕒 configured RTO are displayed. If there is any ↱ deviation, the percentage is displayed. For more information see Viewing RTO Details
Pending Data	Display the data lag and display when the last replication has occurred
Validation	Displays information if the validation has been executed
Config Exposures	Displays the critical and non-critical list

Click on the group name to view the **RG Details** page.

RG Details

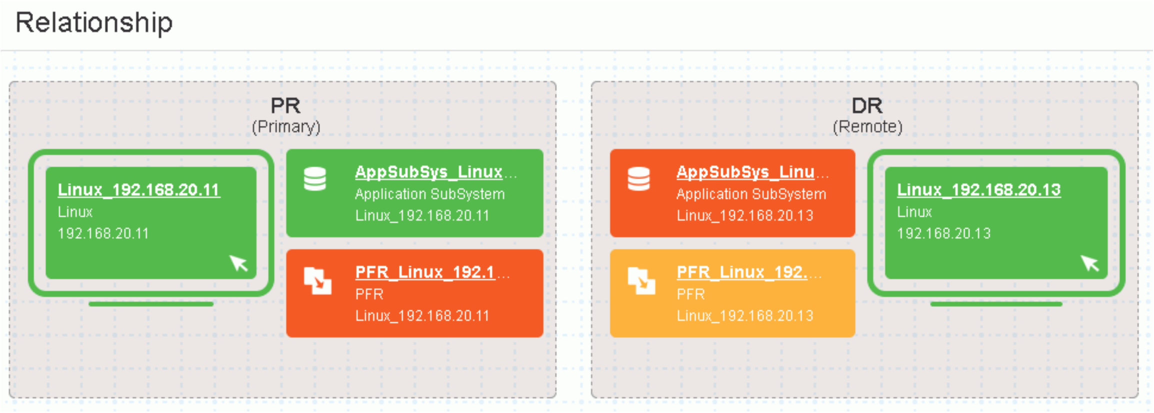
To view the details of each RG, navigate to **Monitor**> **Recovery Groups, and** click on the **RG name**.

Field	**Description**
RTO	Displays the **RTO** status (in minutes) for the Group. The 🕒 current RTO and the 🕒 configured RTO are displayed. If there is any ↱ deviation, the percentage is displayed
RPO	Displays the configured RPO (in minutes) of the Group. **Note:** If the configured RPO and the current RPO for the Group have crossed the threshold value you can view the deviation in red (or orange). If the deviation is within the threshold value, the deviation is represented in green

Field	Description
Service Details	
Events	Displays the events. For more information click Sequence of Events
Validation	Displays information if the validation has been executed
Config Exposures	Displays the critical and non-critical list

Relationship in RG

The **Relationship** image displays the relationship between the RGs within the AG in the PR and the DR site.



↖ represents the component. Clicking on the component link will display a confirmation navigation message. Clicking Yes will take you to the respective component and allow you to only view the component details.

🗄 represents the database. Clicking on the database link will display a confirmation navigation message. Clicking Yes will take you to the respective database and allow you to only view the database details.

⧉ represents the replicator. Clicking on the replicator link will display a confirmation navigation message. Clicking Yes will take you to the respective replicator and allow you to only view the replicator details.

Click **View all workflows** to view the BCO and BP workflows.

The BCO and BP workflows have the following:

- NormalFullCopy
- NormalCopy
- Failover
- Fallback
- FallbackResync
- ReverseNormalcopy

The version status, execution status, and DryRun Status of each workflow are displayed.

Continuity Workflows

To view the business process workflows:

1. Click Monitor > AG/RG > Application Group/Recovery Group Name.
2. The **AG Details**/**RG Details** page is displayed.

3. Click **View All Workflows** if it is an RG.
   - Click the **BCO Workflows** tab and all BCO workflows are displayed for the RG.
   - Click the **BP Workflows** tab, and all BP workflows are displayed for the RG.

The following details are displayed:

Field	Description
Workflow Name	Displays the name of the workflow. Displays the group name for which you want to add the business process.
Version status	Displays the group name for which you want to add the business process.
Execution status	Displays information if the execution was successful, crashed aborted, or is awaiting input.
Dry Run Status	Displays information if the workflow was a success, crashed, not executed, or failed

- Click 👁 to preview the workflow.

Note

- If the group is in switchover or switchback, then the current DR state of the group does not permit any continuity operations.
- To change the state of the group, go to **Discover** > **Groups** page.

To view the execution history and the version history, click on the workflow name.

The **Execution History** displays the following information:

Field	Description
Date	Displays the date of execution
Time Taken	Displays the time taken in seconds for execution
status	Workflow execution status
Version	Displays the version number

The **Version History** displays the following information:

Field	Description
Version	Displays the version number
Created On	Displays the workflow created time
Created By	Displays the username

Executing Workflows

Executing Workflow

You can view the details of the workflow that is currently executing along with the details of each action of the workflow.

To view the Workflow, do the following:

1. Click the **Monitor >** **Executing Workflows** tab on the navigation bar to view the **RG listing** page.
2. For the desired Group, select the **Workflow link** from the **WORKFLOW DETAILS** column. The **Workflow Execution** page appears.
3. Select the RG/AG from the drop-down list filter. If the selected group is RG, then the eight types of **filters** are displayed and if it is an AG, then only four types of filters are displayed.
4. Select the workflow from the drop-down list. If the selected group is a Recovery Group, the workflow drop-down list displays the following workflows:
    - BCO
    - BP
    - Policy
    - System Workflow
    - All

The following details are displayed:

Field	Description
Group	Displays the name of the workflow.
Workflow	Displays the Workflow name and its present version.
Time Started	Displays the start time of the Workflow.
Elapsed Time	Displays the time elapsed from the process of initiation to completion of the Workflow.
Status	Displays the status of the Workflow and the count reflects the number of completed actions versus total actions.

On clicking the Group name, the user is directed to the RG details page or the AG details page of that group.

On clicking the **Workflow**, the Execution History and Version History are displayed.

Click the executing link, the workflow page is displayed.

Note:

- Click **Key Value Pairs** to view the Key values configured for this Workflow.
- Click Abort to stop workflow execution. The Reason to Abort pop-up appears, enter the reason, and click on Reason to Abort.
- Click Export to CSV to export the workflow details to CSV file format.

Click the **Workflow Actions** tab to view the execution details of actions within the workflow.

Field	**Description**
Action	Displays the name of the action.
TIME INITIATED	Displays the exact start time of the action execution.
TIME ELAPSED (SEC)	Displays the time calculated from the process of initiation to completion of the action.
TYPE	Displays the type of action.
STATUS DETAILS	1. Displays the status details of the action execution. Note: 2. If the status is in EXECUTING mode, the user can click on the EXECUTING link to view the Continue as Success or Continue as Failure option buttons. Depending on the requirement and by giving a reason, select any one of the options. 3. If the Status is Awaiting Input, depending on the requirement, the user can select any one of the below options: 4. Continue as a Success 5. Continue as Failure 6. Retry 7. Quit If a user wants to know the reason for Awaiting Input, click the View action log button. 8. Click on any link corresponding to the desired action to view the following details for the action. 9. DB Logs 10. Tail Logs 11. Sys Logs

4. Click the **Go Back** link to view the **Active Workflow Listing** page.

Note:

- DB Logs: Displays the Oracle and MSSQL DB Logs. Configure the Error log path while dataset discovery of MSSQL only then we will get the DB Log link for MSSQL.
- Tail Logs: Displays the logs from the path configured in Custom Action.
- Sys Logs: Displays the Linux Operating System Logs.

In the **Workflow Actions** tab, the actions are grouped under the respective Action Groups so that you can know the action belongs to which Action Group.

Note: Time Elapsed in the Workflow and total time elapsed for all Custom actions in the workflow are not the same. It is dependent on multiple other factors.

Health Monitoring

The health of the group is continuously monitored, and the status is available as a **Group Health Graph** on the Recovery group page. When there is a change in the status of the health of the groups an event arises.

To navigate to the **Group Health Graph**, click **Monitor** OR **Manage on the Navigation bar. Then click** ⊞**Recovery Group.** The Group Health meter on the RG page displays the number of recovery groups under each state.

Viewing Group Relationship

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the relationship details of a Group, perform the following steps:

1. Click **Monitor** on the navigation bar. The **RG Listing/ AG Listing** page appears.
2. Click the desired Group from the **Recovery Groups** column. The **Recovery Group listing** page for the respective RG or AG appears.
3. View the **Relationship** diagram.

Group Dependency

The **Group Dependency** tab under the **Application Group** displays a visual representation of all RGs dependent on the AG. Click each RG name against its box to display its **Recovery Group**. You can also view the order in which Failover will be done during disaster recovery by checking the arrow above the **Group Failover order**.

Recovery Group Relationship

You can view the relationship between the configured production and the DR in a pictorial representation by navigating to the **Recovery Group Details.** This page displays the solution-specific replication details, names, and status of the datasets, protection schemes, and components on production and DR servers.

You can expand or collapse the Replication, Component, and Dataset details by clicking **Expand All** and **Collapse All** links at the top right corner of the page.

RPO and RTO Monitoring

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To view the RPO and RTO details of a Group, perform the following steps:

1. Click **Monitor** on the navigation bar. Click **Recovery Groups.**
2. Click the desired Group from the **Recovery Groups** column. The **Recovery Group** page for the respective RG or AG appears.
3. Click the **RTO/ RPO** tab respectively. The tabs are displayed for the Recovery Group. This displays the following information:

Note:

For VM protection solutions, the **RTO tab is not displayed**. However, the RG Group listing page displays RTO as **Workflow not published**.

Field	Description
App RPO Summary	Displays Configured RPO, Current RPO with the percentage of Deviation from the configured RPO, and the Recovery Point. For more information see Viewing App RPO Details.
Data RPO Summary	Data RPO summary table will be displayed if the solution supports Data RPO. Viewing Data RPO Details.
RTO Summary	Displays Configured RTO, Current RTO with a percentage of Deviation from the configured RTO, and the Recovery Time. For more information see Viewing RTO Details
RTO Breakup	Displays the name of the Recovery Step executed during the recovery process along with the Expected Completion Time in seconds.

Note: If the number of RG’s more than 5 then follow the below instructions:
Change the value of the property ‘**org.quartz.threadPool.threadCount**’ in the file ‘**$EAMSROOT/installconfig/panaces.properties**’ to the number of RG.
For example; if you have 18 RGs then the property should have 18 as below
org.quartz.threadPool.threadCount = 18

Continuity Monitoring Overview

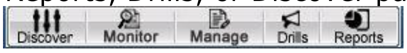
Monitoring facilitates viewing the state information of the continuity operations execution, the replication statistics, and the Events for the groups being monitored.

Once the groups are in the Managed state, you can monitor the following:

- Continuity - Provides information about the continuity state of the group along with the current status of the RPO and RTO.
- Replication - Provides information about the replication mechanism along with the details of data or files replicated for the respective group.
- Events - Provides information about significant Events and warnings for the respective groups.

Click on the respective link to view the current status of the list of groups being monitored. If you want to view the detailed information about Continuity or Replication or Events for a specific group, click on the group from the **Group Name** column available in the respective links.

Note

From Recovery Group or Application Group Dashboard in Continuity, Replication, or Events, you can navigate to the Monitor, Manage, Reports, Drills, or Discover page of a displayed group by clicking on the respective icon  at the top right corner of the respective group's dashboard window.

Pending Data

You can view the detailed Replication List by clicking **Monitor** > **Recovery Groups** and the **Recovery Groups Listing** page appears.

Select any Group name and click the Pending data tab.

On the **Pending Data** tab, you can monitor the replication process for each group by viewing the detailed replication status of the group and the protection scheme associated with the Group. Storage-related information about the monitored RG and information about data consistency i.e. whether the DR site is in sync with the Production without respect to data replication are also displayed. For example, for a Group configured under the SRDF Protection Scheme, you can view the IDs of the source and target symmetric units.

The Replication tab displays the Data log and the last updated time the files have been replicated.

Field	**Description**
Data Lag	Displays the data lag information for the RG
Last Updated	Displays the time when the RG was last updated

Click **Refresh Details** to refresh the replication page.

The replication details are displayed in the table:

Field	Description
Protection	Displays the replication type
Replication status	Displays the status of the replication, Active Inactive and Unknown
Primary-Remote service	Displays the PR and DR information

Note: This table consists of basic information for all groups. Additional information will be displayed, depending on the Replication Type.

Viewing Recovery Group Replication Details

To view the DR solution-specific replication details of the RG, perform the following steps:

1 Click **Monitor > Recovery Groups. The RG Listing Page appears.**

2 Click **Group Name** in the **RG Listing Page.**

3 Click the **Pending Data** tab.

4 The **Replication Details** page is displayed that lists the DR Solution-specific replication details. The Replication tab is displayed only for that Recovery Group.

Click the **Refresh Details** to refresh the information.

Events

Event Life Cycle

Every event has a life cycle. When an event occurs, its status is "New", for which some action (manual or automated) might be required. When the action is being taken the event is associated with "Response in Progress" status. After completion of the action, the event is associated with "Closed" status.

Automatic Closing of Events upon Aging

Aging is a process of moving unattended "New" events to "Closed" state. By default, the aging period is set to 5 days. The aging is computed/performed at 00:00 AM every day.

All Events irrespective of its Severity but with "New" state older than the aging period will be moved to "Closed" state except for User Input events.

Handling UserInputRequiredEvents

UserInputRequiredEvents cannot be moved to "Closed" or "Response in Progress" states by the user. Once input for a userInputRequiredEvent is provided, it will be moved to Closed state immediately. However, the corresponding userInputObtainedEvent will be closed during aging process (or user can move it to "Closed" state).

When Kyndryl Resiliency Orchestration Server is started all userInputEvents (userInputRequiredEvent/userInputObtainedEvent) will be moved to "Closed" state irrespective of its status.

Events with policy execution

When the policy execution succeeds, the corresponding event will be automatically moved to "Closed" state. In case the policy fails, the event will be moved to "Response in Progress" state automatically. The user is expected to respond to such events and move to Closed state.

Event duration

The events that have occurred in the last 5 days / 120 hours (default value) will be displayed in the **Events** page. This value of 120 hours is applicable for events that are listed after applying filters and search text as well as text search without filters.

The display duration is configurable and can be changed by altering the property sanovi.events.displayDuration.hours in the panaces.properties file.

Default configuration in panaces.properties –

```
# Display the events occurred for the past 'n' hours.
# This is specified in hours. The default is 120 hours (5 days).
```

```
sanovi.events.displayDuration.hours=120
```

Event Alarm

Event Alarm displays the number of critical events, serious events, Events awaiting inputs and Config Exposures across the applications. This will be displayed below navigation bar on all the windows of the Kyndryl Resiliency Orchestration.

If there are no corresponding events, then it will show zero. These counts will refresh automatically in every 60 seconds. By default, these counts are shown for events occurred in the past 5 days.

Click the corresponding icon on the **Current Events** to see the filtered list of events based on severity. This navigates you to the **View Events** page.

User can also click on the **Critical** icon to view only critical events and **UserInput** icon to view only **UserInput** events.

View Events

The Events DETAILS page displays Group events, user-input-required events and System events. It displays the events occurred in the past 5 days by default.

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To view Events details, perform the following steps:

1. Click **Current Events** link in the Secondary Navigation Bar in the top right corner. The **Events** page appears.

Following table explains the specific information displayed in the Events page.

Fields	**Functions and Descriptions**
Events Search	Use this box to search by either Event Name or Description. For more information, see **Searching Events**.
Advanced Filter	This option allows advanced filter facility for events, based on event severity, user-input events, and group names. For more information, see **Filtering Events**.
Include	Select the check box(es) to filter the events based on its severity. The available check boxes are **Critical**, **Serious** and **All User Input Events**.
Event name	Displays the name of the event along with the status.
Description	Displays the description of the occurred event.

Fields	Functions and Descriptions
Group Name	Displays the name of the Group.
TIME	Displays date and time at which the event has occurred.
Severity	Displays the severity level of the events. 🔴- Critical 🟠- Serious 🟡- Warning 🔵- Information
OPERATION	Select the respective action for the event from the drop-down list. The available options are: **Show SOE** - Displays the Sequence of Events window. **Provide Input** - This option appears for the events that require your inputs. Selecting this option takes you to the **Recent Execution Status** window where you can provide the required inputs. **Execute Policy-** Executes the policy associated with the event.
Change State	Select the state from the drop-down list. The available options are **Closed** and **Response In Progress.** Select the check box(es) corresponding to the events for which the state must be changed, select the state from the drop-down list and click ✓.
Export to CSV	Click this link to export the events to CSV format.
View All Events	Click this link to view all events.

Click ⇕ to sort the following columns:

Fields	Descriptions
EVENT NAME	Sorts by event name.

Fields	Descriptions
GROUP NAME	Sorts by group name.
TIME	Sorts by time of occurrence of event.
SEVERITY	Sorts by event severity.

2. Click **Event ID**. The **Event Details** page opens as a pop-up window.

Fields	Functions and Descriptions
Name	Displays the event name. More than one event can have a same name.
Description	Displays the description of the event.
Severity	Displays the severity level of the events.
Impact	Displays the impact of the event.
Occurred On	Displays group on which the event has occurred.
Occurred Time	Displays time at which the event has occurred.
Policy Status	Displays the policy status if policy is applicable for the event.

3. Click **Close**.

Note:

In some case, the "Provide Input" operation will be shown even for events for which the input is already provided by some other user or in some other window. In these cases, the user will be redirected to the workflow page but will not see the workflow waiting for input. Refreshing the events page will remove these events from the list.

Viewing Group Events

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To view Group Events details, perform the following steps:

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click **Recovery Group** tab, the **Group listing** page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click the Group Configuration tab.

5. Click the **Events** tab.

Field	**Description**
Event ID	Displays the respective Event ID which identifies each event.
Event Description	Provides a brief description of the respective event.
Event Severity	Displays the level of severity of the respective event.
Event Impact	Provides information on affect/effects about the event.
Notify	Allows you to send notification regarding the event to the user. By default, SERIOUS and CRITICAL events are notified.

Note:

There can be multiple instances of same Event raised for a Group that require execution of same policy. However, only one instance of a policy can run at a time. In such cases, the later instances of the event are put to FAILED status. For example, there are three instances of Event E- E1, E2, and E3, raised for Group G, requiring the execution of policy P. If P is being executed for E1, its execution for E2 and E3 will be put to FAILED status. Once the policy execution for an Event is put to FAILED status, it cannot be initiated again. Instances of same event for different Group do not affect each other.

Filtering Events

Kyndryl Resiliency Orchestration provides you the facility to filter events, based on event severity, user-input events, system events and group names.

Click *Kyndryl Resiliency Orchestration Server User Role Management* to see the privileges.

To view Events details, perform the following steps:

1. Click **EVENTS** on the navigation bar. The **Events** page appears.
   OR
   Click the **List View** link at the top right corner of the **Events Summary** area on the **Dashboard** window.
2. Click the **Advanced Filter** link. This option allows advanced filter facility for events, based on event severity, user-input events and group names.

Fields	Functions and Descriptions
Select Event Type	Select the checkbox(es) to filter events based on event type. The available checkbox(es) is Group Events, All User Input Events, System Events. Note: The "System events" option will be available only to Administrator and Super Administrator users.
Select Event Severity	Select the checkbox(es) to filter events based on event severity. The available checkbox(es) is **Critical**, **Serious**, **Warning**, **Info.**
Select Event Status	Select the checkbox(es) to filter events based on event status. The available checkbox(es) is **New**, **In Progress**, **Closed.**
Select Groups	Select the group(s) for which you want to filter events from the list box. Hold down the "Ctrl" key to select more than one group. To select all groups associated with the user, select "-All My Groups-" option.

Complete Listing of Events

Click *Kyndryl Resiliency Orchestration Server User Role Management* to see the privileges.

You can view detailed information about the different events that have occurred so far in the entire DR environment by performing the following steps:

1. Click **Current Events** link in the Secondary Navigation Bar in the top right corner. The **Events** page appears.
2. Click **View All Events** link. It displays the following information about an event:

It displays the following information:

Fields	Description
Event [ID]	Displays the unique identification for the occurred event.
Event name	Displays the name of the event. More than one event can have the same name.
Group/ Subsystem Name	Displays the name of the Group or Subsystem to which the event is associated.
Severity	Displays severity of the event. The difference in the severity is shown by color coding. Refer **Managing Events** for more details. When the severity level goes high, the events are considered as **CRITICAL**. Refer **Viewing Group Events** topic for information about the possible severity levels for an event.
Status	Displays the status of the event.
Occurred time	Displays the time at which the event occurred in the format yyyy-mm-dd hh:mm:sec. For example, 2006-06-06 15:06:19.0.
Description	Displays the description of the occurred event.

This page lists the events occurred in the DR environment.

The following table shows the functionality of each button:

Button	Description
Refresh	Refreshes the page to fetch the latest events.
Next	This button is displayed when there are more events to be displayed other than the 30 events displayed on the current page.

Every BCO operation will be notified to the users configured in the Notification list of that Group. The following are the sample notifications sent to the users configured to the AG and its associated RGs.

When BCO is initiated on an AG, notifications are sent to users in the notification list in the AG. Here is a ***sample mail***.

Subject:

Resiliency Orchestration: testAG1: Failover started at 2005-05-10 21:10:49.74

Notification:

Notification List: Test_NL1,

Group Details:

...Name: testAG1

Description: this is testAG1

Type: APPLICATION GROUP

Current Status: MANAGED, INACTIVE

Operational Details:

Continuity Operation: Failover

Status: Failover started

Start Time: 2005-05-10 21:10:49.74

End Time: -

Actions to be performed by User: None

After this, notifications are sent to the users of Notification List of every RG. Here is a ***sample mail for RG***.

Subject:

Resiliency Orchestration: testFG1: Failover started at 2005-05-10 21:12:10.292

Notification:

Notification List: Test_NL1,

Group Details:

Name: testFG1

Description: this is testFG1

Type: FUNCTIONAL GROUP

Current Status: MANAGED, INACTIVE

Operational Details:

Continuity Operation: Failover

Status: Failover started

Start Time: 2005-05-10 21:12:10.292

End Time: -

Actions to be performed by User: None

If a user input is required, then a notification is sent to all the users of the Notification lists of the RG. Click ***here*** to see a sample mail.

Subject:

Resiliency Orchestration: testFG1: Failover waiting for user input since 2005-05-10 21:13:17.953

Notification:

Notification List: Test_NL1,

Group Details:

Name: testFG1

Description: this is testFG1

Type: FUNCTIONAL GROUP

Current Status: MANAGED, INACTIVE

Operational Details:

Continuity Operation: Failover

Status: Failover blocked, awaiting user input

Start Time: 2005-05-10 21:12:29.0

End Time: -

You must perform the following actions:

Login to Kyndryl Resiliency Orchestration and take the necessary actions for the Group "testFG1".

When the BCO on RG failed/succeeded then ***notifications*** are sent.

Subject:

Resiliency Orchestration: testFG1: Failover failed at 2005-05-10 21:49:38.0

Notification:

Notification List: Test_NL1,

Group Details:

Name: testFG1

Description: this is testFG1

Type: FUNCTIONAL GROUP

Current Status: MANAGED, INACTIVE

Operational Details:

Continuity Operation: Failover

Status: Failover failed

Start Time: 2005-05-10 21:12:29.0

End Time: 2005-05-10 21:49:38.0

Perform the following actions:

Log in to Kyndryl Resiliency Orchestration and check the detailed Workflow status on the **Application/ Recovery Group > RG listing** > **Group Name** > **Continuity Workflow Details** link to determine the reasons for failure.

When a BCO on RG fails, it translates to a AG failure. Then a ***notification*** is sent to all notification lists of the AG.

Subject:

Kyndryl Resiliency Orchestration: testAG1: Failover failed at 2005-05-10 21:50:04.0

Notification:

Notification List: Test_NL1

Group Details:

Name: testAG1

Description: this is testAG1

Type: APPLICATION GROUP

Current Status: MANAGED, INACTIVE

Operational Details:

Continuity Operation: Failover

Status: Failover failed

Start Time: 2005-05-10 21:12:08.0

End Time: 2005-05-10 21:50:04.0

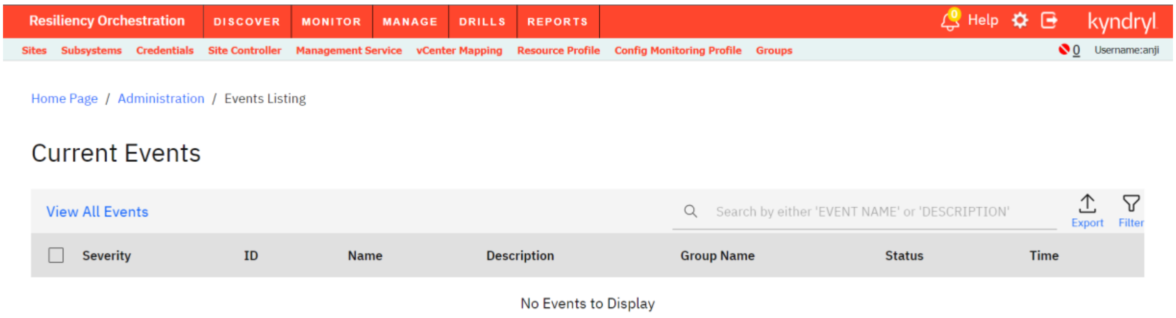
You have to perform the following actions:

Log in to Kyndryl Resiliency Orchestration and check the detailed action set status on the Continuity pages to determine the reasons for failure.

Searching Events

The Event Search feature allows users to search for events by either Event Name or Description. It's a text search capability which will search for the presence of the text in the Event Name or Description of all the events in Kyndryl Resiliency Orchestration.

The following screenshot shows the Events Search text box in the **Events** page.



Current Events

□ Severity	ID	Name	Description	Group Name	Status	Time

No Events to Display

User can enter any text by which they want to search, an IP address for example. If the IP address is present in the Event Name or Description field of any event, such events will be listed.

Events page provides user with filters (refer **Filtering Events**). The search text can be used on top of the event filters. User can enable the filters such as Critical and Serious and then search by plain text such as "is accessible". The result will be a subset of events that are either Critical or Serious and contains the text "is accessible" in the Event Name or Description fields.

System Events

System events can be viewed only by super administrator or administrator. At least one notification list or SNMP Trap Forwarder must be configured to receive notifications regarding system events. There will not be any policy configuration for system events.

Note:

There will not be any auto refresh to this page.

To view system events:

1. Click **Admin > System Events** on the navigation bar.
2. The **System Events** page appears with the following information.

Field	Description
Event ID	Displays the respective Event ID which identifies each event.

Event Description	Provides a brief description of the respective event.
Event Severity	Displays the level of severity of the respective event.
Event Impact	Provides information on affect/effects about the event.
Notify	Allows you to send notification regarding the event to the user. By default, SERIOUS and CRITICAL events are notified.

3. Select the check box corresponding to the Event ID for which you want to notify the user on occurrence of it.

Note: To receive notification regarding the event, at least one notification list or SNMP Trap Forwarder must be associated with the group. For more information on creating notification list, refer to Adding Notification List.

Click the Update Selection button.

Monitoring Events

You can view the summarized view of the properties of all configured Groups by clicking the **EVENTS** tab on the navigation bar.

Following table explains the specific information displayed for each Group in the **Events** page.

Field	**Description**
Group Name	Displays the name of the monitored RG . Click this Group link to view the complete event list of the Group.
Critical	Displays the number of events of severity **CRITICAL** that have occurred at the RG level. Refer **Viewing Group Events** topic for information about the possible severity levels for an event.
SERIOUS	Displays the number of events of type **SERIOUS** that have occurred on the RG.

View the complete list of events across groups by clicking the **View All Events** link. This list displays BCS and Agent events. BCS events are Group specific and are raised on different BCOs of a Group. Agent events are not specific to a Group and are raised for various components of the DR environment.

Monitoring Users and Passwords for Raised Events

Kyndryl Resiliency Orchestration provides monitoring of database users and passwords. Adding, deleting a user, and changing the password for a user raises a BCS Event in Kyndryl Resiliency Orchestration. These events inform you of the changes done for database users and their passwords. It is recommended to add or delete a user and change the password when Normal Copy is in progress.

For MSSQL and Sybase databases, the system level database user and the users authenticated by this user are monitored. However, for the Oracle database, only the user specified at the time of Oracle dataset setup is monitored.

Note: Avoid using system level log-in credential while adding or deleting a user. This is to avoid failing the operations running on the database if you change the password later.

Kyndryl Resiliency Orchestration monitors the users and passwords related changes every ten minutes. If more than one user is added in less than ten minutes, these changes are summarized and reported in a single event. If one or more users are added and deleted in less than ten minutes, two separate events are raised, one each for adding and deleting users.

Recovery Automation

Managing Groups

Group Maintenance - Working with Different Modes of Group

This chapter describes how to change the modes of a Group.

However, Group's BCM state may change automatically as a result of failure of one of the actions in a BCO.

Such situations are handled by Kyndryl Resiliency Orchestration itself in the concrete DR Solution. In a generic DR Solutions, Kyndryl Resiliency Orchestration provides facility to customize BCO workflows as per your needs. As part of this customization, you can trigger another BCO, if the current BCO fails. This is achieved by adding a Trigger BCO action manually in the workflow. However, it may be possible that the intended action from Trigger BCO is already completed or in progress, when the current BCO fails. This results in the failure of Trigger BCO action. In such cases, click **Continue** in the **Workflow Manager** page to skip the failed action and to move to the next.

Continuity Management Overview

You can view the list of groups being managed by Kyndryl Resiliency Orchestration by clicking either the Monitor or the Manage tab on the Kyndryl Resiliency Orchestration GUI.

As soon as the groups are configured, you can edit, delete and manage the following by clicking the Manage tab on the Kyndryl Resiliency Orchestration GUI:

- RG Listing - Provides the list of groups being managed with the group continuity state and the Workflow details.
- Executing Workflows - Provides the list of current actions of the respective continuity operations being executed.

Click the respective links to view the current continuity operation and action set being executed for a specific group.

Click on ⇅ to sort the following columns:

Field Name	**Description**
GROUP NAME	Sorts by group states
CURRENT STATE	Sorts by group continuity states

Note:

In Manage:

- You can change continuity states.
- You can initiate BCOs.
- You can Start and Stop replication.

To navigate to Monitor, Reports, Drills or Discover page of a displayed group:

1. Click **Manage**
2. Select the required tab from the drop down.

Note: If the Group is in Switchover mode, it cannot be managed with only the Recovery license enabled. To manage the Group, enable the Test license and change the state to Normal mode.

Changing Group to Managed Mode

Any BCO on the Group can be performed only when the Group is in the Managed state.

Click **Kyndryl Resiliency Orchestration Server User Role Management to** see the privileges.

To change the Group to MANAGED mode, perform the following steps:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.

2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click 🛠 corresponding to the desired group. The **Continuity Operation** window appears.
4. Click on **Manage Group** button.

   Note: You cannot modify the Group details when the Group is in Managed mode.

5. A message box with successful Group mode change operation is displayed. Click **OK** on the message box displayed.

If the Group is in MANAGED mode currently and not executing any continuity operation, it may be put into MAINTENANCE mode.

Changing Group to Maintenance Mode

Note: If a policy is being executed for a Group, you cannot change that Group to Maintenance mode. Trying to move it anyway will display an error message. You may need to stop the policy execution or let it complete before changing the Group to Maintenance mode.

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To change the Group into Maintenance mode, perform the following steps:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click 🛠 corresponding to the desired group. The **Continuity Operation** window appears.

The maintenance activities can be used by the owner of the Group to bypass certain activities or to recover from certain failures. All maintenance related activities should be done only after moving the corresponding Group to Maintenance mode. Further, all related agents should be stopped before performing maintenance activities.

Caution

Usage of this activity, if not performed correctly, may significantly impact the Continuity Management of the Group. It is not recommended to be used by the end user.

4. Click the **Move to Maintenance** button.
5. A message box with successful Group mode change operation is displayed. Click **OK** in the message box displayed.

Note

To manage AG's, all the RG's should have similar modules assigned to them. And each RG inside the AG should have at least one module assigned.

🛠 icon corresponding to a group is enabled and you can change the group to maintenance mode when no workflows are running or when BP workflows or event policy workflows are running.

🛠 icon corresponding to a group is disabled and you cannot change the group to maintenance mode during any BCO or SO/SB drills execution.

Changing the Business Continuity State of a Group

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To move the Group from current Business Continuity State (BCS) to a new BCS, perform the following operations:

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click 🛠 corresponding to the desired group. The **Continuity Operation** window appears.
4. Click the **Change Continuity State** tab.
5. Select the required **Group State** field from the drop down list.
6. Click **Change**.
7. Click **OK.**

Note

A Group can be moved to a new continuity state only when the Group is not executing any continuity operations.

The following are the **Select Target State** options for the below licenses:

Select Target State options	**Test License**	**Recovery License**	**Test and Recovery License**
NORMAL RESET	✗	✓	✓
NORMAL INACTIVE	✗	✓	✓
FAILOVER ACTIVE	✗	✓	✓

Select Target State options	Test License	Recovery License	Test and Recovery License
FALLBACK ACTIVE	⊗	✓	✓
SWITCHOVER INACTIVE	✓	⊗	✓

Note

- 🛠 icon corresponding to a group is enabled and you can change the Business Continuity State of a Group when no workflows are running or when BP workflows or event policy workflows are running.
- 🛠 icon corresponding to a group is disabled and you cannot change the Business Continuity State of a Group during any BCO or SO/SB drills execution.

Business Continuity Operations

Based on the current BCM and BCS (Business Continuity State) of the Group, continuity operations such as 'Initiate NormalCopy', 'Initiate Failover', 'Initiate Fallback' etc. are possible. These operations are listed as selectable buttons. The complete list of operations is as given below:

Operations	Description
Initiate NormalFullCopy	This operation initiates NormalFullCopy operation.
Initiate NormalCopy	This operation initiates NormalCopy on the specified FG. This typically involves periodic extraction of data from production and application of changed data on DR. In some DR Solutions, NormalCopy is a monitoring only operation, as the replication technology in use handles transferring the data between the production and DR databases.
Stop NormalCopy	This operation stops the NormalCopy on the Group under consideration. Clicking this button displays a page to reconfirm the stopping of the operation.

Operations	Description
Initiate Reverse NormalCopy	This operation is the reverse of the NormalCopy as this is initiated after the Switchover operation and the data is replicated from production (configured DR) to the DR site (configured production).
Initiate Failover	This operation initiates Failover operation on the Group during the failure of the production site. Clicking this button displays a page to reconfirm the initiation of the operation.
Initiate Fallback	This operation initiates a Fallback operation when production comes live again.
Change Continuity State	This operation lets you move a Group from the current BCS to a new BCS. This operation is possible only when the Group is not executing any continuity operations currently.
Resume Operation	This operation lets you to get back Kyndryl Resiliency Orchestration server online after the server crash.

Note

In generic solutions, Kyndryl Resiliency Orchestration provides facility to customize BCO workflows as per your needs. As part of this customization, you can trigger another BCO, if an action in the current BCO fails. This is achieved by adding a Trigger BCO action manually in the workflow. However, it may be possible that the intended action from Trigger BCO is already completed or in progress when an action in the BCO fails. This results in the failure of Trigger BCO action. In such cases, click Continue in the Workflow Manager page to skip the failed action and to move to the next.

The following table lists the next possible operation based on the current state of operation.

Note

Reverse Copy button appear only when the DR Solution type supports these BCOs.

State	Next Operation
Normal Reset	Initiate NormalFullCopy, Change Continuity State, Move to Maintenance

State	Next Operation
Normal Inactive	Initiate NormalCopy, Initiate Failover, Change Continuity State, Initiate Switchover, Move to Maintenance
Normal Transit	-
Normal Active	Stop NormalCopy
Normal Failed	Initiate NormalCopy, Initiate Failover, Change Continuity State, Initiate Switchover, Move to Maintenance
Normal Degraded	Stop NormalCopy
Switchover Inactive	Change Continuity State, Initiate Reverse Copy, Initiate Failover, Initiate Switchback, Move to Maintenance.
Switchover Transit	-
Switchover Active	Stop Reverse Copy.
Switchover Failed	Initiate NormalCopy, Initiate Switchover, Initiate Failover, Change Continuity State
Failover Transit	-
Failover Failed	Initiate Failover, Initiate NormalCopy, Change Continuity State, Move to Maintenance
Failover Active	Initiate Fallback, Change Continuity State, Move to Maintenance
Fallback Transit	-
Fallback Failed	Initiate Fallback, Change Continuity State, Move to Maintenance
Fallback Active	Initiate FallbackResync, Change Continuity State, Move to Maintenance
Normal Shutdown	Resume Continuity operation, Change Continuity State, Move to Maintenance
Normal Stopping	-
Normal Test	Initiate NormalCopy, Initiate Failover, Change Continuity State, Initiate Switchover, Move to Maintenance (Do not perform any BCO when the test exercise are being performed on the Group)

The following table technically explains the Business Continuity Operations and the state of production and DR server. It is applicable only for DR Solutions based on Sybase and MSSQL databases.

BCO	Functionality	Production Server's mode of operation	DR Server's mode of operation
Before NormalFullCopy	Nil	Read, Write	No existence of database
After NormalFullCopy	Takes full dump of data from production to DR site and both servers are in sync with each other.	Read, Write	Standby
NormalCopy	Copies incremental log files from the production to DR.	Read, Write	Standby
Reverse NormalCopy (Not supported for DR Solutions based on MSSQL and Sybase databases)	Copies log files from current production site to current DR site.	Standby	Read, Write
Auto Failover	Production server is brought down and the DR server is made available for access.	No Data is available	Read, Write
Manual Failover		Standby	Read/Write
Before Fallback Start	The server at the production site should not have any data.	NA	Read/Write
After Fallback	The existing copy of data on the DR server (current production server) is copied to the production. The data on the remote is deleted after a copy is made to the production.	Read/Write	Standby

BCO	**Functionality**	**Production Server's mode of operation**	**DR Server's mode of operation**
FallbackResync	This operation copies the incremental log on the current production server (DR) to the production server.	Read/Write	Standby
At the end of FallbackResync	The production server is brought back to production and the DR server is made stand-by	Read/Write	Standby

Configuration of BCOs

Every Group is associated to business continuity operations (BCO) through the supported DR Solution types. The continuity operations for a Group are as follows:

- NormalFullCopy
- NormalCopy
- Failover
- Fallback
- FallbackResync

BCOs are configured when the actions associated to each operation are configured.

To configure a BCO perform the following steps:

1 Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.

2 Click **Recovery Group** or **Application Group** tab, the respective **Group Listing** page appears.

3 Click the required group from the **GROUP NAME** column for which you want to configure the BCOs. The **Group Details** Page appears.

4 Click the **Manage** icon.

5 Click the View all workflows link.

6 Click on the Edit icon of respective BCO to configure its actions. This opens the **Edit Workflow** page with a list of actions.

Note

All actions should be configured and workflow should be published before the execution of respective BCO.

NormalFullCopy

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To start the NormalFullCopy operation perform the steps provided in **Executing Business Continuity Operations** topic in this Help.

In this operation, the full dump of the configured database on the production server is copied to the DR server either manually or through network connection.

Refer to the '**Executing BCOs**' topic in the respective solution guide under DR Solutions Supported by Kyndryl Resiliency Orchestration book in this Help for more information on the execution of the NormalFullCopy operation.

At the end of this operation, the DR server goes to 'standby' mode and the production server remains in read-write mode. At the end of this operation the DR Solutions and the DR database are in-sync with each other.

When NormalFullCopy is initiated at the AG level, the operation gets triggered on the associated RG to perform NormalFullCopy operation at the AG.

When this operation has been initiated, the actions associated with this operation will be executed.

If **Inform Upon** is set to 'ALL' during the action configuration of this Business Continuity Operation, then you can see a window pop-up displaying the status of the operation at the completion of this operation. Suppose a particular action is not executed correctly, then you can see action failure wizard. Click **Retry** button to re-execute the action execution. If this message persists, please contact Kyndryl Resiliency Orchestration support.

If all the actions are executed, the Execution Status of the NormalFullCopy operation can be viewed by clicking the Monitor OR Manage on the Navigation bar and following the path-

Recovery Groups > Group Name > Continuity Workflows > Execution Status.

Note:

You can click the Pause/ Resume button at any time to pause or resume the operation respectively for the Application Recovery on AWS solution (VMware to AWS).

NormalCopy

The operations that can be initiated next to NormalFullCopy are NormalCopy and Failover. Failover is triggered only at the time of disaster. NormalCopy is a recurring process, where the data is replicated to the DR site at a specified time interval to make both the sites in-sync with each other.

Click Kyndryl Resiliency Orchestration Server User Role Management to see the privileges.

To start the NormalCopy operation perform the steps provided in **Executing Business Continuity Operations** topic in this Help.

During NormalCopy the incremental log files generated on the production server are copied to the DR server at equal intervals. This is an on-going process and will never end until the process is intentionally stopped or accidentally stopped by a disaster. So, during this operation the production server is the primary server and the DR server is the Stand by server.

For the SRS solution, NormalCopy is a monitoring only operation, as managing the process of transferring data between the production and DR databases is handled by the Sybase Replication Server.

Note

NormalCopy cannot be initiated during Test Exercises.

The execution window of the NormalCopy operation lists the following details:

- Configured Properties
- Current Properties
- Recent continuity operation
- NormalCopy Operation Additional Details

The table lists the values configured before initiating the NormalCopy operation. The production site is the primary site at the time of NormalCopy operation. These values are listed in the **Configured** column.

The value listed in the **Current** column indicates the current value depending on the BCO execution. The current production site could be either primary or DR site depending on the business continuity operation. When NormalCopy is going on, the production site’s properties are displayed, as production site functions as the primary site.

Properties	Configured	Current
Production site	The name of the primary site. This is applicable to the AG.	The name of the current production site. It may be either primary site or DR site depending on the current BCM. This is applicable to the AG.
Production server	The name of the primary server.	The name of the current production server.
DR site	This gives the DR site name. This is applicable to the AG.	This gives the DR site name if applicable otherwise it’s shown as ‘Not Applicable’. This is applicable to the AG.
DR server	The name of the DR server.	This gives the DR site name if applicable otherwise it’s shown as ‘Not Applicable’.
BCMs	This lists the possible BCMs of the Group. This is applicable to the AG.	This shows the ongoing BCM. This is applicable to the AG.

Properties	Configured	Current
BCM State	Not Applicable.	This gives the current BCM state. For state details refer BCM configuration section under Group properties. This is applicable to the AG.
Current Group State	Current state of the group.	Current state of the group.
Current Continuity Status	Current continuity status of the group.	Current continuity status of the group.

Recent Continuity Operation: (displayed only at the FG level)

Continuity Operation	The name of the recent BCO executed.
Start time	Time stamp of recent BCO start.
End time	Time stamp of BCO completion.

To view the actions configured for the current continuity operation, click on Workflow Details link corresponding to the **Continuity Operation**.

Recent Continuity Operation: (only at AG level)

Continuity Operation	The name of the recent BCO executed.
Start time	Time stamp of recent BCO start.
End time	Time stamp of BCO completion.
Recovery Groups	This lists the RGs associated with the AG. Click on the RG link to view the Workflow details. This is specific to the AG and the following details are common between AG and RG.
Start Time	Displays the start time of the operation on that RG.
End Time	Displays the end time of the operation on that RG.

NormalCopy Operation Additional Details: The following information is common between the RG and the AG and it is specific to the DR Solution types. Refer to the 'NormalCopy' section under 'Business Continuity Operations Management' section in the respective reference guides.

The NormalCopy additional details are displayed separately for all the RGs associated to the AG on the NormalCopy execution window at AG level. For additional detail pertaining to NormalCopy, refer to the respective books under DR Solutions Supported by Kyndryl Resiliency Orchestration book in this Help.

Example: For Application SubSystem solution type, the following information is displayed under NormalCopy operation Additional Details table on the NormalCopy execution page.

Application Files Modification Timestamp	Displays the time and date when the application files got modified.
Last Replicated Application File Timestamp	Displays the timestamp of the last replicated Application file.

During the NormalCopy operation the difference in data is transferred to the DR site. In both these cases the current production site is primary and so the values in the configured property and current property are the same. BCM in the current property tables details the current operation, which is irrespective of production and DR site. BCM in the configured property table shows the possible BCM operation at the time of configuration.

For example: Assume that a disaster strikes at primary site, in this situation the remote site has to be brought up to function as a production site. During this operation the values of 'Configured Property' and 'Current Property' tables are different as the current production site is DR site, BCM is Failover and DR site values turns invalid as DR site does not exist during Failover operation.

Again during Fallback mode where the production starts functioning as primary, the values in both the tables are same.

When the NormalCopy operation is stopped in response to an event that occurs during data replication failure between production and the DR sites, then you can automatically resume NormalCopy through a configured policy.

To know about the event and policy refer to Managing Events section of 'Executing BCOs' chapter under DR Solution Supported by Kyndryl Resiliency Orchestration book in this Help.

You can set the frequency of dump and apply interval for NomalCopy at the time of NormalCopy operation configuration for database log and Application SubSystem solutions. Refer to the respective book under DR Solutions Supported by Kyndryl Resiliency Orchestration book in this Help for information on configuring the NormalCopy frequency.

RPO and the Dump/Apply Intervals

The Apply Interval is usually set to more than or equal to the Dump Interval. The RPO (Recovery Point Objective) should always be more than the greater of Dump and Apply Log Interval. For example, if the Dump Interval is 5 minutes and the Apply Interval is 10 minutes then, RPO should be 12 minutes or more.

Reverse Normal Copy

This operation is performed after performing the Switchover operation. The Reverse Copy operation is similar to the NormalCopy operation, but the replication happens from the current production server to the current DR server.

The Reverse Copy operation execution page is same as the NormalCopy operation execution page. To get information on the Reverse Copy operation page elements, refer to 'NormalCopy' in this section.

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To start Reverse Copy operation perform the steps provided in **Executing Business Continuity Operations** topic in this Help.

Fallback

During this operation a full dump of data from the current production server (DR server) is copied to the configured production server. Then the configured production server is brought back to production at the end of the Fallback operation.

At the end of the Fallback operation, the state of the DR database is dependent on the supported DR Solution type. In all DR Solutions, the production database is brought into production at the end of the Fallback operation.

In Application SubSystem and MSSQL solutions, the DR database is brought into the mounted state at the end of Fallback operation but in Sybase solution, the DR database is brought into standby mode in the beginning of the FallbackResync operation.

Note

All the RGs linked to an AG will be failed over or fallen back together always. Any failure in a RG is treated as a failure in all the RGs and the same continuity action is performed on all.

Refer to **Executing Business Continuity Operations** for information on initiating Fallback operation.

Failover

The Failover operation is initiated when the production server goes down. Failover can be initiated either manually or automatically. Failover is manually initiated by stopping the NormalCopy operation. It is automatically initiated when events are configured to start this operation on occurrence of disaster. Based on the severity level of the occurred Events, the corresponding configured policy set will initiate Failover operation.

For example, if the production database is down, an event will be raised. This event will stop the ongoing NormalCopy and will initiate the Failover operation.

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

The execution status of the Failover operation cannot be seen as the operation automatically triggered due to server down condition. During the server down condition agents will not be able to connect to the server, and hence the execution status of the Failover operation cannot be shown. Refer to **Executing Business Continuity Operations** to know how to initiate Failover operation.

Failover operation can be performed only during certain situations after the sites are switched over. Kyndryl Resiliency Orchestration server is always placed in the configured site i.e. DR site. After Switchover is performed, the configured DR becomes the production server. So, the Kyndryl Resiliency Orchestration server is said to be placed at the production site after Switchover.

This setup (Switchover) supports Failover for the following conditions:

- Database down
- Database server down

This setup (Switchover) cannot support Failover for the following conditions:

- Site Collapse

Kyndryl Resiliency Orchestration supports automatic failure when the events are configured to initiate the Failover automatically on a failure or disaster. Otherwise, the Failover operation is initiated manually.

For execution part of this operation based on the DR Solution type, refer to the respective DR Solution reference guide.

When Failover is initiated at AG level, then this operation is executed on all RGs associated to the AG. All the RGs will be failed over together always. Any failure in a RG is treated as a failure in all the RGs and the same continuity action is performed on all.

During Failover the DR server is brought into production. When the Failover operation is executed on the Group, the 'Additional Details' section in the NormalCopy page that displays the log file details cannot be seen as the Failover operation is automatically triggered due to server down condition. During the server down condition, agents will not be able to connect to the server, and hence, the execution status of the Failover operation will not be shown.

Once Failover operation is complete, follow the path **Manage > Recovery Groups > Group Name > RG Details** page to initiate the next operation or refresh the page to initiate next operation.

The Failover time of the AG is calculated as sum of recovery time of all RGs associated to the AG.

FallbackResync

This operation is initiated to bring the DR database and the production database in sync.

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To start the FallbackResync operation perform the steps provided in **Executing Business Continuity Operations** topic in this Help. This operation has to be started from the AG level **Groups** page.

An Example to have a Clear Understanding of all Five BCOs

Assume that, the production site is at Bangalore and the DR site is at Mumbai.

During NormalFullCopy the full dump is manually transferred from Bangalore server to the Mumbai server. This operation synchronizes the data on the two servers.

During NormalCopy operation only incremental data is transferred to the Mumbai server.

Assume that a disaster strikes the production site (Bangalore) 10.A.M 10-10-2005. The Failover operation transfers the business to the DR server and it starts functioning as the current production server.

Assume that the collapsed site comes back online at 2 P.M the same day. In the Fallback operation the full dump from the Mumbai (current production) server is copied to the Bangalore server (current DR). This operation may take some amount of time (say 4 hours), during which some more transactions may happen in the current production site. This additional data is also copied at the end of the Fallback operation and the Bangalore server is brought into production.

During FallbackResync operation, the two servers are brought into sync and are made ready for the NormalCopy operation.

Executing Business Continuity Operations

You can enable continuity operations on a group and manage its state details by clicking **Manage** tab on the navigation bar. During execution of the BCO, the actions configured for that BCO is executed in the order of configuration.

You can stop Kyndryl Resiliency Orchestration services at any time during the execution of BCO.

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To execute NormalFullCopy, NormalCopy, or Reverse NormalCopy :

1. Click Manage > Recovery Groups > RG listing page is displayed. This page lists all Groups assigned to the current user.
2. Click a group from the **Recovery Groups** column. Click View All Workflows.
3. The BCO workflows are displayed.

Note

Only Super Administrator can start/stop BCOs for Groups of other users. The users with Administrator privileges can start BCOs for Groups assigned to them but cannot stop BCOs initiated by other users for the same Groups.

4. Click the respective BCO to initiate the operation.

   The following are the BCOs displayed:

   - NormalFullCopy
   - NormalCopy
   - ReverseNormalCopy

   Refer to Business Continuity Operations for more information.
5. Click Execute, a confirmation pop-up is displayed with Execute and Cancel.
6. Click Execute to confirm the execution. Click Cancel to cancel the execution.

To execute Failover, Fallback, or FallbackResync :

1. Click Manage > Recovery Groups > RG listing page is displayed. This page lists all Groups assigned to the current user.

2. Click a group from the **Recovery Groups** column. Click View All Workflows.
3. Click the **Recovery Workflows** tab to proceed with the continuity operations execution.

   Note

   Only Super Administrator can start/stop BCOs for Groups of other users. The users with Administrator privileges can start BCOs for Groups assigned to them but cannot stop BCOs initiated by other users for the same Groups.
4. Click the respective BCO to initiate the operation.

   The following are the BCOs displayed:

   - Failover
   - Fallback
   - FallbackResync

   Refer to Business Continuity Operations for more information.
5. Click Execute, a confirmation pop-up is displayed with Execute and Cancel.
6. Click Execute to confirm the execution. Click Cancel to cancel the execution.

On the **Manage** page, click the respective RG link under **Recovery Groups** to view the list of actions executed on the RG along with the notification information. You can manage the action being executed and choose to terminate a particular action from the **Recovery** page.

Failover on any one of the RGs that are linked to an AG is defined as 'Any BCO on one is BCO on all' i.e. if Failover is triggered on any one of the RG will trigger Failover on the AG to which the RG is associated.

Note:

All RGs linked to an AG will be failed over or fallen back together always. Any failure in a RG is treated as a failure in all the RGs and the same continuity operation is performed on all RGs belonging to that AG.

Caution

Usage of the Failover operation may significantly impact the continuity management of the Group, if not performed correctly.

Start and Stop Replication

The Replication Management allows protection parameter configuration, execution and displays the health of replication activity. The replication mechanism is applicable only in Normal mode. The Normal mode operation periodically obtains the protection details and stores them. The Replication Management allows parallel protection management operation on multiple Groups at the same time. You can implement the configuration of protection parameters, based on the privilege specification.

As part of the replication management, Kyndryl Resiliency Orchestration provides the following key capabilities for each database under protection:

- Health of the log replication activity

- Individual database level control

The above management capability is provided at each database level for higher flexibility and decentralized management control.

The Replication Management is enabled only after the Group creation. The replication status of the Application Group can be Active, Inactive, or Degraded based on the status of the Recovery Group attached to it. The data replication occurs at the Recovery Group level only. The replication failures are reported at Recovery Group level, but elevated to Application Group level.

Click **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

Perform the following steps to initiate replication:

1. Click Manage > Recovery Groups on the navigation bar. The Recovery Groups List page appears.
2. Click the desired Group from the **Recovery Groups** column and click Pending Data tab.
3. This page displays the replication details and you can monitor the health of the data replication that is going on. You can perform the following operations on the Group:

- Click **Stop Replication** to stop the replication after initiating the NormalCopy operation.
- Click **Start Replication** to start replication to resume the operation after a halt.
- Click **Refresh Details** to get latest replication details.

Note:

You can also Refresh Details by performing the following steps.

1. Click **Monitor** > **Recovery Groups** on the navigation bar. The **Recovery Groups List** page appears.
2. Click the desired Group from the **Recovery Groups** column and click Pending Data tab.
3. Click **Refresh Details** to get latest replication details.

The information displayed in this page varies with the DR Solution type supported.

The replication properties depend on the BCO. The following topics explain about the replication status during various BCO at Recovery Group and Application Group level.

NormalFullCopy

The following details are displayed on the Recovery Group details > Replication tab.

Field	Description
Replication Status	Active
Last Successful Replication Time	Not Applicable
Last Failed Replication Time	Displays the time of the replication that had failed.
Last Replicated Data size	Displays the size of the data replicated. The data size is zero in case of replication failure or shows the replicated file size in case of successful replication. In case of successful replication the value of Last replicated Data size increases as and when the additional data is copied from the Production to DR server.

NormalCopy and Reverse NormalCopy

The following details are displayed on the Recovery Group details > Pending Data tab.

Field	Description
Fileset Name	Displays the name of the Fileset being replicated.
Protection Mechanism	Displays the protection mechanism used for replicating the Fileset.
Replication Status	Displays the replication status.
Last Successful Replication Time	Displays a time stamp of the last successful replication.
Last Failed Replication Time	The value of this field is displayed only when failure had occurred during last replication.

Note

In the **Normal Copy** operation, if you click **STOP** button to abort the replication, the PFR will not stop immediately. It will complete the file replication in progress and will stop replicating further files. As a result, it may take few minutes to stop the replication from Primary to DR.

On Kyndryl Resiliency Orchestration Server restart, the continuing NormalCopy may not resume again. To start it, refer Resuming NormalCopy on Server Restart for details.

Note

The properties of the **Replication Management** page during Reverse NormalCopy operation (that is initiated after Switchover) remains the same as the NormalCopy operation.

For example, Assume that the time of last replication is 10 a.m. and the amount of data transferred is 4 MB. After replication has happened, consider 2 MB data has been written onto Production and it will take one hour to copy data to the DR site. After the difference in data has been copied to the remote site, the time of last replication would be 11 a.m. and the last replicated data size would be 6 MB. In case of replication failure during this operation, the last successful replication time would remain as 10 a.m. and the replicated data size would be 4 MB and the last failed replicated time would be the exact failure time (i.e. any time between 10 and 11 a.m.).

Switchover, Switchback, Failover, Fallback and FallbackResync

Data replication does not happen during Switchover, Switchback, Failover, Fallback and FallbackResync operation and the non-availability of data is represented as hyphen (’-‘) in the respective field.

The following details are displayed in the Replication tab at Application Group level:

Field	Description
General	Displays Production and DR site names.
Replication Status	This gives the current status of data replication. The various status of data replication are:

Managing Events

Events are failure or input required conditions in the DR environment. They are classified into different severity levels based on the impact they cause to the DR systems.

Different severity types are:

🔴- Critical

🟠- Serious

🟡- Warning

🔵- Info

Event would mean the highest threat level. The impact of an event on different applications means different availability and management actions. The severity level, Events are displayed when production data is down or database server is down. Kyndryl Resiliency Orchestration automates the management and execution of the policies associated with each Event with optimal user intervention. It provides the capability to customize policies associated with an Event condition to suit the needs of the customer environment. Kyndryl Resiliency Orchestration provides following key Event Management capabilities for each Dataset under protection:

1. Identification of events that can impact the production data availability and display the event details with the associated components that got affected.
2. All the events related to database, servers (primary and remote) will be considered.
3. Provide alerts and notifications to configured users. E-mail and SMS notifications will be sent to group of users, associated with a database (application).
4. Customized policy configuration for each Event to suit the customer environment.
5. Automated triggers to initiate the pre-configured policies, in response to the failure condition.

To see all occurred events for a specific group take the following steps.

1. Click **Discover** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click the required group from the **GROUP NAME** column to configure the workflow. The **Group Details** Page appears.
4. Click Group Configuration> Events.

The Events tab displays the following details of Events/ events that occurred with Kyndryl Resiliency Orchestration.

- Event ID
- Event Description
- EVENT Severity
- EVENT IMPACT
- Notify

When event is raised, it does the following:

- Interacts with users to notify respective users about the event.
- Alerts to send notification list.
- Enables Continuity Manager to perform continuity actions such as Failover, Fallback etc.
- Enables RPO/ RTO Manager to report all events that have an impact on RPO and RTO, etc.

An event may be associated to a policy. A policy is a series of actions (operations) that are executed in a certain sequence based on configuration parameters. These are primarily defined to contain the impact caused by the event.

Managing Events through Event Correlation

Event Correlation helps manage the polar events. Polar Events can be explained by an example. A network down event and a network up event are polar to each other. If the network down event is followed by a network up event, then the network down event must be canceled according to Event Correlation.

Event Correlation performs the following:

- It cancels out polar events for all severity of events. However, the events that are in EXECUTING or AWAITING INPUTS states are not cancelled though, their polar events are raised. For example, if a network down is followed by a network up event, then Event Correlation closes the network down event. This allows you to focus on events that need your attention.
- It executes a policy in response to an event. Start of policy execution retires the events that were polar to the event that started the policy execution. Policy execution can be automatic or manual. It does not retire those events that are not related to root cause of same failure. The events that are in EXECUTING or AWAITING INPUTS states are not cancelled.

The polar events must be defined in an XML file to be used by the Kyndryl Resiliency Orchestration. At the time of installation, Kyndryl Resiliency Orchestration deploys such XML files for the solutions it supports. You may wish to edit these files to customize them to your needs. However, you must restart the server after editing the XML file. Following Table gives the names of the files that are deployed for the supported solutions.

Kyndryl Resiliency Orchestration Supported DR Solutions	Event Correlation XML Filename
MS SQL with PFR	BCS-MSSQL-Logs-with-Panaces-File-Replicator-aec-rules.xml
Sybase with PFR	BCS-SybaseLogPFR-aec-rules.xml
Sybase ASE with SRS	BCS-SybaseSRS-aec-rules.xml
Application Subsystem with PFR	BCS-ApplicationSubSystem-with-Panaces-File-Replicator-aec-rules.xml

The naming convention for the XML files is BCS-<BCSType>-aec-rules.xml. These files must be placed under $EAMSROOT/installconfig/rules folder on Kyndryl Resiliency Orchestration Server.

Following Table gives the information about the XML tags that are used to define Event Correlation rules:

Note

In XML, a tag with '/' indicates the end of that tag. For example, a tag </Rule> indicates the end of the tag <Rule> used to define an Event Correlation rule.

Tag	Description
<EventCorrelationRuleList>	This tag indicates the start of the Event Correlation rules list.
<Rule>	This tag indicates the start of definition of an Event Correlation rule.
<RuleType>	This tag is used to specify the rule name you are going to define.

Tag	Description
<InputEvent>	This is used to specify the Event name that triggers the Event Correlation mechanism.
<PolarEvents>	This tag indicates the start of the list of polar Events that are associated with <InputEvent>.
<PolarEvent>	This tag specifies the name of the polar Event.

You may wish to do away with Event Correlation completely or partially. To disable Event Correlation completely, you can do one of the following:

- Delete the XML file
- Take the back-up of the file in some other directory and remove it from the current location or
- Delete the values specified for each tag.

To partially disable the unwanted rules in the XML file, do one of the following:

- Delete Rule
- Comment the rule tags
- Delete the tag values

List of Events based on severity can be classified as

Severity	Events
Critical	▪ DR Related failure events like ○ Replication failure for long time ○ Server/App/DB down ▪ InfraFailures like ○ Invalid credentials ○ Remote server access failures ○ Vault related failures
Serious	▪ SLA deviations like ○ RPO deviation ○ RTO deviation ○ Datalag deviation ▪ Failures like ○ Replication stopped/paused ○ Process down ○ App/DB specific or state related events1

Severity	Events
Warning	▪ Kyndryl internal events o Unable to compute RPO o Agents down o Network down2
Info	▪ All happy events ▪ Workflow user-input events3

Event Status

The interaction of Event Manager with others depends on the event status. The following table lists possible status of an event:

Event Status	Description
Open	The status of an event is 'Open' only when the event is raised.
Notified	An event for which notifications are sent to the corresponding users through notification list. For further details on notification list refer to Alerts topic.
Executing	An event status is said to be 'Executing' only when a policy set for that event is under execution. Some events may not have a policy set. In this case, this status is not applicable for that particular event.
Awaiting input	The status change happens when the policy under execution requires user input. Again this status is applicable for those events, which have a policy associated to it.
Success	An event status is successful when the policy under execution is successfully executed.
Failed	An Event status is said to be 'Failed', when the policy under execution has failed.
Closed	This state is manually set by the user when the associated problems are solved. But an event can be closed manually irrespective of the event status. At any given point, only one instance of an event can be in open state and all other will be cancelled.

Event status is automatically updated by Kyndryl Resiliency Orchestration in response to the occurrence of above conditions.

Synchronizing Date and Time between Kyndryl Resiliency Orchestration Server and Client Machines

To adjust the Date and Time on client machines, perform the following steps:

1. Stop all Business Continuity Operations (BCO) including NormalCopy operation on the Group(s) to which the machine belongs.
2. Move these Groups to Maintenance mode on Kyndryl Resiliency Orchestration Server.
3. Stop all agents on the machine.
4. Adjust the date/ time to be as close as possible to Kyndryl Resiliency Orchestration Server system time.
5. Restart all agents.
6. Restore Groups to Managed state.
7. Resume BCO operations on the Group(s).

To adjust Date and Time on Kyndryl Resiliency Orchestration Server, perform the following steps:

1. Stop all Business Continuity Operations (BCO) including NormalCopy operation on all the Group(s).
2. Stop Kyndryl Resiliency Orchestration Server.
3. Adjust the date/ time to clock time.
4. Restart Kyndryl Resiliency Orchestration Server.
5. Resume BCO operations on all the Group(s).

Drills

Majority of the DR solutions fail at the time of disaster even with huge infrastructure installation. This is either because there is no DR test plan in place or because the plan is too complex or expensive to execute. Test Exercise provides complete management control for performing DR test exercises and rehearsals. It provides wizard based control to handle the exercises in an automated and reliable way.

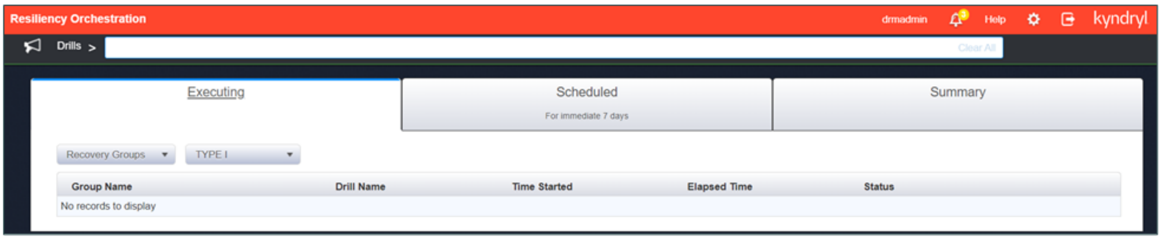
Kyndryl Resiliency Orchestration provides automated test exercise management for key intrusive and non-intrusive tests. It provides following important capabilities:

- Individual FileSystem level test exercise execution and monitoring the status of the same
- Automated execution of tests with wizard control for user intervention where desired
- Intrusive test support – provides ‘Failover of the FileSystem’ test

- Non-intrusive test support – provides 'DR FileSystem consistency and integrity' test

Each drill is pre-configured with a workflow to do the actual test and each of the exercise is customized according to your environment.

You have to execute the drills manually. Kyndryl Resiliency Orchestration supports executing multiple Drills in parallel. When Drills are being executed, allowing continuity operations depends on the mode of the Drills you are executing. However, Drills are not allowed, if the intended Group is under Unmanaged or Maintenance mode.



Group Name	Drill Name	Time Started	Elapsed Time	Status
No records to display				

The drills undergo different status during its life cycle. The possible values of status are given in the following table:

Status	Description	Next Possible Status
NEVER EXECUTED	The drills has never been executed so far.	START TEST
EXECUTING	The drill is currently running.	EXECUTING
SUCCESS	The execution process has been successfully executed.	NO OPERATION
FAILED	The execution process has been failed.	STOP TEST/EXECUTING
AWAITING INPUT	The process is executing but requires user input. In this case, there will be an action handler pop-up window requesting user input.	NO OPERATION
STOPPING	This is an intermediate state indicating the drills in stopping. It goes in to this state when it is been manually triggered.	NO OPERATION
SHUTDOWN	This occurs when Kyndryl Resiliency Orchestration software	NO OPERATION

Status	Description	Next Possible Status
	or hardware fails or abnormal crash occurs.	

The life cycle of the drills goes through seven processes. The initial state of the drills is always NEVER EXECUTED.

Configuring Drills

Drills can be executed in any continuity state of a Group. It can be executed, while a Business Continuity Operation (BCO) is running. If a drill interferes with a BCO, it can impact the State of the System, BCOs, Group and Continuity health, and may cause an Event.

Multiple drills can be run on Recovery Group simultaneously except for Switchover/Switchback. However only one drill at a time can be executed on an application Group.

During drill execution, the Group image will change to indicate that a drill is in progress for that Group.

Go to ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

To configure Drills, perform following steps:

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click the Recovery Group tab, the Recovery Group Listing page appears.
3. Click the required group from the **GROUP NAME** column. The **Group Details** Page appears.
4. Click the Group Configuration tab.
5. Click the **Drills** tab.

Switchover

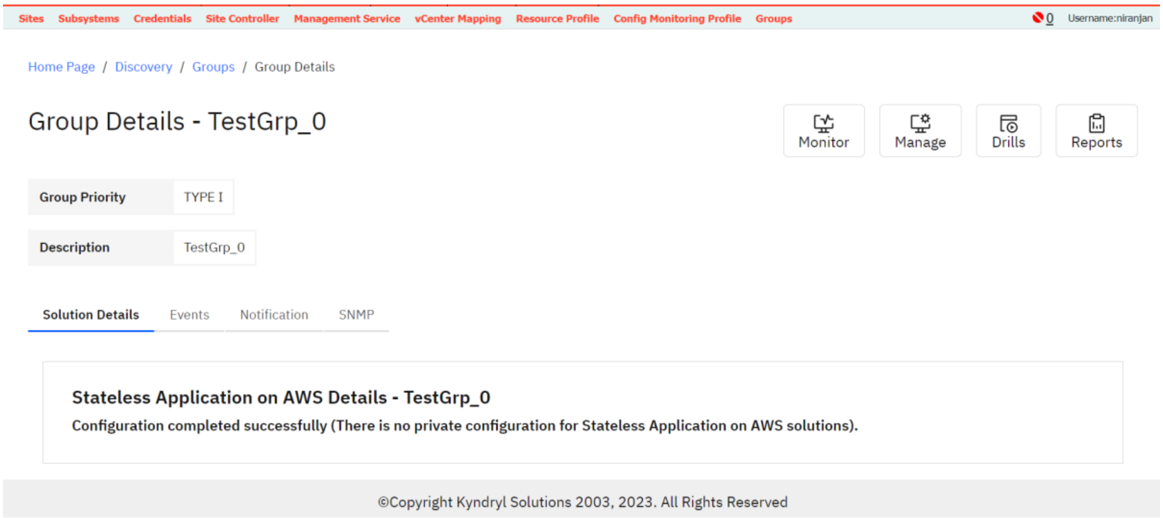
The Switchover operation is performed to run the business from the DR site, i.e. the remote server is made to function as primary (production) server and the primary is made to function as remote server for a desired amount of time.

The Switchover operation can be executed after NormalFullCopy operation or by manually stopping the NormalCopy. To manually stop the NormalCopy operation click **Stop NormalCopy** button on the **NormalCopy operation execution** page.

To configure switchover follow the path:

Go to **Drills > Summary > Group Name**.

The **Drill Listing** page is displayed.



Group Details - TestGrp_0

Group Priority	TYPE I
Description	TestGrp_0

Stateless Application on AWS Details - TestGrp_0

Configuration completed successfully (There is no private configuration for Stateless Application on AWS solutions).

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

Click **Switchover.**

Caution:

Disable the 'Auto-Failover' policy before initiating Switchover operation. To disable the auto-failover policy, refer to the respective DR Solution book under *DR Solutions Supported by Kyndryl Resiliency Orchestration*.

During Switchover the BCM state is Switchover Transit.

The window elements after the Switchover has happened are same as the NormalCopy Inactive BCM state except for a few things.

During Switchover Inactive state (i.e. after Switchover is complete) the Configured properties and the Current properties differ i.e. the properties are interchanged.

For example consider the following configured properties:

Production Site: Mumbai

Production Server: Windows 1

DR Site: Bangalore

Production Server: Windows 2

After Switchover operation, the following information is displayed in Current Properties section.

Production Site: Bangalore

Production Server: Windows 2

DR Site: Mumbai

Production Server: Windows 1.

If the operation fails during Switchover Transit, then BCM state moves to Switchover Inactive.

Note

For Switchover, auto-failover policies need to be manually switched to manual for RG's that are part of an AG.

Switchback

This operation brings the configured primary server to production and configured DR server to function as remote (standby) server. This setup is same as the NormalCopy operation. Once the Switchback operation is performed, the NormalCopy is started on the Group.

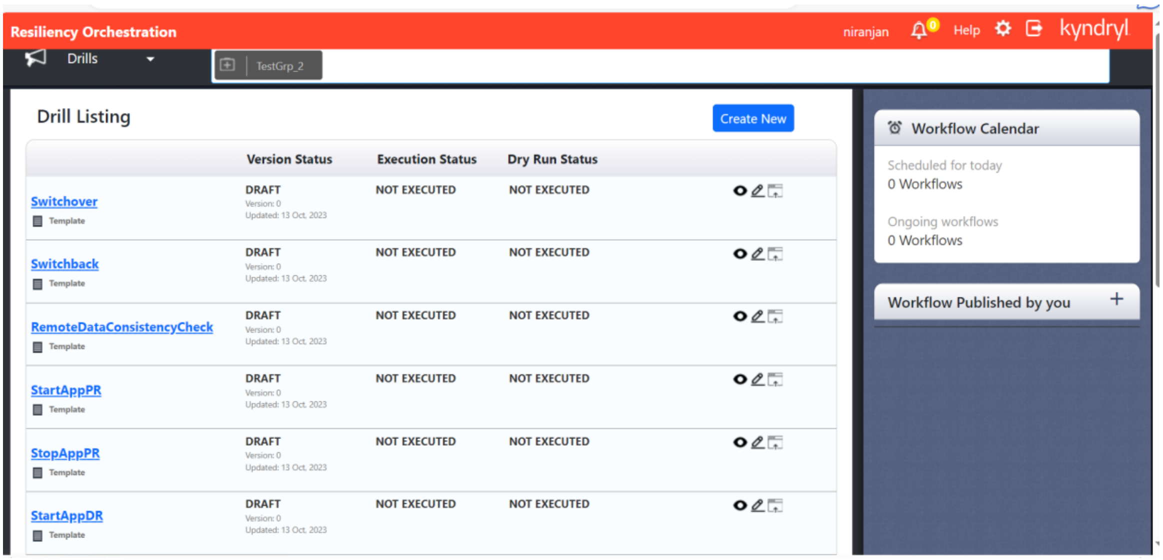
To start the Switchback operation perform the steps provided in Executing Drills topic in this Help.

To configure switchback follow the path:

Go to **Drills > Summary > Group Name**.

The **Drill Listing** page is displayed

Click **Switchback.**



Drill Listing

	Version Status	Execution Status	Dry Run Status
Switchover Template	DRAFT Version: 0 Updated: 13 Oct, 2023	NOT EXECUTED	NOT EXECUTED
Switchback Template	DRAFT Version: 0 Updated: 13 Oct, 2023	NOT EXECUTED	NOT EXECUTED
RemoteDataConsistencyCheck Template	DRAFT Version: 0 Updated: 13 Oct, 2023	NOT EXECUTED	NOT EXECUTED
StartAppPR Template	DRAFT Version: 0 Updated: 13 Oct, 2023	NOT EXECUTED	NOT EXECUTED
StopAppPR Template	DRAFT Version: 0 Updated: 13 Oct, 2023	NOT EXECUTED	NOT EXECUTED
StartAppDR Template	DRAFT Version: 0 Updated: 13 Oct, 2023	NOT EXECUTED	NOT EXECUTED

Scheduled for today
0 Workflows

Ongoing workflows
0 Workflows

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

Note

For Switchback, auto-failover policies need to be manually switched to manual for RG's that are part of an AG.

Custom Drills

Customized drills can be added into or removed from Kyndryl Resiliency Orchestration dynamically. These drills can be created while creating a workflow. Such drills can be added from Drills Dashboard page of a Recovery Group and Application Group. Various actions can be imported into the customized test exercise using XML file import. However, conventional method of configuring Drills by adding an action and configuring it can also be followed.

To configure the Custom drills follow the path:

1. Click **Drills** on the navigation bar and click the **Summary** tab**.**
2. Click the desired Group Name. The **Drill Listing** page is displayed.
3. Click the custom drill.

Adding Drills

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

To add a Drill:

*1 Click **Drills** on the navigation bar and click the **Summary** tab.*
*2 **Click the desired Group Name. The Drill Listing page is displayed.***
Or
*Click **Discover>Groups** on the navigation bar. Click **Recovery Group** tab and the Recovery Group listing page appears. Click the desired group name from the **Group Name** column. The **Group Details** Page appears. Click **Drills** on the sub navigation bar. The **Drills Listing** Page is displayed.*
*3 Click **Create New** on the top right side of the page**.***
*4 Enter Workflow Name in the text box and select **Drill** from the **select Category** drop down list.*
*5 Click **Create New.***

Removing Drills

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

.

Only customized test exercises can be deleted.

1 *Click* ***Drills*** *on the navigation bar and click the* ***Summary*** *tab.*

2 ***Click the desired Group Name. The Drill Listing page is displayed.***

Or

Click ***Discover>Groups*** *on the navigation bar. Click* ***Recovery Group*** *tab and the Recovery Group listing page appears. Click the desired group name from the* ***Group Name*** *column. The* ***Group Details*** *Page appears. Click* ***Drills*** *on the sub navigation bar. The* ***Drills Listing*** *Page is displayed.*

3 *Click* 🗑 *corresponding to the customized drill to be deleted. A confirmation pop up appears. Click* ***Delete.***

Configuring Drills

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

1 *Click* ***Drills*** *on the navigation bar and click the* ***Summary*** *tab.*

2 ***Click the desired Group Name. The Drill Listing page is displayed.***

Or

Click ***Discover>Groups*** *on the navigation bar. Click* ***Recovery Group*** *tab and the Recovery Group listing page appears. Click the desired group name from the* ***Group Name*** *column. The* ***Group Details*** *Page appears. Click* ***Drills*** *on the sub navigation bar. The* ***Drills Listing*** *Page is displayed.*

3 *Click on the* ***Edit*** *button against the desired test exercise you want to configure. The* ***Edit Workflow*** *page appears.*

4 *You can configure the drill either by adding actions one by one or by importing a XML file containing workflow of the exercise.*

IntegrityCheck Test Place holder

Integrity Check is a default drill which is applicable for all the DR solutions. When an RG is created, by default IntegrityCheck drill will be displayed on GUI in the below two places:

To configure the Integrity Check follow the path:

Go to **Drills > Summary > Group Name**.

The **Drill Listing** page is displayed

Click **Integrity Check.**

or

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group Listing page appears.
3. Click the required group from the GROUP NAME column. The **Group Details** Page appears.
4. Click Group Configuration > Drills

IntegrityCheck drills cannot be deleted and this comes with “custom” action configuration.

Note:

The report will be enabled only if the Banking Module is licensed.

Listing Drill Schedules

To list the schedule of all the drills configured for a Recovery Group, perform the steps given below:

1. On the Navigation bar, click **Drills**> **Summary**.
2. Click on the **Group name.**
3. The **Workflow Calendar** at the right displays the scheduled and ongoing workflows.
4. On clicking the Workflow Calendar, a table is displayed with the information on Workflow, Group, Date Recurrence and Approvers.

Executing Drills

Each Drill is pre-configured with a workflow to do the actual drill and each of the exercise is customized according to your environment.

You have to manually execute the Drill. Kyndryl Resiliency Orchestration supports executing multiple Drills in parallel. When Drills are being executed, then no continuity operations are allowed and vice-versa.

In the other continuity modes, even if the Drill is initiated, it fails. When a Drill is initiated on an AG, the Group continuity mode is changed to MANAGED_TEST. The drills performed at AG level executes each drill at RG level and the result is elevated to the AG. Common drills must be done sequentially in an order.

If an AG contains any RGs in parallel relationship then the Drill will be done serially. As a result, Drills will ensure the orderly dependency among RGs. If there are any parallel RG's, they would not be resolved simultaneously. Instead they will be taken up one after the other. A Group cannot move into MAINTENANCE mode when in MANAGED_TEST. During Drill, Change State is not allowed and during metadata crash-recovery, MANAGED_TEST should not be allowed.

The Drills undergoes different status during its life cycle. The possible values of status are given in the following table:

Status	Description	Next Possible Status
NEVER EXECUTED	The Test Exercise has never been executed so far.	START TEST
EXECUTING	The Test Exercise is currently running.	EXECUTING
IDLE	The Test Exercise has been successfully executed.	STOP TEST
FAILED	The execution process has been failed.	STOP TEST/EXECUTING
AWAITING INPUT	The process is executing but requires user input. In this case, there will be an action handler pop-up window requesting user input.	NO OPERATION
STOPPING	This is an intermediate state indicating the Test Exercise in stopping. It goes in to this state when it is been manually triggered.	NO OPERATION
SHUTDOWN	This occurs when Kyndryl Resiliency Orchestration software or hardware fails or abnormal crash occurs.	NO OPERATION, RESUME TEST

Life cycle of a Drill goes through seven processes. The initial state of the Drill is always NEVER EXECUTED.

The list below explains the next possible state after each state.

- ***Start Now***

  This operation initiates any test by triggering the associated workflow execution. To start a test on the FG no BCO should be executing on the Group. Upon successful initiation the status of the test is changed to EXECUTING. After successful execution of test, the status is changed to success. In case of failure, the status is changed to Failed. The events that require input from you to proceed are listed in the Events list page. In this page, select the ***Requires Action*** *check box to display only those events that require your input. In case of system crash or Kyndryl Resiliency Orchestration software crash the Test Exercise state is changed to shutdown.*
- ***Stop Drills***

  This operation stops the test in progress. Whenever a test is stopped, it is always considered as aborted. When the test is stopped, the status is changed to FAIL.

Note

If you stop the Test Exercise then a message box is displayed confirming if you want to stop it or not.

- ***Resume Drills***

  This operation resumes the test from the last executed action. As of now, it always executes the workflow from the beginning.

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

The Drills can be executed by performing the following steps:

1. Click **Drill>** on the navigation bar. The **Drill** page appears.
2. Click **Executing** tab. All the active groups are displayed.
3. Click desired Group from the **GROUP NAME** column for which you want to execute the drills. The **Drill Listing** page appears. This page provides the following information:
   - Drill Summary: This provides the summary of the drills as given below:
   - **Total Tests Run** - Displays total number of drills that were run for the group.
   - **Tests Successful** - Displays total number of drills that were successfully run for the group.
   - **Tests Failed** - Displays total number of drills that were failed and not successfully completed the execution.
   - Next Scheduled- Schedule the execution for a later time.

   List of Groups with the following information:
   - DRILL NAME - List of configured drills for the Group
   - STATUS - Displays the status of the drill.
   - LAST INITIATED - Displays the last execution time of the respective drills.
   - ACTION - Displays option to Start or Stop or Resume the drills execution.
4. Click the **Start Test** link in the **ACTION** column to initiate the corresponding test exercise of the respective group. You can configure the test exercise by clicking **Configure** link in the **Action** column.
5. Click ☰ icon of the respective Group to view the workflow details of the drill.
6. Click **Back to Details** to go back to the **Drills** page.

Drills State

Based on the current state of the Group, Drills such as 'Initiate Switchover', 'Initiate Switchback' etc are possible. These operations are listed as selectable buttons. The complete list of operations is as given below:

Initiate Switchover	This operation initiates Switchover operation on production and DR site. On completing the Switchover operation, the DR site becomes production and production site becomes DR site.
Initiate Switchback	This operation switches back the DR site to production and the production site to DR after the Switchover operation.

Note:

In generic solutions, Kyndryl Resiliency Orchestration provides facility to customize drills as per your needs. In case of failure of an action, click **Continue** in the **Workflow Manager** page to skip the failed action and to move to the next.

The following table lists the next possible operation based on the current state of operation.

State	Next Operation
Normal Reset	Initiate NormalFullCopy, Change Continuity State, Move to Maintenance
Normal Inactive	Initiate NormalCopy, Initiate Failover, Change Continuity State, Initiate Switchover, Move to Maintenance
Normal Transit	-
Normal Active	Stop NormalCopy
Normal Failed	Initiate NormalCopy, Initiate Failover, Change Continuity State, Initiate Switchover, Move to Maintenance
Normal Degraded	Stop NormalCopy
Switchover Inactive	Change Continuity State, Initiate Reverse Copy, Initiate Failover, Initiate Switchback, Move to Maintenance.
Switchover Transit	-
Switchover Active	Stop Reverse Copy.

State	Next Operation
Switchover Failed	Initiate NormalCopy, Initiate Switchover, Initiate Failover, Change Continuity State
Failover Transit	-
Failover Failed	Initiate Failover, Initiate NormalCopy, Change Continuity State, Move to Maintenance
Failover Active	Initiate Fallback, Change Continuity State, Move to Maintenance
Fallback Transit	-
Fallback Failed	Initiate Fallback, Change Continuity State, Move to Maintenance
Fallback Active	Initiate FallbackResync, Change Continuity State, Move to Maintenance
Normal Shutdown	Resume Continuity operation, Change Continuity State, Move to Maintenance
Normal Stopping	-
Normal Test	Initiate NormalCopy, Initiate Failover, Change Continuity State, Initiate Switchover, Move to Maintenance (Do not perform any BCO when the test exercise are being performed on the Group)

The following table technically explains the drills and the state of production and DR server. It is applicable only for DR Solutions based on Sybase and MSSQL databases.

BCO	Functionality	Production Server’s mode of operation	DR Server’s mode of operation
Switchover (Not supported for DR Solutions based on MSSQL and Sybase databases)	Configured production server is made as DR and vice-versa	NA	NA
Switchback (Not supported for DR Solutions based on MSSQL and Sybase databases)	Reverse of Switchover operation	NA	NA

Drill Listing

The Drill Listing page displays the following draft workflows. The user can also create New Workflows.

The following are the twelve Draft workflows the user can select, namely

- Switchover
- Switchback
- Failover Exercise
- Remote Data Consistency
- StartAppPR
- StopAppPR
- RoleSwitchtoPR
- RoleswitchtoDR
- Recovery
- IntegrityCheck

Click on **Edit** ✎ to edit the workflow

Click on **View** 👁 to view the workflow.

Tracking Drills

You can track the Group on which Drill is running under Restricted or Unrestricted mode. There are three following ways to track such Groups:

1. From the Drills Listing page
2. From the Drills Summary tab page

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

To track the Group for a Drill from Drill Listing page, follow the steps given below:

3. In the navigation bar, click **Drill> Executing**.
4. In the **Drills** page, check the **In Progress** column against the desired Group. It shows the number of drills being run on that Group.

To track the group for a Drill from Summary tab page, follow the steps given below:

1. In the navigation bar, click **Drill> Summary**.

2. In the **Summary** page, check the WORKFLOW TYPE, CURRENT WORKFLOW, and WORKFLOW STATUS columns for the desired Group. They give information of whether or not a drills type of WORKFLOW TYPE is being executed on the Group, its name and its execution status.

Changing Drills Mode

You can change the default Unrestricted mode of a drills to Restricted. To do this, you need to edit a parameter value in the *panaces.properties* file.

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

Follow the steps given below to change the mode:

1. On the Kyndryl Resiliency Orchestration Server, go to the $EAMSROOT/installconfig directory.
2. Open panaces.properties file.
3. Edit the value of *panaces.testExerciseMode* parameter. The value of 0 indicates Restricted mode and 1 indicates the Unrestricted mode.

Drills Interfering with BCO

While Restricted mode does not allow executing Drills along with any BCO, Unrestricted mode does.

However, caution must be taken while configuring and executing a drill so as not to interfere with the running BCO. If an Unrestricted Drill interferes with a BCO, it can impact the State of the System, the BCO, Group and Continuity health, and may cause an Event.

A Failover drill being executed at the time of Normal Copy operation is the simplest example of a drill interfering with a BCO. Such execution can cause the Normal Copy to fail.

Identifying Group under Unrestricted Test Mode

Unrestricted Test Exercise (UTE) allows you to execute a drill in any continuity state of a Group. It can be run while a Business Continuity Operation (BCO) is running. When a UTE is running for a Group, it does not put under TEST mode. As a result, the Group health is not changed. During UTE, the Group image does not change to indicate that an Unrestricted Test Exercise is in progress for that Group. This makes it difficult to identify the Group on which UTE is being run.

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

Follow the steps given below to identify such Groups:

1. Click **Monitor** or **Manage** on the navigation bar.
2. Click Executing Workflow.
3. In the **Recovery Group Listing** window, check WORKFLOW TYPE, WORKFLOW DETAILS, and STATUS columns for the desired Group.

A Group with a UTE running on it will have WORKFLOW TYPE as Test Exercise, WORKFLOW DETAILS will display the details of the workflow being executed, and STATUS column will show the execution of the workflow of the Drills.

Effect of Drills on Group Status

In Kyndryl Resiliency Orchestration, the Group mode changes are based on the mode of Drills being run on it. If Restricted mode of Drills is running on a Group, the Group is put under MANAGED_TEST mode. However, if Unrestricted mode of Drills is running on a Group, the Group mode does not change. This makes it difficult to identify the Group on which Unrestricted Test Exercise (UTE) is being run.

Viewing Drills for a Group

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

This page will list all the Drills configured for a Group. The details displayed are:

Field	**Description**
Test Exercise Name	Displays the Drill name.
Last Executed Status	Displays the last execution status of the drill, BCO and BP.
Version	Displays the published version or the draft version of the Drill, BCO and BP.

Field	Description
Dry Run status	Displays the last dry run status of the Drill, BCO and BP.
Visible Distinction of Workflows	**Template** ▤ - Kyndryl Services does not own these Workflows and will not be accountable. Information is applicable only to Workflow Listing pages. **Pre packaged** ⊞ - Kyndryl Services owns these Workflows and is accountable. information is applicable to only Workflow Listing pages All NC's are Pre-Packaged **User Added** - The workflows created by the user are displayed as the User Added, and are not delivered as a part of the solution.
Workflow Listing Icons	Start Test Click ▶ Execute icon to start a Drill. On clicking the **Execute** button, it displays another pop up, to confirm the execution. Click **Execute** to confirm or click **Cancel** to cancel the execution.

Viewing Automation Status

To view the automation status, perform the following steps:

1. In the navigation bar, click **Drills > Executing Workflows**.
2. Select Viewing automation completeness status.

Field	Description
Base workflows	Displays the name of the basic workflows: Normal copy Normal full copy Switch over Switch back Failover Failback
Fusion Chart	Click on ◔ to display the number of groups configured.

Base workflow publish status	Displays the number of base workflows published. Click on a group from the list. Base workflow configuration page appears.

Viewing Workflow Calendar

To view the list of workflows scheduled, perform the following:

1. In the navigation bar, click **Drills> Drill List**.
2. Click Workflow Calendar.

The calendar lists the following:

Field	**Description**
workflow	Displays the workflow name.
Group name	Displays the workflow name.
Date	Displays the scheduled date
Recurrence	Displays the type of recurrence to schedule the workflow. For example: Just once Daily monthly weekly.
Approvers	Displays the approvers' name.

Drills Management

Majority of the DR solutions fail at the time of disaster even with huge infrastructure. This is either because there is no DR test plan in place or because it is too complex or expensive to execute. The Drills provides complete management control for performing DR drills and rehearsals. It provides wizard based control to handle the exercises in an automated and reliable method.

Kyndryl Resiliency Orchestration provides automated drills management for key intrusive and non-intrusive drills . It provides the following important capabilities:

- Individual FileSystem level drills execution and monitoring the status of the same.
- Automated execution of drills with wizard control for user intervention where desired.
- Intrusive drills support – provides 'Failover of the FileSystem' drills.
- Non-intrusive drill support – provides 'DR FileSystem consistency and integrity' drills.

You can view list of drills configured for a group by clicking **Drills** on the **Navigation bar**. The **Drills** page appears. This page provides the following information:

Field	**Description**
Group Name	Displays the name of the RG or AG
In Progress	Displays the number of Drills which are currently being executed for the Group
Configured	Displays the number of Drills configured for the Group
Never Executed	Displays the number of configured drills that were not executed
Failed	Displays the number of Drills that were not successfully completed
Success	Displays the number of Drills that were completed successfully
Aborted	Displays the number of Drills that were aborted manually

Note:

- Click ⇕ of GROUP NAME column to sort by Group states.
- In Drills page, click on group from the **GROUP NAME** column for which you want to execute the drills.

Scheduled

Viewing Scheduled

- Click **Drills** > **Scheduled >** on the navigation bar.
- Select RG /AG from the drop -down list. Select the filter.
- Click **For Immediate 7 days** to view the workflows which are scheduled for the next seven days.

The Scheduled workflow page displays the following:

Field	Description
Group Name	Displays the name of the RG.
Drill name	Displays the type of Drills
Scheduled Start Time	Displays the time when the drill has occurred

Scheduling Workflows

The workflows which have the version status as Published can be scheduled for execution.

To schedule workflows,

- Click Drills > Summary > Group Name
- The Drill Listing page is displayed.
- Click the Calendar 📅 to schedule the workflow.

The **Schedule Workflow** Calendar is displayed

Field	Description
Group	Displays the Group name
Workflow	Displays the Workflow name

On selecting the **Enable Schedule**

Field	Description

Recurrence Frequency	The radio button is set to Just Once
Once on	Select the date from the Calendar
Start Executing This Process at	Select time from the clock

Click **Cancel** to cancel the schedule and **Done** to save the changes.

Executing

Executing

- Click Drills > Executing
- Select RG /AG from the drop - down list. Select the filter.

The Executing page displays the following:

Field	**Description**
Group Name	Displays the name of the RG.
Drill name	Displays the type of Drills
Time Started	Displays the time when the drill has occurred
Elapsed Time	Displays the time for execution
Status	There can be two status namely Awaiting Input Executing

On clicking the group name, the **Drill listing** page is displayed.

On clicking the status, the Execution page of the workflow is displayed. The following information is displayed in the execution workflow page.

Field	Description
Group Name	Displays the name of the RG.
Workflow Name	Displays the workflow name along with the version
Start Time	Displays the time when the drill has occurred
Time Elapsed	Displays the time for execution
Status	There can be five status namely ▪ Awaiting Input ▪ Executing ▪ Success ▪ Failed ▪ Aborted

The next table displays information at the RAL level.

Field	Description
Action	Displays the RAL action
Time initiated	Displays the time the execution has started
Time Elapsed	Displays the time of execution of the RAL
Status	The status can be ▪ Awaiting input ▪ Unable to execute ▪ Success

Field	Description
	▪ Crashed ▪ Aborted

Click on **Key Value Pairs** to view the key values in the execution page.

Click on **Export to CSV** to export the workflow.

Summary

Viewing Summary

To view the summary for a list of Groups, on the **Navigation Bar**, click **Drills> Summary> Group Name**. You can also view from the Dashboard, by clicking **Drills.**

The user can select either the recovery groups or Application groups from the drop - down list. **Filter** is set to Type I by default. The continuity status is represented by the color beside the group name.

The **Summary** tab has the following fields:

Field	Description
Group name	Displays the name of the Recovery Group or Application Group
Drafts	Displays the state of the workflow
Published	Displays the workflow
Executing	Displays the number of configured drills that are being executed
Last Executed	Displays the date and time when the last execution has successfully been completed.
Next Scheduled	Displays the date for the next drill

Click **View all** to view all the Recovery groups.

Note:

Click ⬍ of GROUP NAME column to sort by group states.

Select Workflow

Click **Drills** > **Summary** > **Group Name**.

The **Drills Listing** page is displayed.

Click **Create New.**

The **Select workflow** tab is displayed.

- Click on ✎ to edit the workflow.
- Click on 👁 to view the **Remote Check Preview** page.

Viewing Workflow details

To view the workflow details, perform the following:

1. In the navigation bar, click **Drill> Summary**.
2. Select the group.
3. The **Drill Listing** page displays the following information:

Current State:

Field	Description
Current state	Displays the current status of the workflow.
Version	Displays the version number of the workflow.
Dry Run	Displays the dry run status.
Executed	Displays the last execution time stamp and the status of the workflow.

4. Click the view 👁 to view each workflow.
5. The **View Workflow** page is displayed. To view the RALs in the workflow, select the category from the drop - down list.
6. Click on ℹ to add action node information to the workflow.
7. Click Zoom in 🔍 or 🔍 view the workflow.
8. Click **Edit** to edit the workflow.

On clicking the workflow name the execution history and the version history details are displayed.

Execution History:

Field	Description
Date	Displays the last execution date of the workflow.
Time	Displays the time of the workflow in seconds.
Status	Displays the last executed status of the workflow.

Version History:

Field	Description
Version	Displays the version number of the workflow.
Created ON	Displays the date creation of the workflow.
Created BY	Displays the user name, who created the workflow.
Executed	Displays the last execution status.

Editing Workflows

- Click Drills > Summary > Group Name > 👁 > View Workflows.
- Click ✎ **Edit**.

On clicking **Edit** more actions can be carried out to the workflows.

- Click on ADD to include Actions, Action Groups, Workflows into the workflow
- On selection of **Actions** the Replication category drop - down list is displayed
  - Click the drop - down list to choose any category
  - Click on ⊕ to add a new action node
  - Click **Show all RALs** to view all the RALs which opens the RAL Library.
- On selection of the **Action Groups**, the **Show all RALs** is highlighted. On clicking it, the RAL Library is displayed.
- On selection of the **Workflows**, the user can select a signature solution from the **Select Signature Solution** from the drop -down list. Click **Import Workflow** to browse for the workflow files.
- Click ⎘ to copy the node

- Click 🗑 to delete the node
- Click on ⑂ icon to add a **fork** node. It is used to execute actions in parallel.
- Click on ⑃ icon to add a **join** node. It is used to wait for executed forked actions.
- Click ⊞ to rearrange the workflow.
- Click **Key-Value List** to Add key Value.
- Click **Save Now** to save the Workflow
- Click **Export**. A popup window is displayed. Click **No** to cancel the action and **Yes** to export the workflow.
- Click **Next** to **Publish** Workflow.

Viewing Published workflow by logged in user

Viewing Published workflow by logged in user

These published workflow can be viewed in the following ways.

From the Summary page, Executing page and Scheduled page:

1. Click the Summary, Executing or Scheduled tab from the Drills page.
2. Click on the specific group name. The Drills Listing page appears.
3. Click the Workflow Published by You button on the right of the page to view the workflows published by the logged in user.

OR

1. Click the Drill name in the Drills Listing page. The drill history details page appears.
2. Click the Workflow Published by You button on the right of the page to view the workflows published by the logged in user.

Working with Workflow Manager

Working with Workflow Manager

Workflow is a sequence of steps/tasks performed to complete a business process. The business process could be a Business Continuity Operation or DR Drill or EOD operation.

Actions and workflows are a set of procedures that are configured to act against an event in the DR environment. You cannot add or delete an Action from a Workflow when it is being executed.

Workflow manager enables you to design the workflow logic, execute and view the execution status.

Configuring the workflow involves:

- Design the workflow logic

- Insert/delete actions to be performed

- Provide/alter inputs to the actions

- Flow control

- Conditions to quit/abort workflow

- Handle failure conditions

- Recursion (execute an action periodically)

- Scheduling the workflow

Executing the workflow involves:

- Execute (start/stop) workflow
- Schedule workflow

Execution Status:

- Show execution status

System Workflows

Kyndryl Resiliency Orchestration will execute certain workflow(s) periodically based on the DR solution for monitoring. Such workflows are called System workflows.

Workflow Execution Page

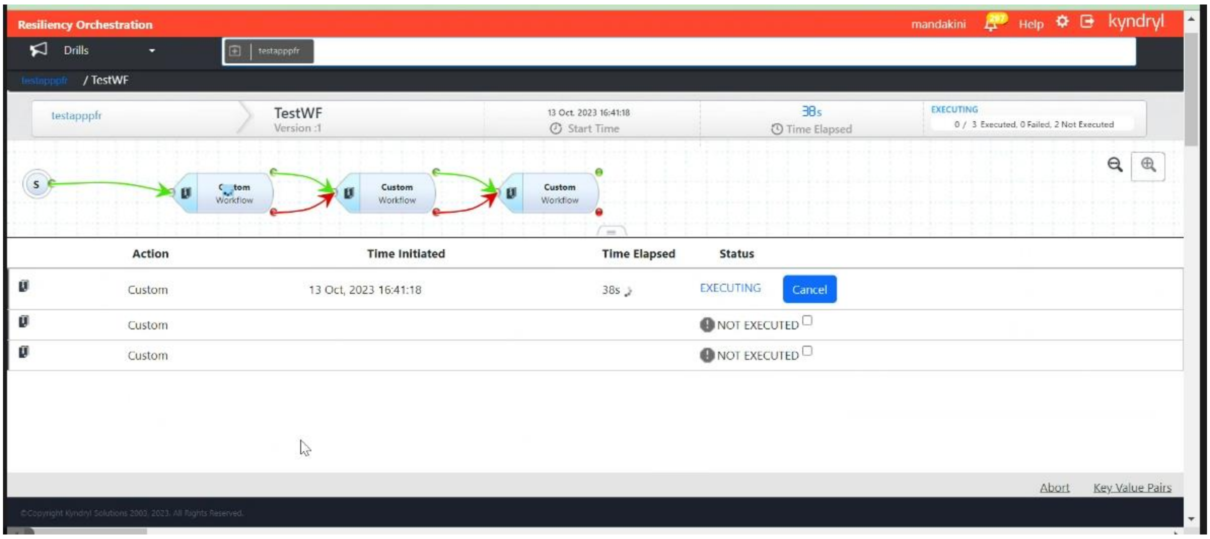
Clicking the **Executing** or **Awaiting Input** link in the Execution Status column will navigate the user to the workflow execution page. This page will display the information in the following table.

- Click the **Show Canvas** button to view the workflow details by loading the canvas.
- Click zoom in to make the canvas bigger.
- Click zoom out to make the canvas smaller.

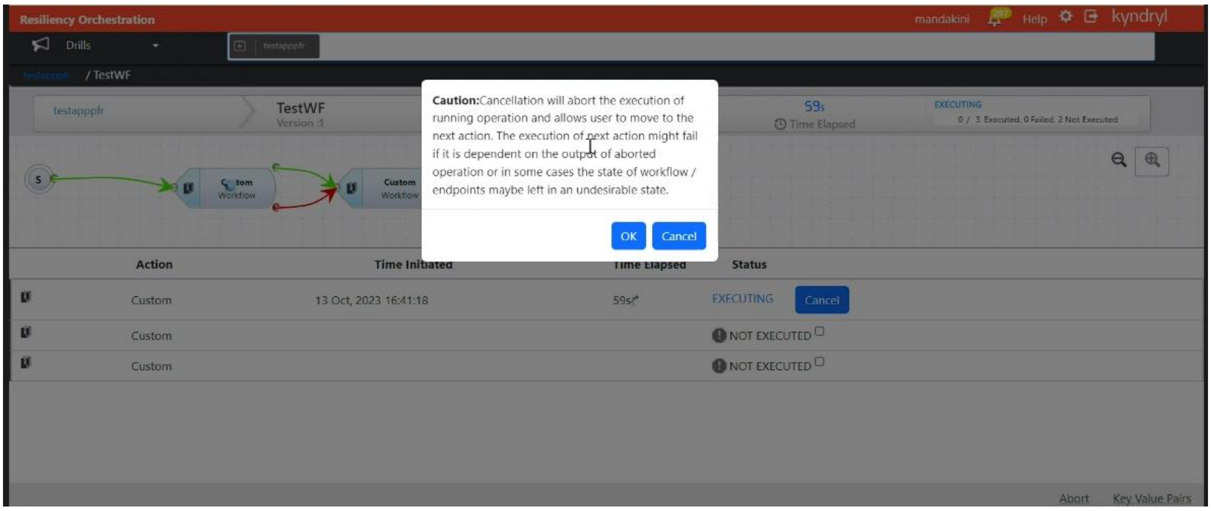
Field	Description
Action	Displays the name of the action.
TIME INITIATED	Displays the exact start time of the action execution.
TIME ELAPSED (SEC)	Displays the time calculated from the process of initiation to completion of the action.
TYPE	Displays the type of action.
STATUS DETAILS	Displays the status details of the action execution. Note: 1 If the status is in **EXECUTING** mode, the user can click on the EXECUTING link to view Continue as Success or Continue as Failure option buttons. Depending on the requirement and by giving a reason, select any one of the option. A **Cancel** button is provided when the status is "**EXECUTING**" as explained in the section Cancelling an Action in a running workflow. This button provides the ability to cancel the action which is in progress. 2 If the Status is **Awaiting Input**, depending on the requirement, user can select any one of the below options: • Continue as Success • Continue as Failure • Retry • Quit If user wants to know the reason for Awaiting Input, click the **View action log** button. Click on any link corresponding to desired action to view the following details for the action. • DB Logs • Tail Logs • Sys Logs

Cancelling an Action in a running workflow

The following screenshot shows the workflow in an EXECUTING status, along with a **Cancel** button.



Action	Time Initiated	Time Elapsed	Status
Custom	13 Oct, 2023 16:41:18	38s	EXECUTING Cancel
Custom			NOT EXECUTED □
Custom			NOT EXECUTED □



Caution: Cancellation will abort the execution of running operation and allows user to move to the next action. The execution of next action might fail if it is dependent on the output of aborted operation or in some cases the state of workflow / endpoints maybe left in an undesirable state.

Action	Time Initiated	Time Elapsed	Status
Custom	13 Oct, 2023 16:41:18	59s	EXECUTING Cancel
Custom			NOT EXECUTED □
Custom			NOT EXECUTED □

The **Cancel** button provides the ability to stop the current action and move to the next one in a workflow so that you can avoid aborting the whole workflow due to one problematic action.

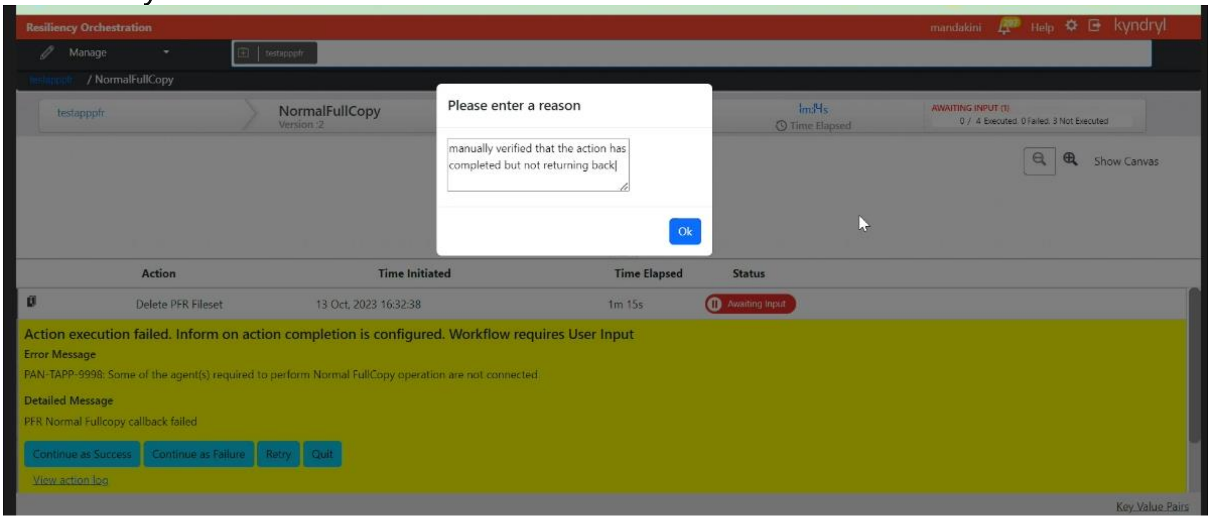
When you click the **Cancel** button, a pop-up window with a note of caution as shown below is displayed. Please read the message completely and carefully, and if you decide to go ahead with the cancel action, click **OK** button on the pop-up to confirm the cancel action. Click **Cancel** button on the pop-up to return to the execution page.

***Note of Caution**:*

Cancelling the action is a step which should be done in extreme cases and cannot be undone, it may result in undefined side effects and may potentially put the systems in unusable state. RO will simply stop monitoring the action and will not be able to kill or stop the actual action.

***Please consider the below risks before proceeding with Cancelling the action**:*

1. No attempt from Resiliency Orchestration will be made to roll back the steps already completed by the action.
2. The action may have been executed completely and waiting to exit Or it might be in the middle of executing a command which may continue to execute after cancelling the action in Resiliency Orchestration.
3. User must verify this action to either partially or fully execute the step manually as appropriate outside Resiliency Orchestration.
4. Any downstream RALs that depend upon the Key Values set from this action may fail.



Please enter a reason

manually verified that the action has completed but not returning back|

Action	Time Initiated	Time Elapsed	Status
Delete PFR Fileset	13 Oct, 2023 16:32:38	1m 15s	Awaiting Input

Action execution failed. Inform on action completion is configured. Workflow requires User Input

Error Message

PAN-TAPP-9998: Some of the agent(s) required to perform Normal FullCopy operation are not connected

Detailed Message

PFR Normal Fullcopy callback failed

When you click the **OK** button, a second pop-up window as shown in following screenshot is displayed where the reason for cancelling the action needs to be entered in the provided text box. Click **OK** button in the second pop-up and reconfirm the cancel action. Once you click **OK**, the action goes to **Awaiting Input** status.

Resuming Workflow After Kyndryl Server failure

If Kyndryl Resiliency Orchestration server fails due to hardware, network or other problems, all workflows being executed also stops. When the server is up again, the failed workflows can be resumed automatically or manually, depending on the presence of recurring actions in it.

Note

When Kyndryl Resiliency Orchestration server is up, if a workflow contains at least one recurring action, the complete workflow is resumed from the start.

For a workflow that does not have any recurring actions, you need to take a decision on its further execution. To do so, perform the following steps:

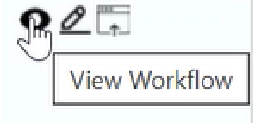
1. Click Manage> Recovery Groups > Group Name > on the navigation bar. The Recovery Groups details page appears.
2. Click the Execute button for the workflow in the Continuity Workflows section.
3. Click the Resume button to continue the operation. UserInputRequired004 event will be raised and will be shown in the event banner indicating that user intervention is required.
4. Click the Provide Input link on the Event Banner to open the Action Execution Handler page. In the Workflow Execution Section on the right, do any one of the following.

- Click Start to restart the Workflow from the beginning.
- Click Skip As Success to skip the current action considering it to be successfully executed and continue with the next action.
- Click Skip As Failure to skip the current action considering it to be failed and continue with the next action. The next action will be that pointed to by the Failure path of the current failed action, not the normal Success path. If the failure path of the failed action is pointing to "None" then the workflow will terminate.
- Click Resume to continue executing the current action.
- Click Quit to stop workflow execution. The complete workflow terminates without executing any more actions.

Dealing with Failures of Workflow Execution

When certain action's execution is failed, you can view the action failure details in the **Recent Execution Status** window.

To open the Recent Execution Status window:

1. Click the  icon to view the events waiting for user input. All actions which are configured to be informed are displayed here.
2. Click the **Provide Input** link for the event requiring your inputs. The **Recent Execution Status** page appears.

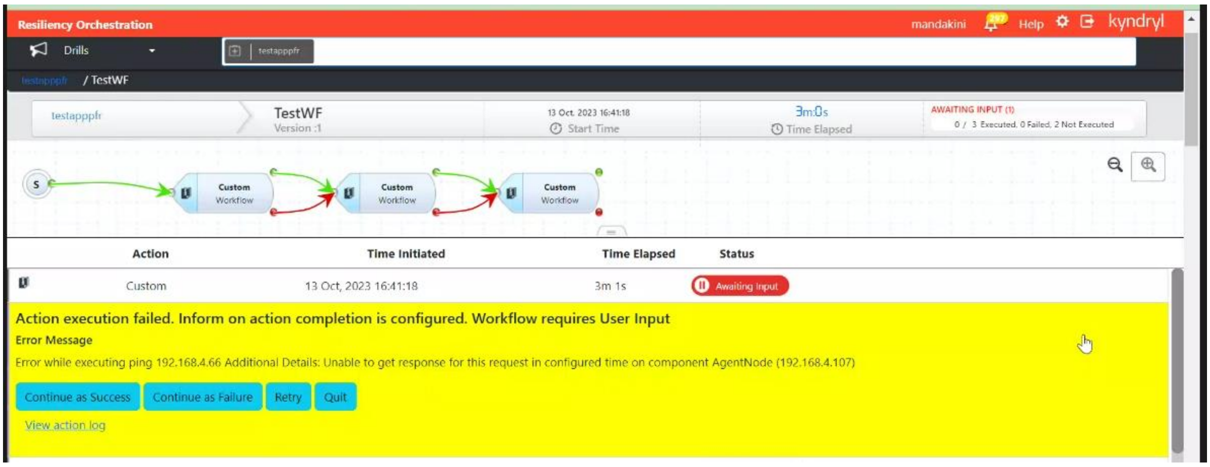
In Workflow Graph & Inputs tab:

- In case of Action Execution Failed:
    - Click **Retry** to retry the execution of the failed action.
    - Click **Continue** to execute the next action. The next action will be that pointed to by the Failure path of the current failed action, not the normal Success path. If the failure path of the failed action is pointing to **None** then the workflow will terminate.
    - Click **Quit** to stop workflow execution. The complete workflow terminates without executing any more actions.

- In case of Workflow Execution Recovery:
    - Click **Start** to restart the Workflow from the beginning.
    - Click **Skip As Success** to skip the action as success and continue with next action.
    - Click **Skip As Failure** to skip the action as failure and continue with next action.
    - Click **Resume** to continue executing the current action.
    - Click **Abort** to abort executing Workflow.

Limitation:

Skip As Success and Skip As Failure features do not work if we configure Time to execute property. Time to execute property is used to wait before execution.



Action	Time Initiated	Time Elapsed	Status
Custom	13 Oct, 2023 16:41:18	3m 1s	Awaiting Input

Action execution failed. Inform on action completion is configured. Workflow requires User Input

Error Message

Error while executing ping 192.168.4.66 Additional Details: Unable to get response for this request in configured time on component AgentNode (192.168.4.107)

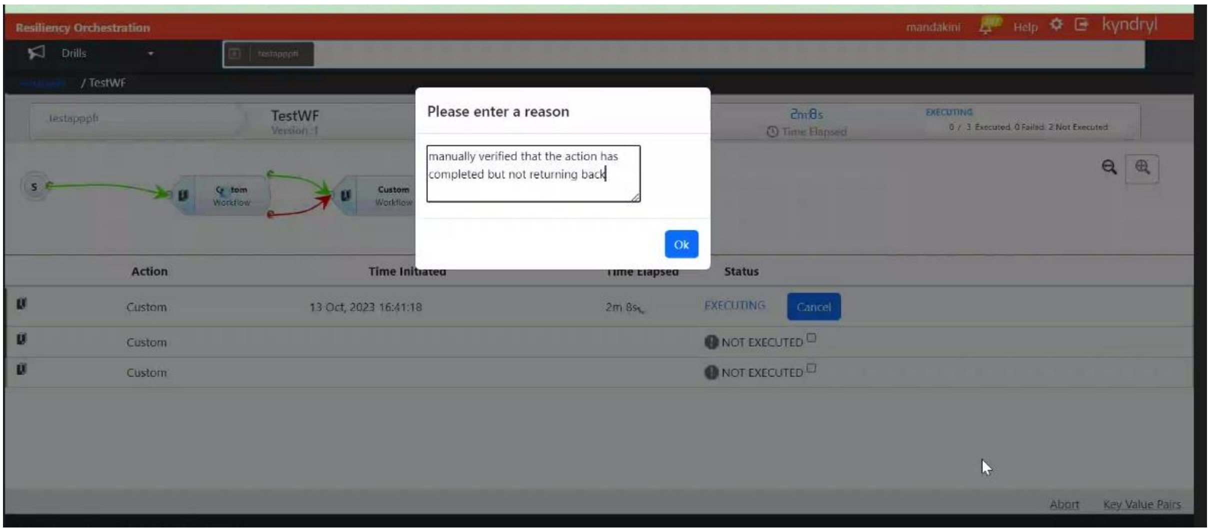
Stopping Workflows

Workflows will be stopped only after completing the execution of current action/action group. If there are any user input required by the action, then the workflow will stop only after the input is provided.

The following is the behaviour of stopping workflows with various configurations:

Action: If the action is executing, workflow will stop only after its completion.

Time To Execute (**Wait**): If this property is set, the action will wait for the configured time before it actually performs the task. Workflow will stop only after the action completes the **Wait** and performs the actual task.



Please enter a reason

manually verified that the action has completed but not returning back

Ok

	Action	Time Initiated	Time Elapsed	Status
	Custom	13 Oct, 2023 16:41:18	2m 8s	EXECUTING Cancel
	Custom			NOT EXECUTED □
	Custom			NOT EXECUTED □

i. **Execution mode Manual**: If this property is "**Manual**", then the action will notify the user before performing the actual task.

- Clicking **Continue** will stop the workflow after performing the actual task
- Clicking **Quit** will stop the workflow immediately without performing the actual task

i. **Inform on Completion**: If this property is set, then the action will notify the user after the actual task. Workflow will stop only after clicking "**Continue**" or "**Quit**". However, if this is a "**retryable**" action then clicking on "**Retry**" will execute the action again. [For more information on "**Inform completion**" and "**Is Retryable**" options, refer to **Configuring Actions**.

2. **Action Group**: If the action group is executing, the workflow will stop only after completing all actions in the action group.

If execution of an action within the action group results in abort of workflow, then no further actions within action group will be executed. For example, clicking "**Quit**" in "**Execution Mode Manual**" or "**Inform Completion**" for the action.

If there are multiple actions waiting for user input, then clicking "**Quit**" for one of the actions will only complete that action/action group, but not the workflow. You need to click "**Quit**" on all the actions that are waiting for user input for the workflow to stop. For example, when "**dump log**" and "**apply log**" recurring actions need user input, then clicking on "**Quit**" for "**dump log**" will complete only dump log but not "**apply log**" action. Clicking on "**Quit**" on the "**apply log**" will stop the workflow. Any workflow in progress can be aborted by clicking the "**Abort**" link on the **Workflow Execution Status** page.

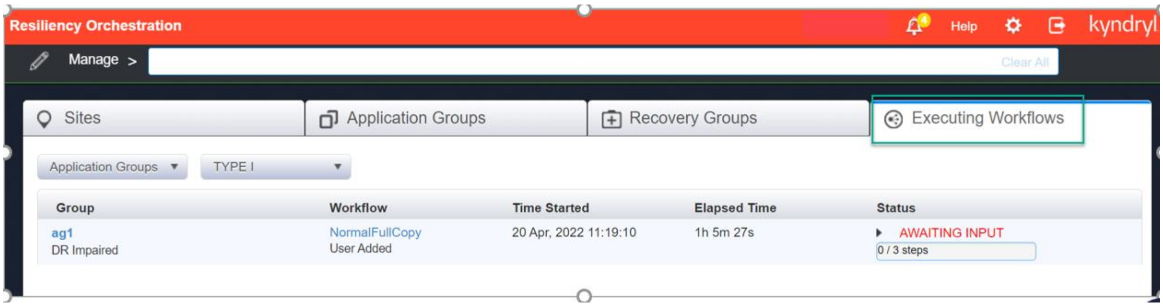
Approving/Rejecting a workflow before execution

After the workflow is created, the approver for a particular workflow can approve/reject for further execution. A notification e-mail is triggered to all users on the approver list having valid e-mail IDs stating that the current workflow needs approval.

To approve/reject the workflow, perform the following steps:

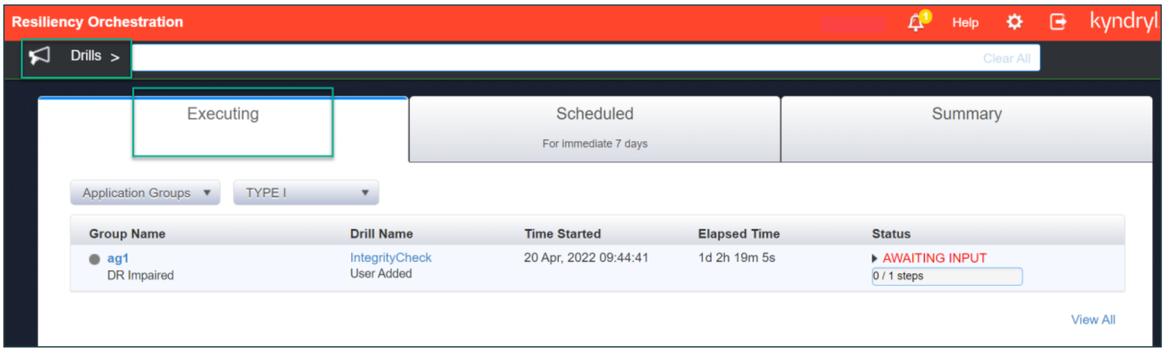
1. Log in to Kyndryl RO.

2. Click **Manage** -> **Executing Workflows**.



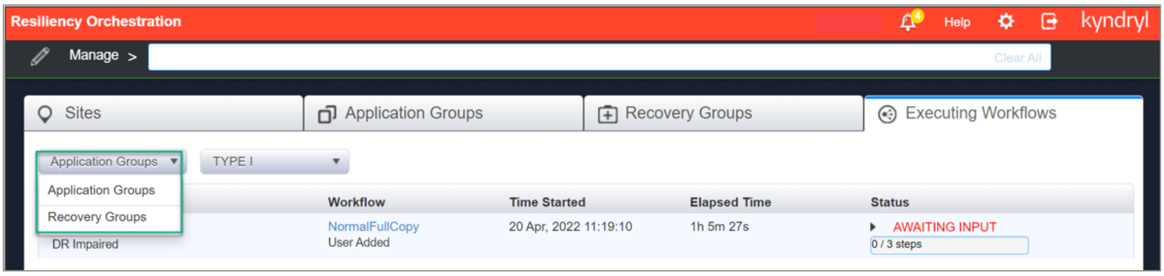
Group	Workflow	Time Started	Elapsed Time	Status
ag1 DR Impaired	NormalFullCopy User Added	20 Apr, 2022 11:19:10	1h 5m 27s	AWAITING INPUT 0 / 3 steps

Note: If the Workflow for a particular Application Group/Recovery Group is not listed, then navigate to **Drills -> Executing**.



Group Name	Drill Name	Time Started	Elapsed Time	Status
ag1 DR Impaired	IntegrityCheck User Added	20 Apr, 2022 09:44:41	1d 2h 19m 5s	AWAITING INPUT 0 / 1 steps

3. Select the appropriate Application Group or Recovery Group from the **Application Groups** drop-down.

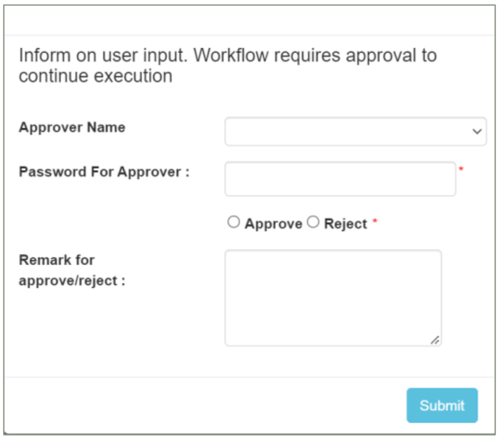


	Workflow	Time Started	Elapsed Time	Status
DR Impaired	NormalFullCopy User Added	20 Apr, 2022 11:19:10	1h 5m 27s	AWAITING INPUT 0 / 3 steps

The following details are visible for the selected group:

- Group: Includes the Group name of the Application Group or Recovery Group.
- Workflow: Includes the Workflow name provided by the user.
- Time Started: Provides the Timestamp when the Workflow is executed.
- Elapsed Time: Includes the time duration of the workflow execution.
- Status: Provides the status of the workflow.

4. Click **Awaiting Input** under the Status column. The following screenshot appears.



Inform on user input. Workflow requires approval to continue execution

Approver Name

Password For Approver : *

○ Approve ○ Reject *

Remark for approve/reject :

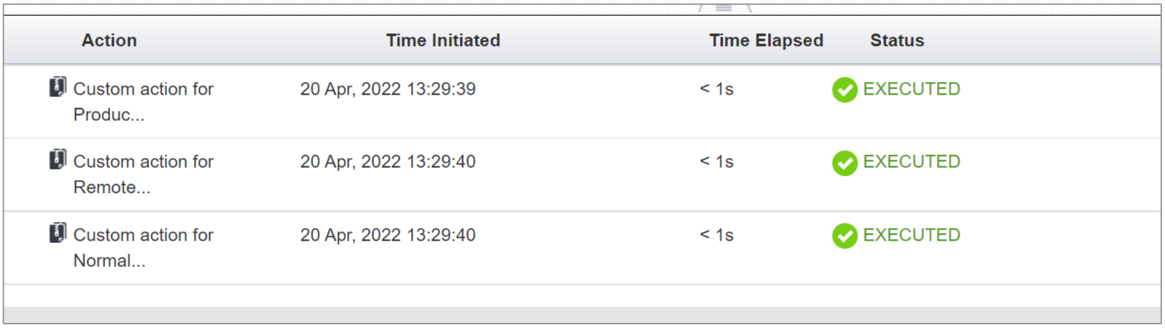
Submit

5. Enter the following details:

Field Name	**Description**
Approver Name	Includes the Approver name. This is a drop-down to select any different user also.
Password for Approver*	Enter the valid password for the approver. **Approve**: Click the Approve button to approve the workflow. **Reject**: Click the Reject button to reject the workflow.
Remark for Approve/Reject	Provide details in the text box to approve or reject the workflow.

6. Click **Submit** to submit the details.

Step Result: The following screenshot appears after execution of the workflow.



Action	Time Initiated	Time Elapsed	Status
Custom action for Produc...	20 Apr, 2022 13:29:39	< 1s	✓ EXECUTED
Custom action for Remote...	20 Apr, 2022 13:29:40	< 1s	✓ EXECUTED
Custom action for Normal...	20 Apr, 2022 13:29:40	< 1s	✓ EXECUTED

Note: If you select the Reject option in Step 5, the workflow does not execute and the status displays as "Not Executed". The Approval/Rejection of the workflow is audit logged in the system for future reference.

Using the new debugging capability for Dry run

While using the Dryrun debug feature, the user can choose any Group and Workflow pair and then debug it in greater detail.

Add property dryrun.debug.workflow.group=<GroupName>&<WFName>

to the file $EAMSROOT/installconfig/panaces.properties.

For example, AG/RG 'TestGroup' and workflow 'Failover,'

the property to be updated as given below

dry run.debug.workflow.group=TestGroup&Failover

NOTE: Server restart is NOT required to use this feature

After identification of the workflow for debugging and the Dryrun has initiated, the log files will be generated till the Dryrun ends.

dryrun.debug.workflow.group=all --> will debug all the dry runs..

which will produce a log file at the location $EAMSROOT/var/logs

example of a log filename: DryrunDebug.log

which will produce a log file at the location $EAMSROOT/var/log/DryrunDebug.log

Configuring Multiple Dry Run Limit

Executing multiple dry runs in parallel is limited to available CPU resources by default. You can, however, configure the number of dry runs that can be executed parallelly to avoid exhausting or running out of resources.

It is recommended to change the setting below, in case you would want to execute more than 1000 dry runs in parallel.

Perform the following steps to set the multiple dry run execution limit:

1. Login to the Kyndryl Resiliency Orchestration Server and open folder $EAMSROOT/installconfig. You will see the Panaces.Properties file.
2. In the Panaces.Properties file., locate the following two parameters with their default values.

   ```
   panaces.dryrun.usePool=false
   panaces.dryrun.poolsize=1000
   ```

Parameter	Value	Description
panaces.dryrun.usePool	false	This value disables the use of thread pool defined in panaces.dryrun.poolsize.
	True	This value enables the use of thread pool defined in panaces.dryrun.poolsize.
panaces.dryrun.poolsize	<whole number>	A user defined value of maximum number of dry run that can be executed parallelly.

3. To set the user defined values, first set the panaces.dryrun.usePool to true and then set the required value of dry run.

   Example:

   ```
   panaces.dryrun.usePool=true
   panaces.dryrun.poolsize=2000
   ```

   Note: The above configuration indicates that the dry run is user defined and that 2000 dry runs can be executed parallelly.
4. Save the properties file.

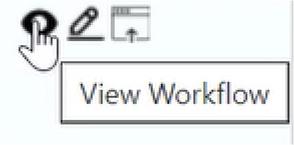
Nested Workflow (Navigation to Workflow within a Workflow)

"Workflow Calling Workflow" enables the user to call sub workflows from the main workflow execution page.

After configuring the workflow calling workflow, a nested workflow link is displayed in the main execution page. Clicking the nested workflow link will navigate to the sub workflow execution page.

From the sub workflow execution page, the user can navigate to the main workflow execution page by clicking on parent workflow name on the breadcrumb.

View Workflows



Click on the View icon against the workflow.

The view workflow page is displayed. In this page the user can only view (Read only) RALs. The user cannot modify any values in the view workflow page.

Click on the edit icon in the view workflow page. The user is enabled now to navigate to the Workflow Editor page.

Workflows Visual Distinction

The workflows are categorized into three types namely

1. Prepackaged
2. Template and
3. User Added

Pre-Packaged: These workflows are owned and shipped by Kyndryl.

Template: Template is a workflow that can be used with modifications as per the requirements.

User Added: The workflows created on the field by the user.

Stopping/Aborting Parent Workflows

While stopping/aborting the parent workflow, the child workflows are stopped.

Propagation of Nested Workflow Status

The child workflow status needs to be displayed in the parent workflow during all stages: preexecution, execution, and post execution.

Parent Workflow Summary Counts

The following counts of parent workflow execution include the actions count of child workflows:

- Completed steps
- Total steps
- Failed steps
- Not executed steps

In the parent workflow execution page, the Trigger action, which calls the child workflow, displays the progress bar with count of Completed steps, Total steps, Failed steps, and Not executed child workflow steps.

Glimpse of Nested Workflows

In the Parent Workflow Execution page, the user can expand the Trigger action to see trending actions, which are in executing state and which need inputs. The corresponding details such as action name, start time, elapsed time, and status details displays.

Validating and Fortifying Nested Workflows

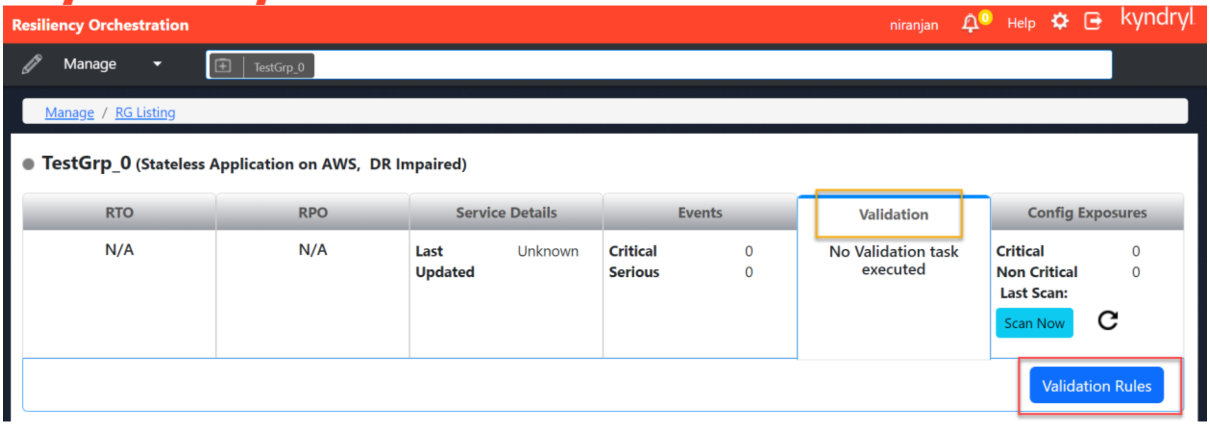
Prior to executing the parent workflow, all child except NormalCopy or ReverseNormalCopy workflows will be locked, which means the user cannot Edit, Delete, or Execute child workflows until the parent workflow completes its execution.

The user can edit parent workflow although it has child, which is in execution. The user can edit the parent workflow when it has common child and other parent workflow is in execution.

Validation Manager

Validation

Validation Manager framework identifies the configuration drifts between PR and DR infrastructure and raise alerts in case of deviations that will impact the recovery.



Validation Rules

A Rule is a template that executes a command to validate the configuration differences between PR/DR. The execution result output will be either of the following:

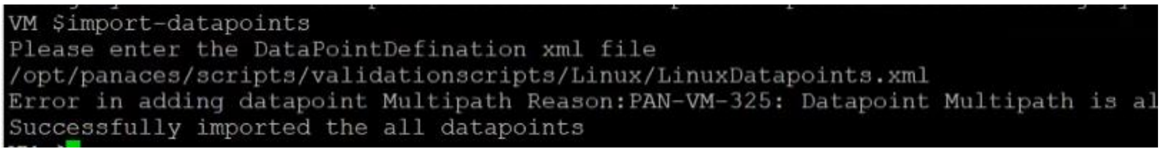
- Success – If the configuration matches.
- Failed – If the configuration does not match.

Importing Validation Rules

Auto Import Validation Rules

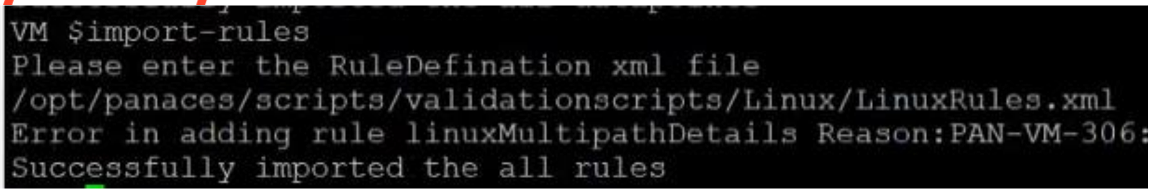
By default, all the validation rules are auto imported at the time of RO installation. If you are developing new validation rules, then you can manually import them using the following steps:

1. Datapoints and Rules (.xml files) are imported using VMClient.sh
2. Path of VMClient - /opt/panaces/bin/
3. Run VMClient.sh
4. First use command "import-datapoints" to import datapoints.
5. Provide path of datapoint xml files.



```
VM $import-datapoints
Please enter the DataPointDefination xml file
/opt/panaces/scripts/validationscripts/Linux/LinuxDatapoints.xml
Error in adding datapoint Multipath Reason:PAN-VM-325: Datapoint Multipath is al
Successfully imported the all datapoints
```

6. Secondly use Command "import-rules" to import rules.
7. Provide path of Rules xml files.



```
VM $import-rules
Please enter the RuleDefination xml file
/opt/panaces/scripts/validationscripts/Linux/LinuxRules.xml
Error in adding rule linuxMultipathDetails Reason:PAN-VM-306:
Successfully imported the all rules
```

Listing Validation Rules

To list the Validation Manager Rules available in a Resiliency Orchestration Server perform the following steps:

1. Click **Monitor** OR **Manage** on the Navigation bar.
2. Click **Recovery Groups > Group Name > Validation.**
3. Click **Validation Rules** button. The **Task Summary List** window appears.
4. Click **View Rules** tab on the top left corner of the page.
5. Click on the specific category and the following details can be seen:

Field	Description
Name	Displays the rule name.
Description	Displays the description of the rule selected.

Note

- CUSTOM / Linux / Oracle / MSSQL / NetApp / IBMSpectrumProtect, and VCentre default categories are available.
- Validation Manager is not supported in case of RO Upgrade if customer is using Oracle 21C prior to June 2022. After June 2022, Validation Manager works fine in both cases (Upgrade or fresh RO installation with a newly discovered Oracle 21C group.
- Validation manager supports local and remote agent model.

Successful and Failure Events

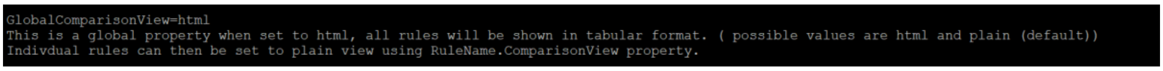
- In case of successful validation, an event is created as **Info** event.
- In case of failed validation, an event is created as **Critical** or **Serious** depending on the configurated validation rule.
- In the Incident table database, **ValidationTaskSuccess** and **ValidationTaskFailed** are recorded.
- In case of failure, when the failure reasons are resolved, **PolarEvents** are generated. The validation tasks that were failed earlier, become successful and

PolarEvents (Info) against the Critical/Serious events are generated. The respective Critical/Serious event is closed.

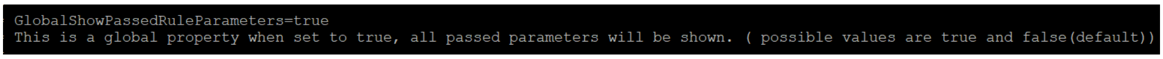
Reporting

The Validation Manager Reports enables the customers to view configuration differences between PR and DR sites. The configuration differences are highlighted in the UI and Reports (PDF format).

Property *(/opt/panaces/installconfig/validation_rules_metadata.properties*) modification is required to enable the reporting enhancements such as tabular view for Validation Manager.

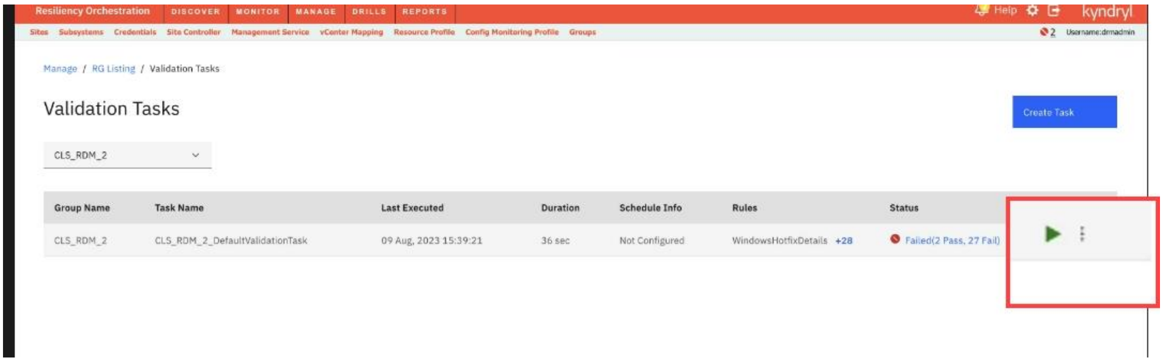


```
GlobalComparisonView=html
This is a global property when set to html, all rules will be shown in tabular format. ( possible values are html and plain (default))
Indivdual rules can then be set to plain view using RuleName.ComparisonView property.
```



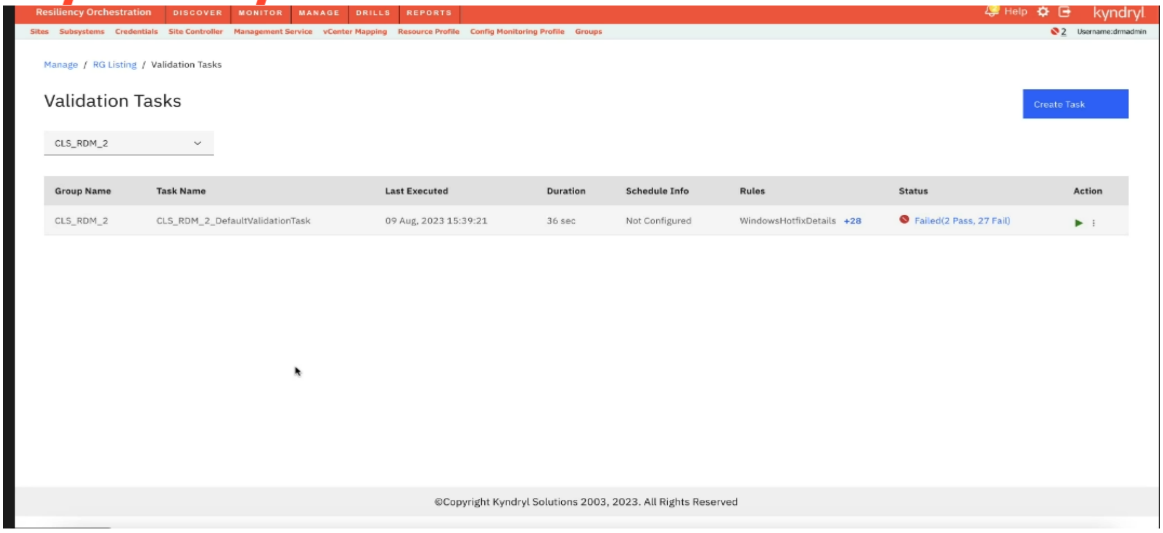
```
GlobalShowPassedRuleParameters=true
This is a global property when set to true, all passed parameters will be shown. ( possible values are true and false(default))
```

Validation rules can be executed from task summary page. Execution results can be reviewed/downloaded as a report by clicking the status.



Validation Tasks

Group Name	Task Name	Last Executed	Duration	Schedule Info	Rules	Status
CLS_RDM_2	CLS_RDM_2_DefaultValidationTask	09 Aug, 2023 15:39:21	36 sec	Not Configured	WindowsHotfixDetails +28	Failed(2 Pass, 27 Fail)



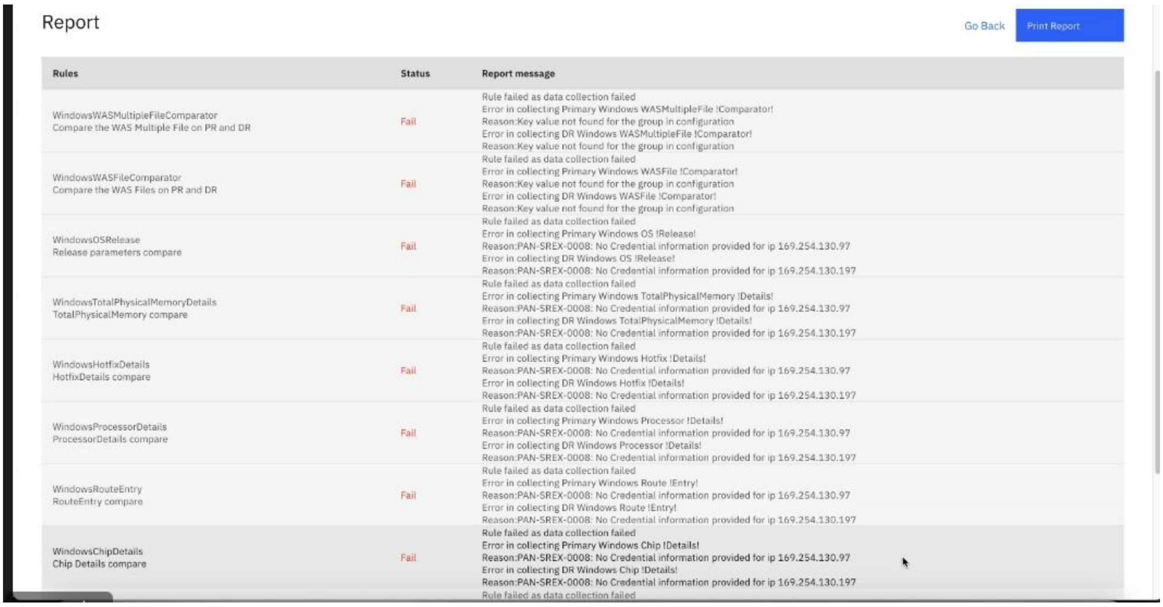
Validation Tasks

Group Name	Task Name	Last Executed	Duration	Schedule Info	Rules	Status	Action
CLS_RDM_2	CLS_RDM_2_DefaultValidationTask	09 Aug, 2023 15:39:21	36 sec	Not Configured	WindowsHotfixDetails +28	Failed(2 Pass, 27 Fail)	▶ ⋮

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

Steps to navigate to capture this screen. (Navigation path to be added)

For example,(If you execute the following validation rule and if the status is failed, the following report is displayed on your screen with the 'Failed' status.



Report

Rules	Status	Report message
WindowsWASMultipleFileComparator Compare the WAS Multiple File on PR and DR	Fail	Rule failed as data collection failed Error in collecting Primary Windows WASMultipleFile !Comparator! Reason:Key value not found for the group in configuration Error in collecting DR Windows WASMultipleFile !Comparator! Reason:Key value not found for the group in configuration
WindowsWASFileComparator Compare the WAS Files on PR and DR	Fail	Rule failed as data collection failed Error in collecting Primary Windows WASFile !Comparator! Reason:Key value not found for the group in configuration Error in collecting DR Windows WASFile !Comparator! Reason:Key value not found for the group in configuration
WindowsOSRelease Release parameters compare	Fail	Rule failed as data collection failed Error in collecting Primary Windows OS !Release! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.97 Error in collecting DR Windows OS !Release! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.197
WindowsTotalPhysicalMemoryDetails TotalPhysicalMemory compare	Fail	Rule failed as data collection failed Error in collecting Primary Windows TotalPhysicalMemory !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.97 Error in collecting DR Windows TotalPhysicalMemory !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.197
WindowsHotfixDetails HotfixDetails compare	Fail	Rule failed as data collection failed Error in collecting Primary Windows Hotfix !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.97 Error in collecting DR Windows Hotfix !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.197
WindowsProcessorDetails ProcessorDetails compare	Fail	Rule failed as data collection failed Error in collecting Primary Windows Processor !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.97 Error in collecting DR Windows Processor !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.197
WindowsRouteEntry RouteEntry compare	Fail	Rule failed as data collection failed Error in collecting Primary Windows Route !Entry! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.97 Error in collecting DR Windows Route !Entry! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.197
WindowsChipDetails Chip Details compare	Fail	Rule failed as data collection failed Error in collecting Primary Windows Chip !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.97 Error in collecting DR Windows Chip !Details! Reason:PAN-SREX-0008: No Credential information provided for ip 169.254.130.197
		Rule failed as data collection failed

.

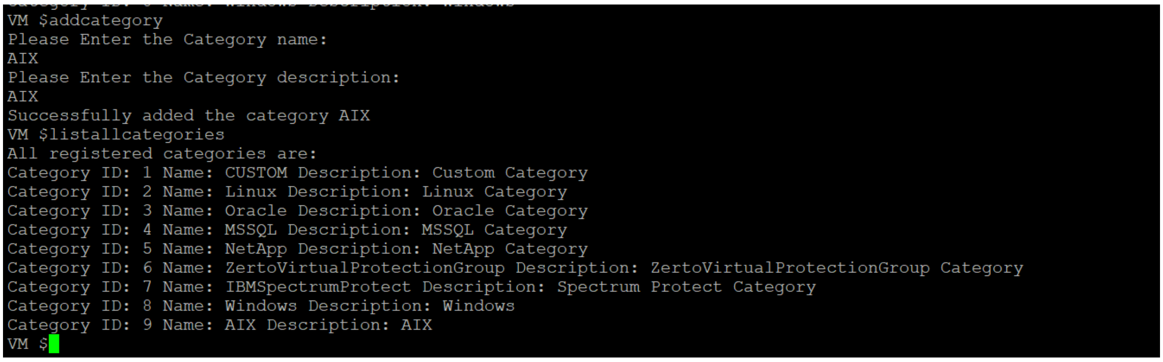
Adding Categories

The Validation Manager in RO supports 3 categories (OS, Database, and Middleware):

- **OS**: Linux, Windows, AIX, Solaris, Ubuntu
- **DB**: Oracle, MSSQL
- **Middleware**: Weblogic, Jboss

When you navigate to **List Categories**, it lists all the default categories as shown in the image below. Some of the default categories that are available are:

CUSTOM / Linux / Oracle / MSSQL / NetApp / IBMSpectrumProtect, and VCentre



```
VM $addcategory
Please Enter the Category name:
AIX
Please Enter the Category description:
AIX
Successfully added the category AIX
VM $listallcategories
All registered categories are:
Category ID: 1 Name: CUSTOM Description: Custom Category
Category ID: 2 Name: Linux Description: Linux Category
Category ID: 3 Name: Oracle Description: Oracle Category
Category ID: 4 Name: MSSQL Description: MSSQL Category
Category ID: 5 Name: NetApp Description: NetApp Category
Category ID: 6 Name: ZertoVirtualProtectionGroup Description: ZertoVirtualProtectionGroup Category
Category ID: 7 Name: IBMSpectrumProtect Description: Spectrum Protect Category
Category ID: 8 Name: Windows Description: Windows
Category ID: 9 Name: AIX Description: AIX
VM $
```

Steps to add a new category.

To add a new category, follow these steps:

1. Navigate to the install location.
2. Run the *vmcscript.sh* file.
3. Execute *Add Category* command.

Now create a folder with a specific name and then import the relevant rules.

IBMSpectrumProtect

IBMSpectrum Protect Validation Rules

There are four validation rules for IBMSpectrum Protect. The following table displays all validation rules for IBMSpectrum Protect:

SL No.	Rule Name	Description
1.	SpectrumProtectServerVersionCompare	Compares the Spectrum Protect Operating System version between Primary and DR server.
2.	SpectrumProtectClientVersionCompare	Compares the Spectrum Protect client version between Primary and DR server.
3.	SpectrumProtectUserPrivilege	Compares the user privilege is same on Primary and DR server.

4.	SpectrumProtectValidatePolicy	Compares the Spectrum Protect policy mode is set to STANDARD on Primary and DR server.

- If the rule is successfully executed and passed, the status of the corresponding rule displays **Pass.**
- If the rule fails, an error message displays the details about the failure and the status of the corresponding rule displays **Fail**.

AIX Validation Rules

- AIXProcessorType
- AIXCpuCount
- AIXCpuEntiled
- AIXCpuSpeedInfo
- AIXCappedUncapped
- AIXMemoryDetails
- AIXRunningServices
- AIXLastRebootInfo
- AIXVolumeGroups
- AIXMemoryUtilization
- AIXDiskDetails
- AIXNfsVersion
- AIXNetstatDetails
- AIXTCPTuneParameter
- AIXUDPTuneParameter

Linux Validation Rules

- linuxDirectoriesPermission
- linuxMountPermission
- linuxRouteEntry
- linuxLogicalVolumeDetails
- linuxCPUspeedDetails
- linuxPvDetails
- linuxVgDetails
- linuxLast20patchList
- linuxLastRebootDetails
- linuxLoadAverageDetails

- linuxNTPStatusDetails
- linuxRMcommandHistory
- linuxDNSserverDetails
- linuxJavaVersion
- linuxSystemDetails
- linuxMultipathVersion
- linuxRAMhealthStatus
- linuxHardDiskDriveDetails
- linuxLimitCheck
- linuxMultipathDetails
- linuxCPUcount
- linuxSpeedAndDuplexSettings
- linuxMotherboardStatus
- CompareWeblogicXML
- linuxFilesChecksum
- CompareWebLogicPatch
- linuxMemoryDetails
- linuxDfCommandDetails
- linuxNFSVersion
- linuxWWNNumber
- linuxSEPolicy
- LinuxHostName
- LinuxIPAddress
- LinuxEstablishedPortDetails
- LinuxHostFile
- LinuxKernelDmesg
- LinuxNetworkInterface
- linuxKernelParameters
- linuxReadhatOSRelease

Oracle Validation Rules

- oracleVDollarParameters
- oracleVDollarSpParameters
- oracleTnsnamesOraFile
- oracleSqlnetOraFile

- oracleListenerOraFile
- oracleOpatchID
- oracleDbSize
- oracleUndoFileSize
- oracleTempFileSize
- oracleVDollerLogCount
- oracleVDollerLogInfo
- oracleVDollerLogFileCount

MSSQL Validation Rules

- MSSQLVersionInfo
- MSSQLServerName
- MSSQLServerBuildInfo
- MSSQLListColumns
- MSSQLSysServers
- MSSQLSysDatabaseDetails
- MSSQLSysAltFilesDetails
- MSSQLSPHelpDBDetails
- MSSQLDBCCTraceStatus
- MSSQLSPhelprevLogin
- MSSQLServicePackDetails
- MSSQLLicenseTypeInfo
- MSSQLLicenseCount
- MSSQLConfigurationInfo
- MSSQLCollationInfo

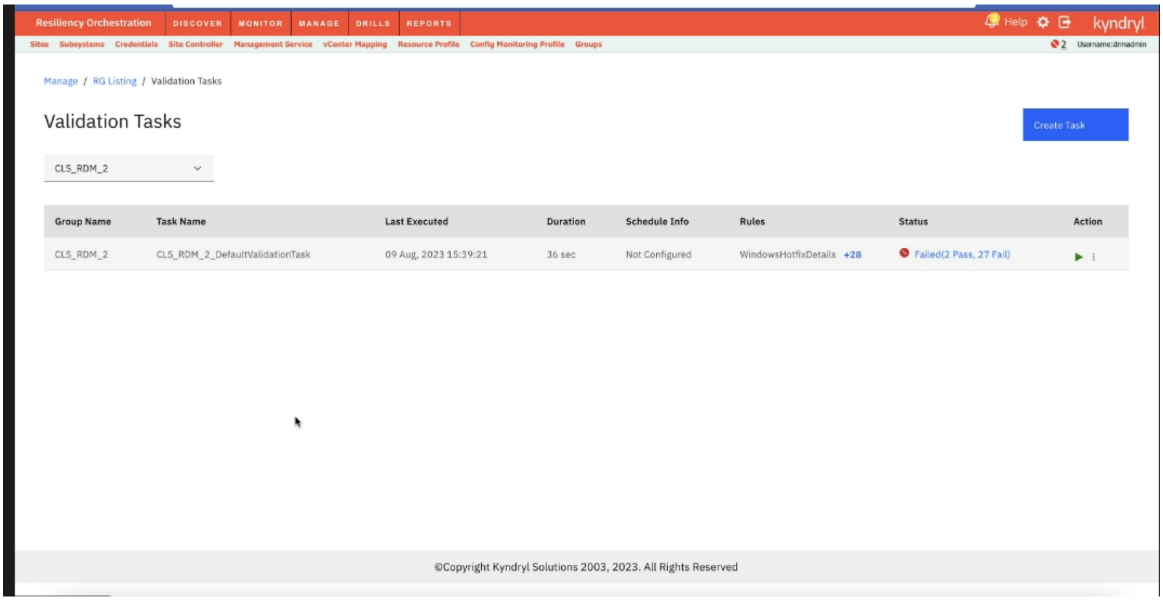
Windows Validation Rules

- WindowsOSRelease
- WindowsTotalPhysicalMemoryDetails
- WindowsOSVersion
- WindowsHotfixDetails
- WindowsProcessorDetails
- WindowsRouteEntry
- WindowsChipDetails
- WindowsCPUDetails

- WindowsCPULoadDetails
- WindowsFreePhysicalMemoryDetails
- WindowsFreeVirtualMemoryDetails
- WindowsRamHealth
- WindowsDiskFreeSpace
- WindowsCpuSpeedInfo
- WindowsCPUTypeInfo
- WindowsLogicalDiskDetails
- WindowsSpeedandDuplexDetails
- WindowsHostName
- WindowsRunningServicesInfo
- WindowsNetstatDetails
- WindowsBIOSVersion

Tasks

Listing Tasks



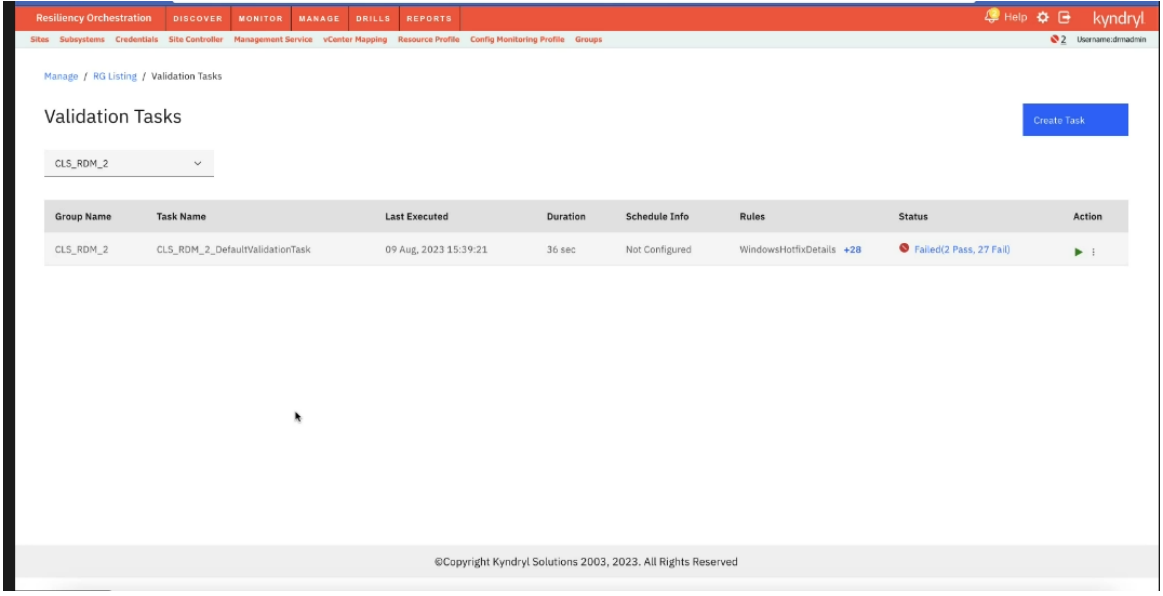
Validation Tasks

Group Name	Task Name	Last Executed	Duration	Schedule Info	Rules	Status	Action
CLS_RDM_2	CLS_RDM_2_DefaultValidationTask	09 Aug, 2023 15:39:21	36 sec	Not Configured	WindowsHotfixDetails +28	Failed(2 Pass, 27 Fail)	▶ ⋮

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

To view the Task list perform the following.

1. Click **Monitor** OR **Manage** on the Navigation bar.
2. Click **Recovery Groups** > **Group Name** > **Validation**.
3. Click **Validation Rules** button. The **Task Summary List** window appears.



Manage / RG Listing / Validation Tasks

Validation Tasks

CLS_RDM_2

Group Name	Task Name	Last Executed	Duration	Schedule Info	Rules	Status	Action
CLS_RDM_2	CLS_RDM_2_DefaultValidationTask	09 Aug, 2023 15:39:21	36 sec	Not Configured	WindowsHotfixDetails +28	Failed(2 Pass, 27 Fail)	▶ ⋮

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

The table displays the following information.

Field	Description
Task Name	Displays the task name
Start Time	Displays the start time
End Time	Displays the end time
Execution Count	Displays the execution Count
Execution Status	Displays the execution status

Click the to ▶ view the Description and the Schedule Frequency.

Pre-Requisite:

To view the Task list, a group should be available.

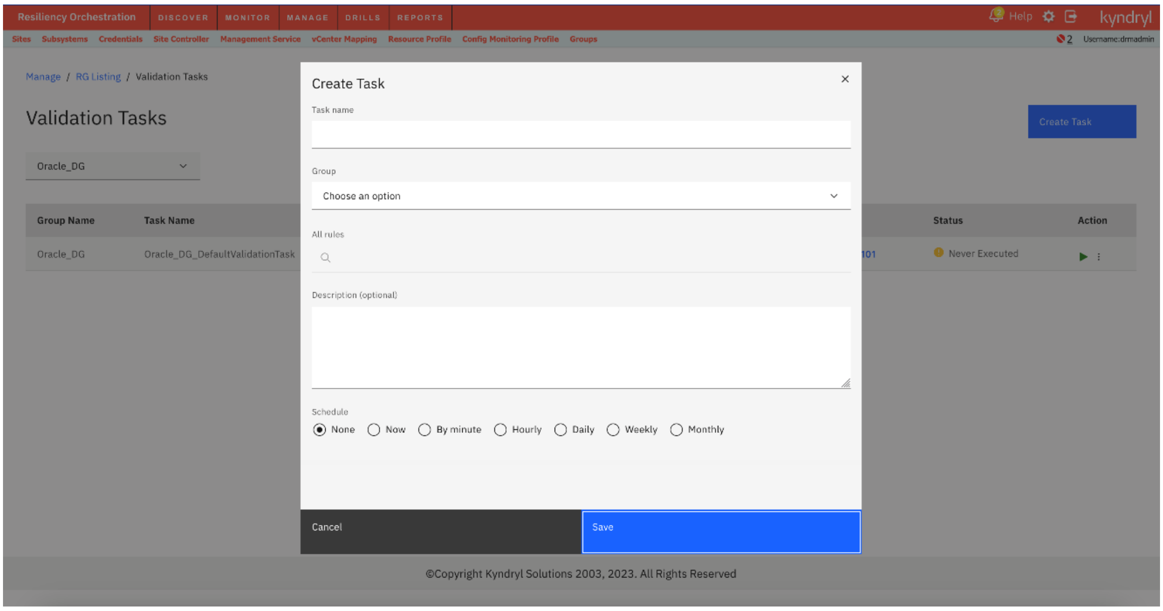
Creating Tasks

To create a task, perform the following steps:

1. Click Manage > Recovery Groups > Group Name > Validation.
2. Click **Validation Rules** button. The **Task Summary List** window appears with the list of tasks for that specific group.

Note: Select Group from the drop-down list to create tasks for a different group.

3. Click the **Create Task** button at the top right corner of the Task window. The **Create Task** window is displayed.
4. Configure the following field elements.



Validation Tasks

Oracle_DG

Group Name	Task Name	Status	Action
Oracle_DG	Oracle_DG_DefaultValidationTask	Never Executed	▶ ⋮

Create Task

Task name

Group: Choose an option

All rules

Description (optional)

Schedule
● None ○ Now ○ By minute ○ Hourly ○ Daily ○ Weekly ○ Monthly

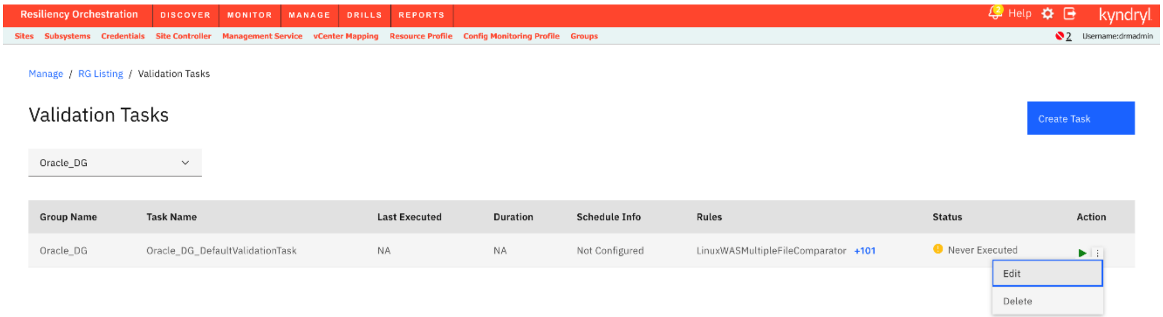
Field	Description
Task Name	Enter a task name. This field is mandatory.
Description	Enter a description for the task.
Group name	Select a group from the drop down list. This field is mandatory.
Selected Rules	▪ Select one or more rules to add into the selected rules window by selecting the rule from All Rules window. ▪ Select one or more rules to remove from the selected rules window by selecting the rule back into the All Rules window.
Schedule	Select the type schedule from the drop down list. ▪ Minutes ▪ Hourly ▪ Daily ▪ weekly ▪ monthly ▪ Now Now

Field	Description
	Now can be used to schedule a task execution, immediately.

5. Click **Save** to add the task.

Modifying Tasks

Click Create Task.



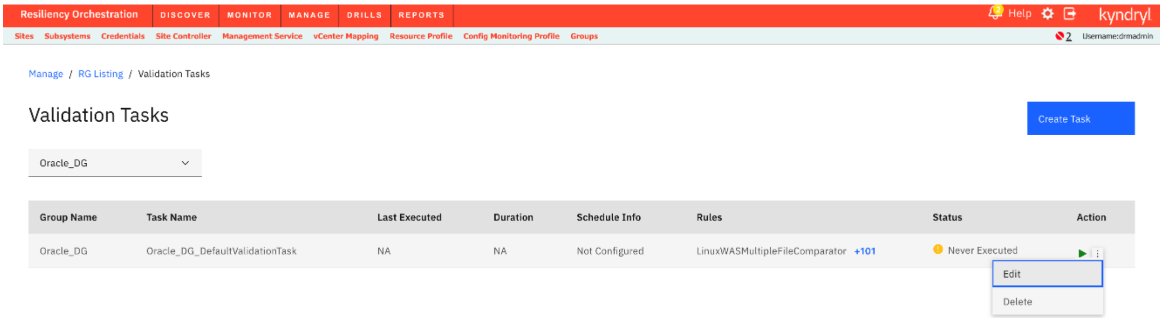
Validation Tasks

Group Name	Task Name	Last Executed	Duration	Schedule Info	Rules	Status	Action
Oracle_DG	Oracle_DG_DefaultValidationTask	NA	NA	Not Configured	LinuxWASMultipleFileComparator +101	● Never Executed	▶ ⋮

Click **Save** to save the modifications.

Deleting Tasks

Click Delete



Validation Tasks

Group Name	Task Name	Last Executed	Duration	Schedule Info	Rules	Status	Action
Oracle_DG	Oracle_DG_DefaultValidationTask	NA	NA	Not Configured	LinuxWASMultipleFileComparator +101	● Never Executed	▶ ⋮

Reports

Reports Overview

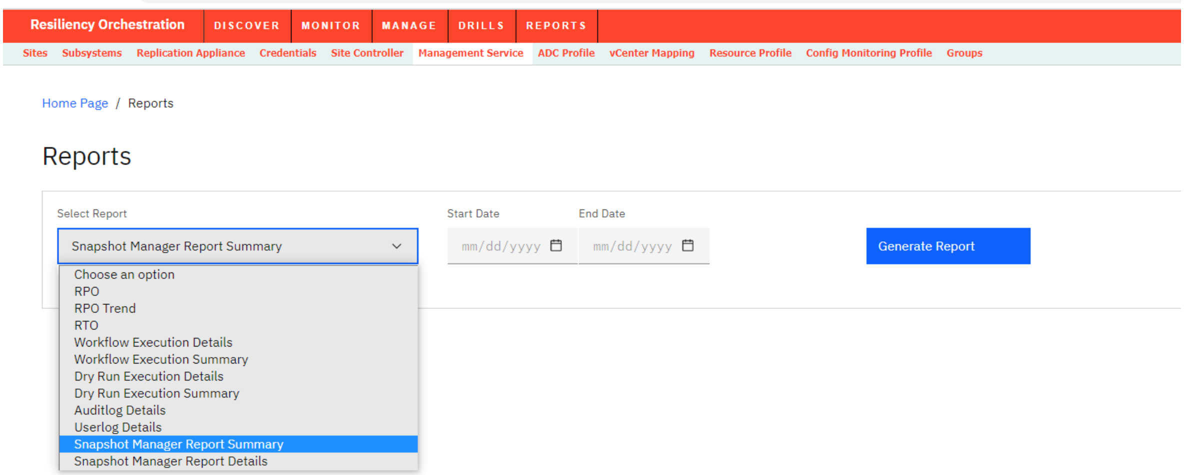
Reports can be generated on various continuity management and monitoring metrics that includes RPO, RTO, and continuity operations for Groups under Kyndryl Resiliency Orchestration.

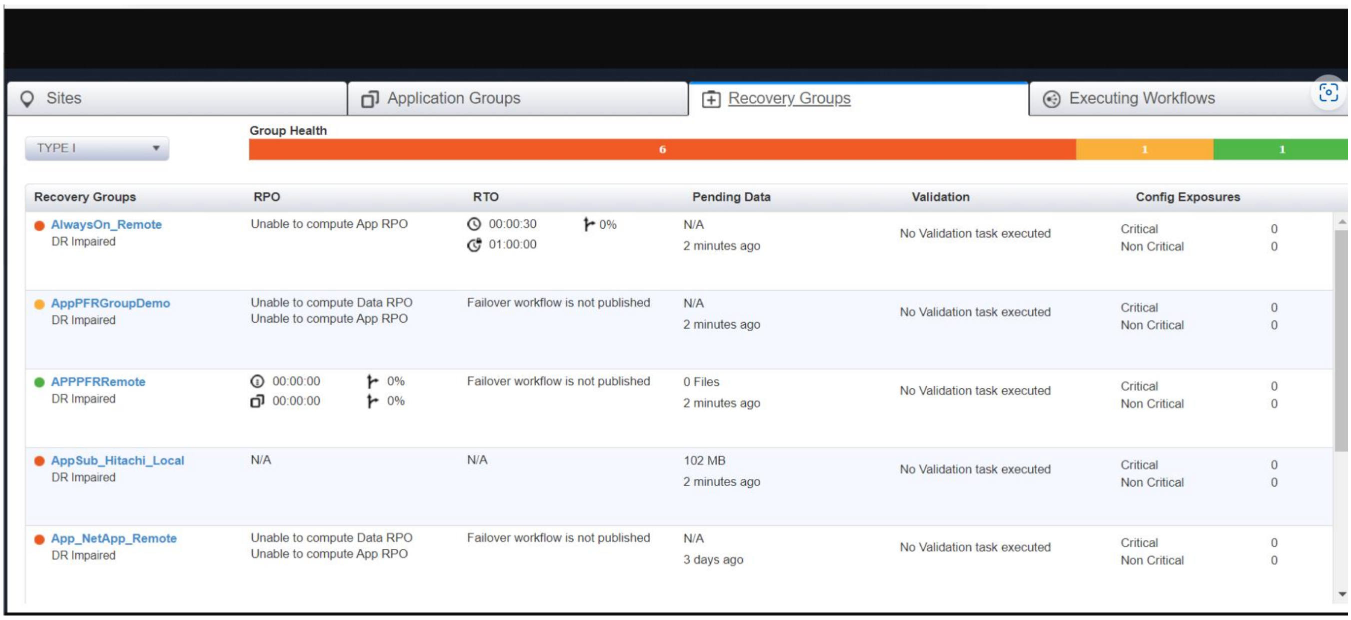
Note: User must allow required popups for generating the corresponding reports.

Browser settings for reports:

- The preferred browser is Chrome.
- If you are using the Firefox browser, enable two settings in Firefox.
  - Print headers and footers.
  - Print backgrounds.

You can generate the following reports:





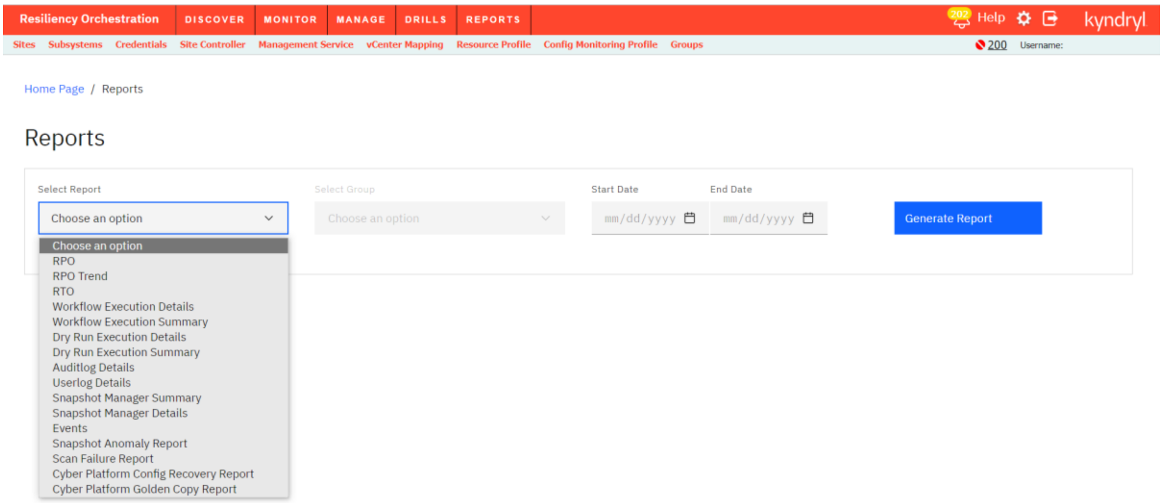
Recovery Groups	RPO	RTO	Pending Data	Validation	Config Exposures	
AlwaysOn_Remote DR Impaired	Unable to compute App RPO	00:00:30 0% 01:00:00	N/A 2 minutes ago	No Validation task executed	Critical Non Critical	0 0
AppPFRGroupDemo DR Impaired	Unable to compute Data RPO Unable to compute App RPO	Failover workflow is not published	N/A 2 minutes ago	No Validation task executed	Critical Non Critical	0 0
APPPFRRemote DR Impaired	00:00:00 0% 00:00:00 0%	Failover workflow is not published	0 Files 2 minutes ago	No Validation task executed	Critical Non Critical	0 0
AppSub_Hitachi_Local DR Impaired	N/A	N/A	102 MB 2 minutes ago	No Validation task executed	Critical Non Critical	0 0
App_NetApp_Remote DR Impaired	Unable to compute Data RPO Unable to compute App RPO	Failover workflow is not published	N/A 3 days ago	No Validation task executed	Critical Non Critical	0 0

RO Module	UI Path	Description/purpose
Reports	Main Home page	Gives the option to Select Report, Select Month, Select Year, and Generate Report.
RPO Report	Reports -> RPO	Generates the report in .csv format.
RPO Trend Report	Reports -> RPO Trend Report	Generates the report in .csv format. Limitation: It currently does not generate the report.
Workflow Execution Report	Reports -> Workflow Execution Report	Generates the report in .csv format.
DryRun Execution Report	Reports -> DryRun Execution Report	Generates the report in .csv format.
RTO Report	Reports -> RTO	Generates the report in .csv format.
Audit Log	Reports -> Audit Log	Generates the report in .csv format.

RO Module	UI Path	Description/purpose
User Log Report	Reports -> User Log	Generates the report in .csv format.
Workflow Execution Summary	Reports -> Workflow Execution Summary	Generates the report in pdf format (Detail reports of each execution also available on clicking of workflow name).
Dryrun Execution Summary	Reports -> Dryrun Execution Summary	Generates the report in pdf format (Detail reports of each execution also available on clicking of workflow name).
Test summary report	Reports -> Test summary report	Generates the report in pdf format.
Group summary report	Reports -> Group summary report	Generates the report in pdf format.
DR drill report	Reports -> DR drill report	Generates the report in .csv format.
Data RPO Report	Reports -> Data RPO report	Generates Report in csv format, showing computed value and % deviation of Data RPO at regular intervals of time, for the given time range.
Snapshot Manager Details	Reports -> Snapshot Manager Details report	Generates a a CSV report, gives a detailed report of all activities captured by the Snapshots Manager for a given duration, it can be configured to email a Point in time report or to send the report at a determined interval.
Snapshot Manager Summary	Reports -> Snapshot Manager Summary report	Generates pdf report.This report gives a summary report of all activities captured by the Snapshots Manager for a given duration, it can be configured to email an Point in time report or to send the report at a determined interval.
BCP Readiness Report	Report-> BCP report	Generates the report in pdf format. Showing executive

RO Module	UI Path	Description/purpose
		summary, DR setup description, Application DR readiness detail and the configured failover recovery steps.

You can generate the following reports:



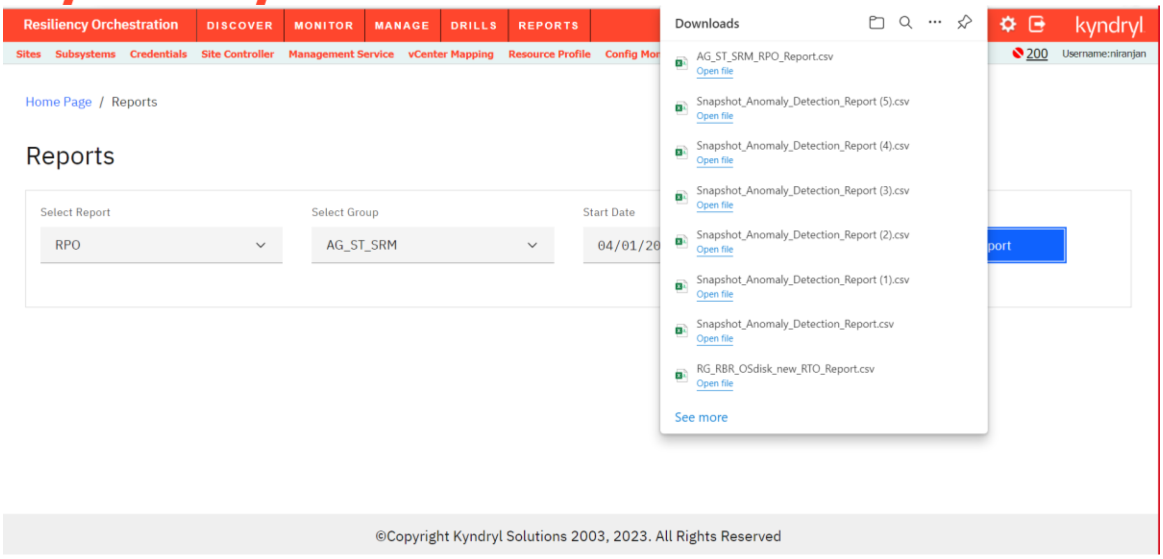
Reports

Select Report

Choose an option

- Choose an option
- RPO
- RPO Trend
- RTO
- Workflow Execution Details
- Workflow Execution Summary
- Dry Run Execution Details
- Dry Run Execution Summary
- Auditlog Details
- Userlog Details
- Snapshot Manager Summary
- Snapshot Manager Details
- Events
- Snapshot Anomaly Report
- Scan Failure Report
- Cyber Platform Config Recovery Report
- Cyber Platform Golden Copy Report

Viewing RPO Report



Reports

Select Report: RPO

Select Group: AG_ST_SRM

Start Date: 04/01/20

AG_ST_SRM_RPO_Report.csv
Open file

Snapshot_Anomaly_Detection_Report (5).csv
Open file

Snapshot_Anomaly_Detection_Report (4).csv
Open file

Snapshot_Anomaly_Detection_Report (3).csv
Open file

Snapshot_Anomaly_Detection_Report (2).csv
Open file

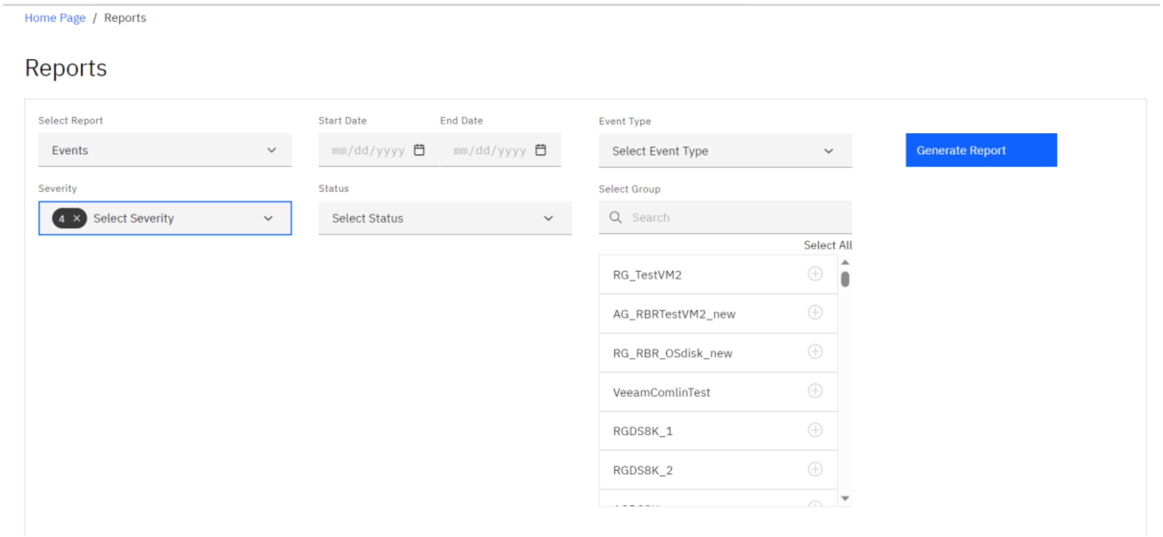
Snapshot_Anomaly_Detection_Report (1).csv
Open file

Snapshot_Anomaly_Detection_Report.csv
Open file

RG_RBR_OSdisk_new_RTO_Report.csv
Open file

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

Viewing Events Report



Reports

Select Report: Events

Start Date: mm/dd/yyyy

End Date: mm/dd/yyyy

Event Type: Select Event Type

Severity: 4 × Select Severity

Status: Select Status

Select Group: Search

RG_TestVM2

AG_RBRTestVM2_new

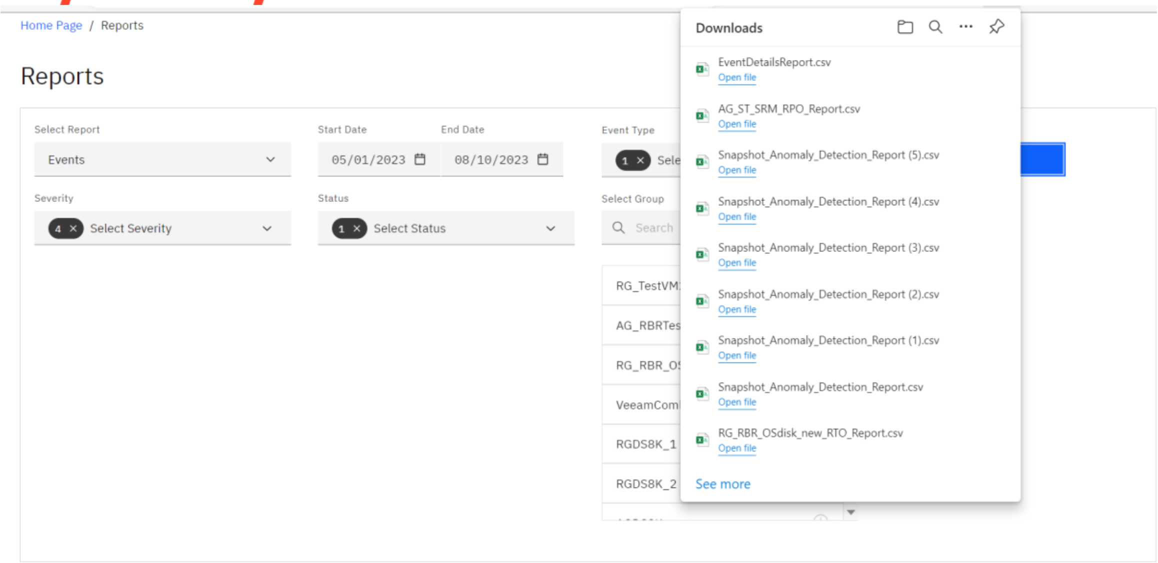
RG_RBR_OSdisk_new

VeeamComlinTest

RGDS8K_1

RGDS8K_2

After selecting all tabs example report generated as below



Home Page / Reports

Reports

Select Report: Events

Start Date: 05/01/2023

End Date: 08/10/2023

Event Type: 1 × Sele

Severity: 4 × Select Severity

Status: 1 × Select Status

Select Group: Search

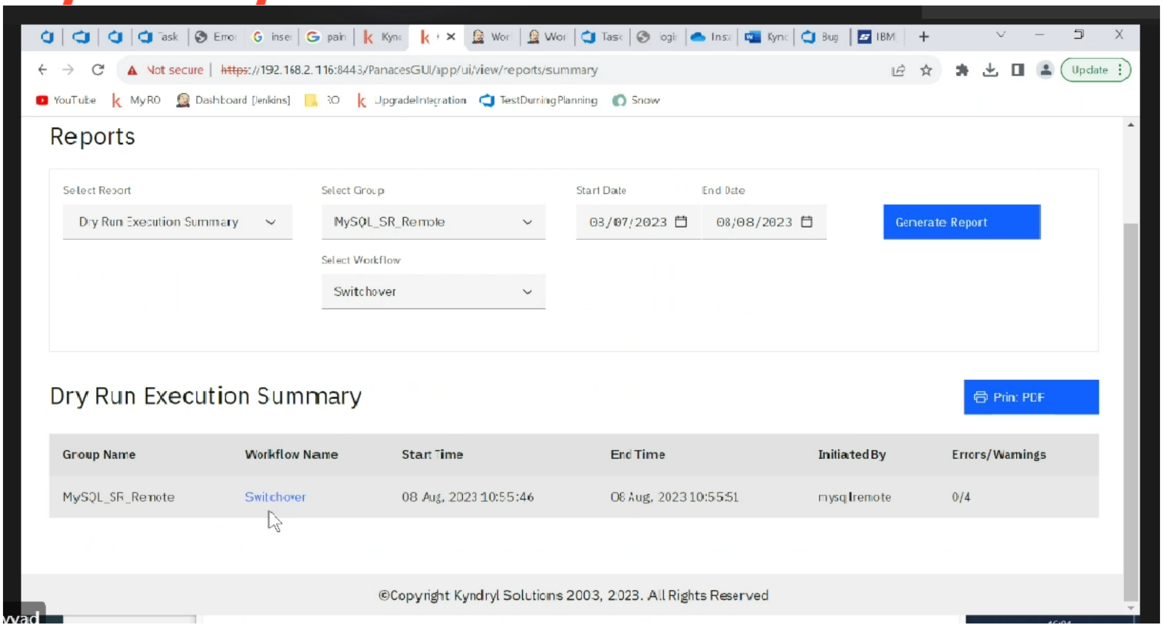
RG_TestVM
AG_RBRTes
RG_RBR_OS
VeeamCom
RGDS8K_1
RGDS8K_2

Downloads

- EventDetailsReport.csv Open file
- AG_ST_SRM_RPO_Report.csv Open file
- Snapshot_Anomaly_Detection_Report (5).csv Open file
- Snapshot_Anomaly_Detection_Report (4).csv Open file
- Snapshot_Anomaly_Detection_Report (3).csv Open file
- Snapshot_Anomaly_Detection_Report (2).csv Open file
- Snapshot_Anomaly_Detection_Report (1).csv Open file
- Snapshot_Anomaly_Detection_Report.csv Open file
- RG_RBR_OSdisk_new_RTO_Report.csv Open file

See more

Viewing Dry Run Report


Not secure | https://192.168.2.116:8443/PanacesGUI/app/ui/view/reports/summary
Update

Reports

Select Report: Dry Run Execution Summary

Select Group: MySQL_SR_Remote

Start Date: 08/07/2023

End Date: 08/08/2023

Select Workflow: Switchover

Generate Report

Dry Run Execution Summary

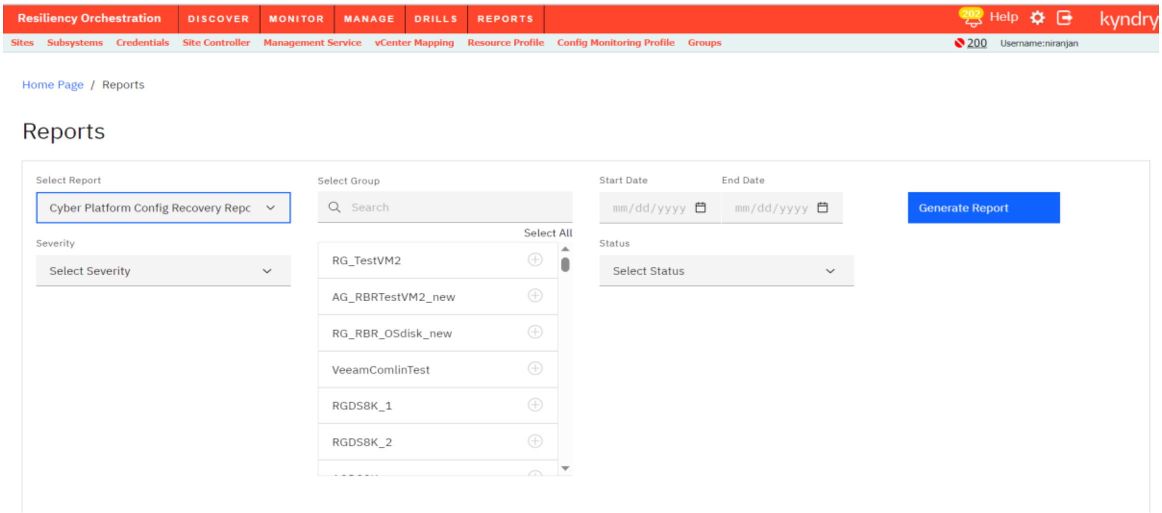
Print PDF

Group Name	Workflow Name	Start Time	End Time	Initiated By	Errors/Warnings
MySQL_SR_Remote	Switchover	08 Aug, 2023 10:55:46	08 Aug, 2023 10:55:51	mysqlremote	0/4

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

Cyber Incident Recovery Reports

Cyber platform config Recovery Report



Reports

Select Report: Cyber Platform Config Recovery Repc

Severity: Select Severity

Select Group: Search

Select All

- RG_TestVM2
- AG_RBRTestVM2_new
- RG_RBR_OSdisk_new
- VeeamComlinTest
- RGDS8K_1
- RGDS8K_2

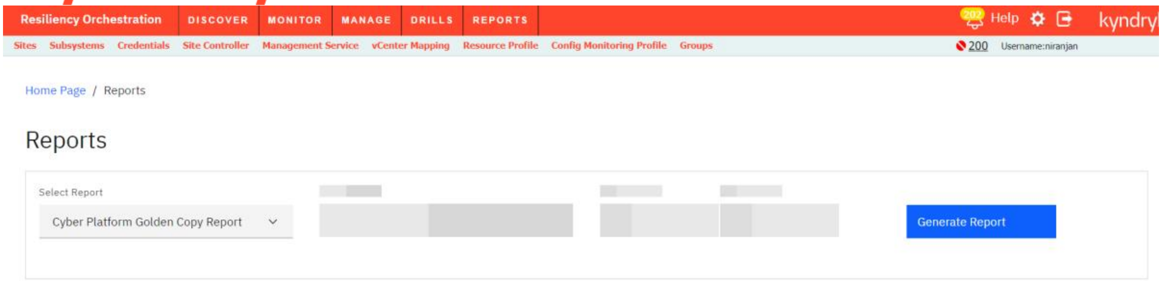
Start Date: mm/dd/yyyy

End Date: mm/dd/yyyy

Status: Select Status

Generate Report

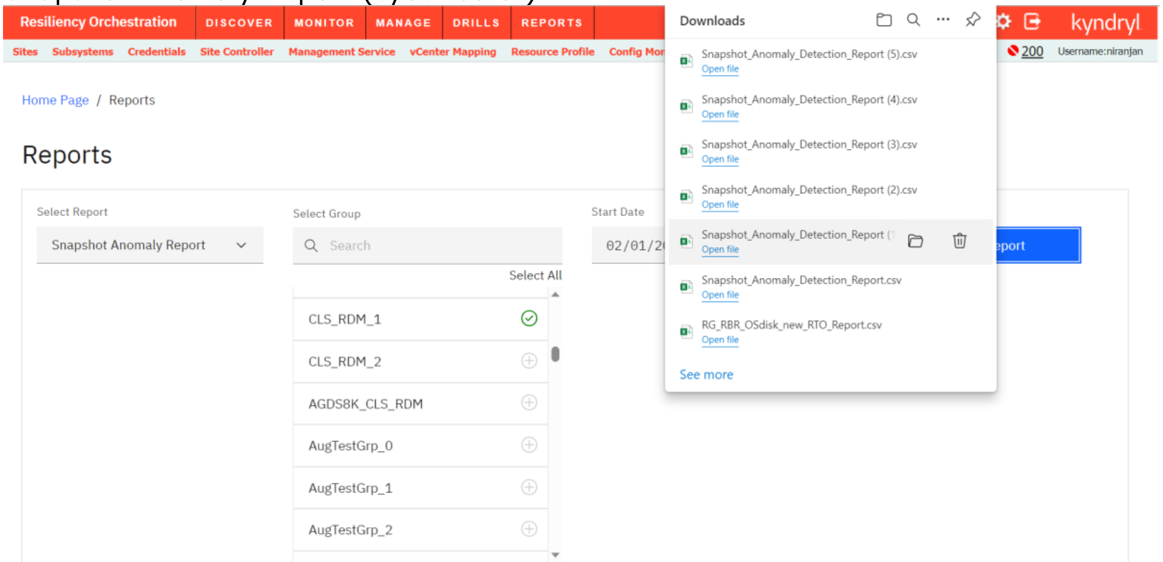
Cyber Platform Golden copy Report



Cyber Platform Golden Copy Report

Cyber Resiliency Data Reports

Snapshot Anomaly Report (cyber data)



Snapshot Anomaly Report

CLS_RDM_1
CLS_RDM_2
AGDS8K_CLS_RDM
AugTestGrp_0
AugTestGrp_1
AugTestGrp_2

02/01/2

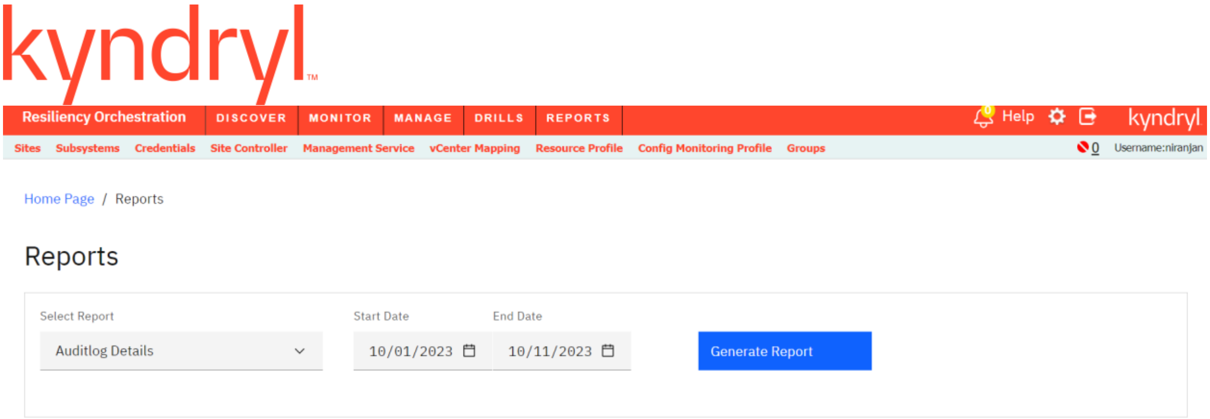
Snapshot_Anomaly_Detection_Report (5).csv
Snapshot_Anomaly_Detection_Report (4).csv
Snapshot_Anomaly_Detection_Report (3).csv
Snapshot_Anomaly_Detection_Report (2).csv
Snapshot_Anomaly_Detection_Report (
Snapshot_Anomaly_Detection_Report.csv
RG_RBR_OSdisk_new_RTO_Report.csv

Viewing Audit Log Report

The following table explains the privileges –

Operations	Basic	Advanced
Viewing Reports	Operator, Administrator and the Super Administrator have the privilege to View Reports.	Operator, Administrator and the Super Administrator have the privilege to View Reports.

To view Audit Log Report (also known as Activity Report), perform the following steps:



Select Report: Auditlog Details

Start Date: 10/01/2023

End Date: 10/11/2023

1. Click **REPORTS** on the navigation bar. The **Reports** page appears.
2. Select **Audit Log** from the list of reports in the **Select Report** drop-down.
3. Select the start and end date and click **Generate Report** The Audit Log report is generated as a pdf and appears in a pop-up window with the requited information.

Discovery

Sites

Setting Up Sites

This chapter describes how to work with sites in the DR environment.

This section explains the following:

Credentials

The following 3 authentication methods are supported for group credential.

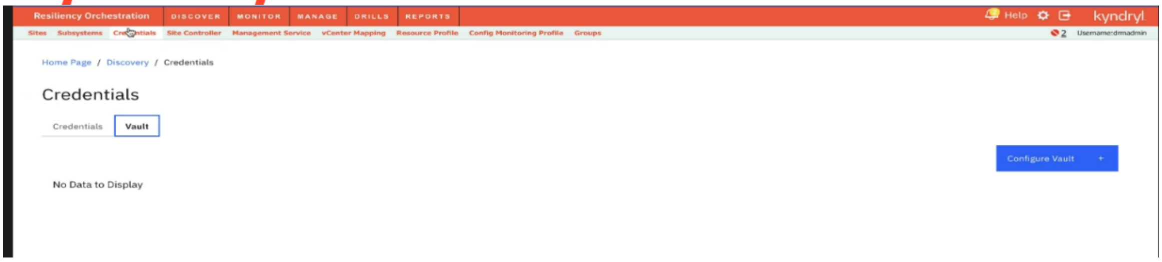
1. Password
2. Vault
3. SSH key

1. Password authentication method:

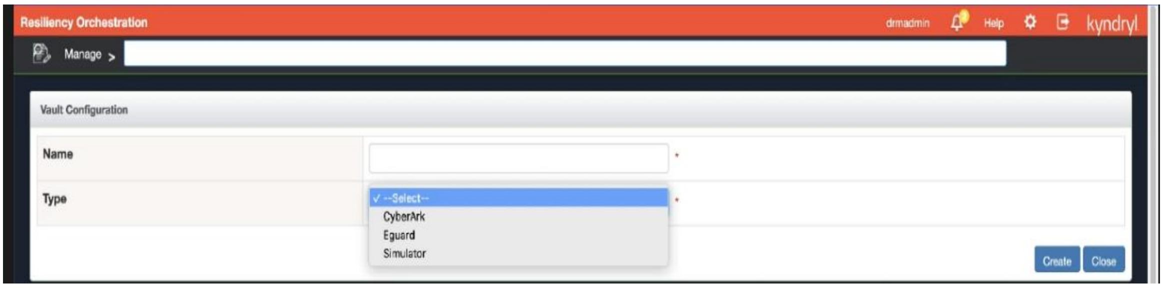
User can provide a password as an authentication method.

2. Vault authentication method:

Click **DISCOVER > Credentials** on the navigation bar**.** The **Credentials** page appears. The Credentials page now allows the creation of new **Credential** and **Vault**.



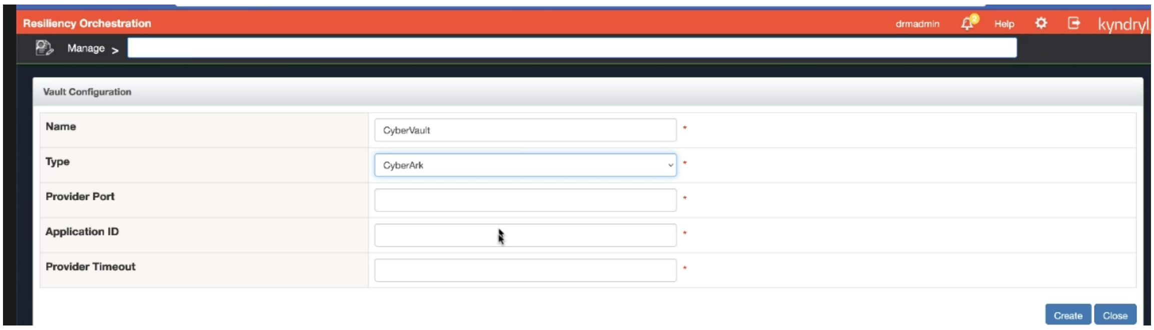
No Data to Display



Create New Vault for CyberArk

To create a new Vault

1. Click **DISCOVER > Credentials** on the navigation bar**.** The **Credentials** page appears.
2. Click on Vault tab
3. Click on Configure Vault button.
4. Click **Create New Vault** link in the top right corner. The **Create Vault** page appears with the following fields:

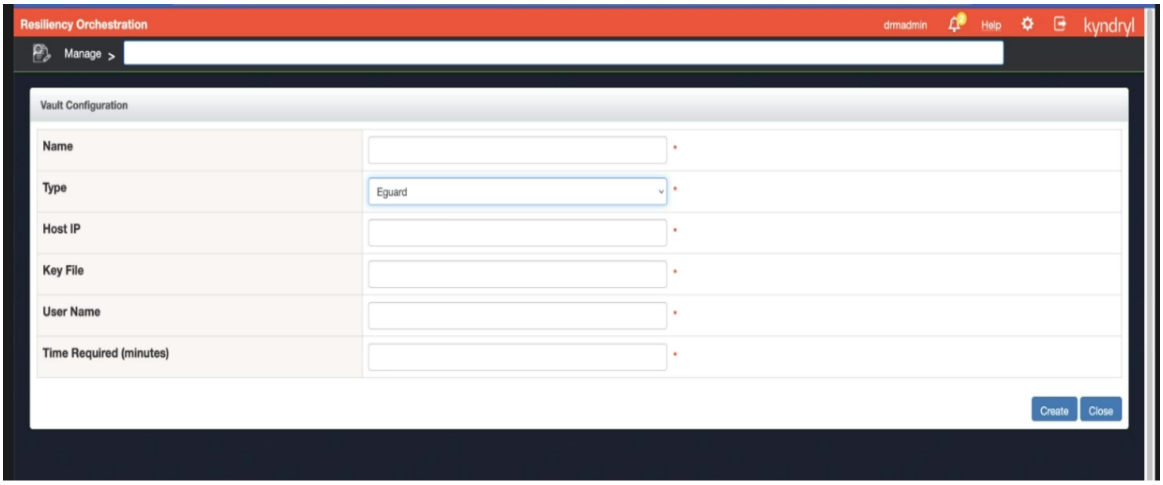


Name	CyberVault *
Type	CyberArk *
Provider Port	*
Application ID	*
Provider Timeout	*

Field	Description
Vault Name	Name that is used to identify a vault.
Vault Type	Select CyberArk from the drop - down list.
Provider Port	Enter the port number on which the provider runs. Default port number is **18923.**
Application ID	Enter the ID that is configured in Cyber-Ark Vault software. Default ID is **ResiliencyOrchestrationApp**.
Provider Timeout	Default provider timeout is **30 seconds**.

3. **Create** to save the vault or **Close** to cancel the vault creation.

Create New Vault for Eguard



Vault Configuration

Name	
Type	Eguard
Host IP	
Key File	
User Name	
Time Required (minutes)	

1. Click **DISCOVER > Credentials** on the navigation bar**.** The **Credentials** page appears.
2. Click **Create New Vault** link in the top right corner. The **Create Vault** page appears with the following fields:

Field	Description
Name	Name that is used to identify a vault.
Type	Select Eguard from the drop down list.

Field	Description
Host IP	Enter the IP address number on which the provider runs.
Key File	Link the key file
User Name	Enter the user name
Time Required (minutes)	

To view the Vault

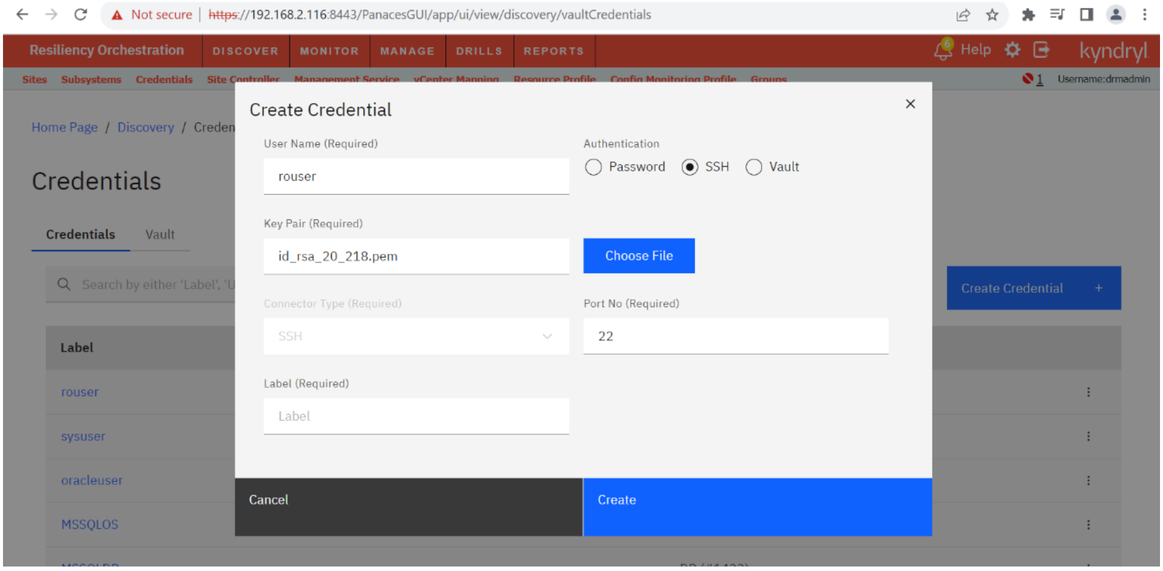
1. Click **DISCOVER > Credentials** on the navigation bar**.** The **Credentials** page appears.
2. Under **Vault List** section, click the **Vault Name** to view the **Vault** details.

To delete a Vault

1. Click **DISCOVER > Credentials** on the navigation bar. The **Credentials** page appears.
2. Click the corresponding **Delete** icon to delete a Vault.

3. SSH key authentication method:

From RO 8.4.4.0 onwards The supported private key files are .pem and .txt to create group credential using SSH key.



Create Credential

User Name (Required): rouser

Authentication: ○ Password ● SSH ○ Vault

Key Pair (Required): id_rsa_20_218.pem

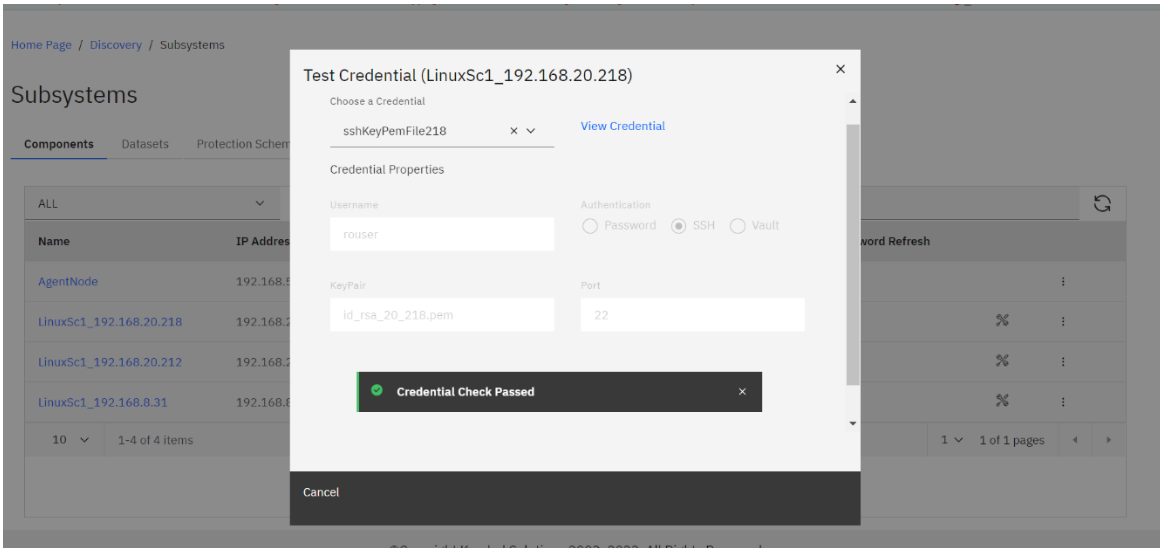
Choose File

Connector Type (Required): SSH

Port No (Required): 22

Label (Required): Label

Cancel | Create



Test Credential (LinuxSc1_192.168.20.218)

Choose a Credential: sshKeyPemFile218

View Credential

Credential Properties

Username: rouser

Authentication: ○ Password ● SSH ○ Vault

KeyPair: id_rsa_20_218.pem

Port: 22

Credential Check Passed

Migration: privatecredmigration script is also supported for SSH key private credential into the named (Group) Credential.

Agent Upgrade

Configuration

When Agentless model is used, Resiliency Orchestration software needs additional configuration.

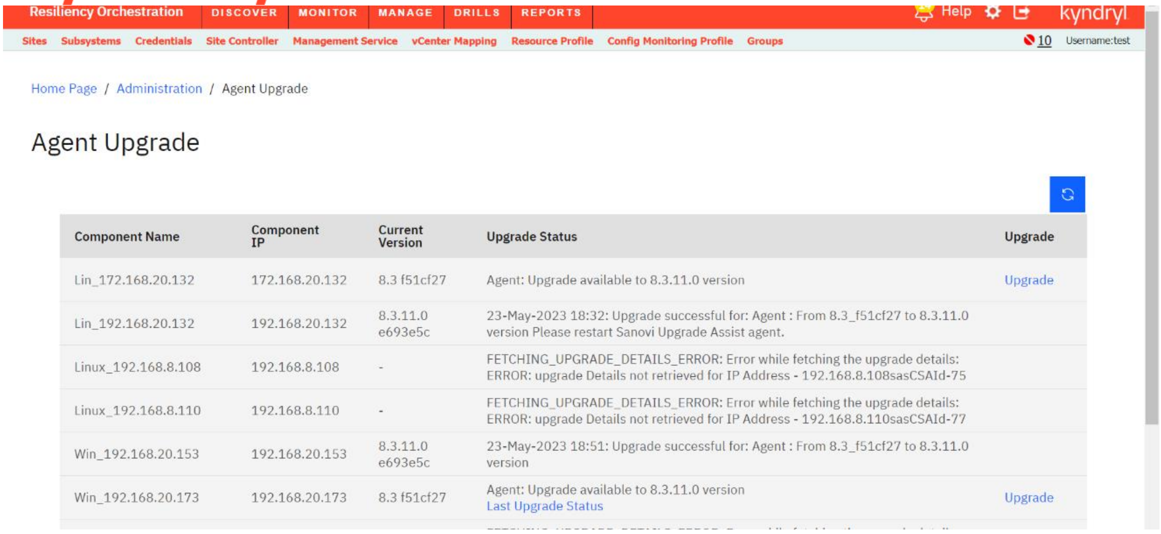
As part of subsystem discovery, user needs to provide additional information which is used to access customer servers remotely. This include credential information to access a customer server. These are described in subsystem discovery page in detail.

If multiple servers can be accessed using same credential information, Resiliency Orchestration provides option to enter the credentials once and then can be attached to any number of subsystems. This is explained under **Credentials.**

To use Kyndryl Resiliency Orchestration as an Agentless model, user needs to discover Resiliency Orchestration server machine as a component and start an agent on the Resiliency Orchestration server system.

Refer to the Management section, to start agent and refer to the Configuration section, to discover a component. Once this step is done, user can go ahead with other subsystems and group discovery.

kyndryl



Home Page / Administration / Agent Upgrade

Agent Upgrade

Component Name	Component IP	Current Version	Upgrade Status	Upgrade
Lin_172.168.20.132	172.168.20.132	8.3 f51cf27	Agent: Upgrade available to 8.3.11.0 version	Upgrade
Lin_192.168.20.132	192.168.20.132	8.3.11.0 e693e5c	23-May-2023 18:32: Upgrade successful for: Agent : From 8.3_f51cf27 to 8.3.11.0 version Please restart Sanovi Upgrade Assist agent.	
Linux_192.168.8.108	192.168.8.108	-	FETCHING_UPGRADE_DETAILS_ERROR: Error while fetching the upgrade details: ERROR: upgrade Details not retrieved for IP Address - 192.168.8.108sasCSAId-75	
Linux_192.168.8.110	192.168.8.110	-	FETCHING_UPGRADE_DETAILS_ERROR: Error while fetching the upgrade details: ERROR: upgrade Details not retrieved for IP Address - 192.168.8.110sasCSAId-77	
Win_192.168.20.153	192.168.20.153	8.3.11.0 e693e5c	23-May-2023 18:51: Upgrade successful for: Agent : From 8.3_f51cf27 to 8.3.11.0 version	
Win_192.168.20.173	192.168.20.173	8.3 f51cf27	Agent: Upgrade available to 8.3.11.0 version Last Upgrade Status	Upgrade

Prerequisites

The following are prerequisites for Agent upgrade:

1. The required ports (mentioned in the following sections) should be opened between the Resiliency Orchestration Server and agents.

2. The user needs chmod 744 permissions to upload binaries to jackrabbit repository.3. Kyndryl Upgrade Assist agent is installed in all the local agent components.4. Kyndryl Upgrade Assist agent is installed in the local machine where Kyndryl Resiliency File Replicator is installed.

Agent upgrade in non-secure mode(http)

Follow these steps:

1. The following ports should be opened between the Resiliency Orchestration Server and agents:

Field	Description
8081	This is the port on which Jackrabbit listens.
8083	This is the port for Jackrabbit RMI connection.

2. RO Panaces.properties ------> set parameter -jackrabbit.https.deployment as **false**.

Agent upgrade in secure mode(https)

Prerequisite:

To identify the dynamic port by Tomcat, use the following command and enable it in the RO server:

```
lsof -i -P -n | grep LISTEN | grep tomcatuser | grep -v 8080 | grep -v 8443 | grep
-v 10443 | grep -v 5099 | grep -v 8005
```

Example of the output of this command:

```
[root@q4rhelrost01 ~]# lsof -i -P -n | grep LISTEN | grep tomcatuser | grep -v 8080
| grep -v 8443 | grep -v 10443 | grep -v 5099 | grep -v 8005
```

```
java 1577299 tomcatuser 243u IPv4 17815178 0t0 TCP *:<PortNumber> (LISTEN)
```

Add the port to the firewall exceptions using the following commands:

```
firewall-cmd --zone=public --add-port=<PortNumber>/tcp --permanent
```

```
firewall-cmd --reload
```

To verify the port after reloading the firewall, execute the following command:

```
firewall-cmd --list-all
```

Follow these steps:

1. The following ports should be opened between the Resiliency Orchestration Server and agents:

Field	Description
10443	This is the port on which Jackrabbit listens.
5099	This is the port for Jackrabbit RMI connection.

2. RO Panaces.properties -----> set parameter -jackrabbit.https.deployment as **true**.

RO upgrade scenario

When you upgrade RO from any lower veriosn to the latest version, then it is recommended to upgrade agents with the http mode.

Once all the agents are upgraded, then change the parameter **jackrabbit.https.deployment = true** in the RO panaces.properties file.

Run **SecurityUsersinjection** script and restart the panaces services.

Note: Panaces restart is required for any change in the panaces.properties file.

Upgrading the Agents

The following table explains each field in the Agent Upgrade page.

Field	Description
Component Name	This displays the name of the component discovered. For Agent, the component name is displayed and for Kyndryl Resiliency File Replicator, the protection schema dependent component name is displayed.
Component IP	This displays the IP address/name of the component.
Current Version	This displays the version of the Agent or Kyndryl Resiliency File Replicator. **Note** Agent version is displayed if only the Agent is installed in the component. Agent version is displayed if Agent and Kyndryl Resiliency File Replicator both are installed in the component. Kyndryl Resiliency File Replicator version is displayed if only Kyndryl Resiliency File Replicator is installed (no local agent is installed) in the component. If Kyndryl upgrade assist agent is not running then "-" is displayed.

Field	Description
Upgrade Status	This displays the upgrade information whether it is: **Upgrade available** If the required binaries are available in the repository. **Upgrade needed** If Agent/ Kyndryl Resiliency File Replicator version is lesser than Kyndryl Resiliency Orchestration version, and Kyndryl Resiliency Orchestration version agent/ Kyndryl Resiliency File Replicator binaries are not available in repository. **Upgraded** if already agent/ Kyndryl Resiliency File Replicator version is equal to Kyndryl Resiliency Orchestration version. Click on the link **Last Upgrade Status** to view the details. This displays the last upgrade information for the component. Upgrade status can be successful or can display an error message, if any error has occurred during the upgrade. If the upgrade has failed then the rollback status will also be displayed in upgrade status. N/A will be displayed if no upgrades are done on the component. **Note** If there is any error with the repository or Kyndryl Upgrade Assist, an appropriate error message is displayed.
Upgrade	**Agent and Kyndryl Resiliency File Replicator are installed in component:** The upgrade button should be displayed only if the Agent and Kyndryl Resiliency File Replicator are in **Upgrade available** state. **Note** If either of the state is in **upgraded/upgrade needed,** the upgrade button will not be displayed. **If only the Agent is installed in the component:** The upgrade button should be displayed only if the of Agent is in **Upgrade available** state. Kyndryl Resiliency File Replicator upgrade is not applicable. **If only the Kyndryl Resiliency File Replicator is installed in component:** The upgrade button should be displayed only if the Kyndryl Resiliency File Replicator is in **Upgrade**

Field	Description
	available state. Agent upgrade is not applicable.

The following are steps to upload binaries in the Jackrabbit repository for low touch agent upgrade:

1. Download the agent binary files to Kyndryl Resiliency Orchestration Server in the following folder in zip format:

   $EAMSROOT/upgrade/cli/installer_binaries

   For PFR, copy the Kyndryl Resiliency File Replicator Services installer files in zip format in the above location.

   For Example: Copy Windows64_DRMAgent_8.1.zip and Windows64_PFR_8.1.zip files to the $EAMSROOT/upgrade/cli/installer_binaries/ folder.
2. Run the UploadClient.sh script in the following folder:

   $EAMSROOT/upgrade/cli/bin/

   When the script is executed, the UpgradeAssist prompt displays.
3. Enter the string **help** at the UpgradeAssist prompt to display the help for using the UpgradeAssist tool.

4. Run the following command to upload the installer files.

   ```
   upload_installer_files
   ```

   For Example: When the command upload_installer_files is executed successfully, the following success message displays:

   ```
   Files are uploading. It will take few minutes. Please wait...
   Upload status:
   Windows64_DRMAgent_8.1.zip installer file successfully uploaded in the repository
   ```

5. Select **Admin > Go to Agent Upgrade**. The upgrade button should be enabled by default.
6. Click the upgrade button corresponding to the agent to upgrade the agent.

   Note:

   - The readme file, which includes information to upload binaries in the Jackrabbit repository for low touch agent upgrade is available in the following folder: /opt/panaces/upgrade/cli/installer_binaries/
   - PFR service pack upgrade needs to be done using either PFR installer or low touch upgrade (Upgrade Asist feature).

Note –

If you notice the below exception during Agent Upgrade --

ROAGENT_UPGRADE_ERROR: Resiliency Orchestration Agent Upgrade failed with error message: Runtime Error: Please retry later, Remark
: REPOSITORY_ERROR: Unknown Repository error: java.rmi.ConnectException: Connection refused to host: 127.0.0.1; nested exception is:

Follow these corrective steps -

1. Ensure that first line added in /etc/hosts/ file by Resiliency Orchestration Installer -
   <Server_IP> localhost <hostname>

is modified to

<Server_IP> <hostname> <hostname>

For example –

The first line in /etc/hosts may be

192.168.5.91 **localhost** stlnro91

This should be changed to

192.168.5.91 **stlnro91**

2. Restart the Resiliency Orchestration server services.

Limitation

1. After AIX and Linux local agent upgrade using the **Agent Upgrade** page in Kyndryl Resiliency Orchestration UI, even though the upgrade is successful, there is an error message displayed (socket communication error) and the **Upgrade** button is still visible in the **Agent Upgrade** page. It is expected that after successful upgrade, the **Upgrade** button should not be available for users.
2. After upgrading Kyndryl Resiliency File Replicator (PFR) agent using low touch agent upgrade, even though the agent upgrade is successful, there is an error message displayed.

Replicationset Name	Replication set name which you have created on replication server.
HOST IP	Enter the replication host IP Address. For primary protection scheme, enter the source host IP Address and for DR protection scheme, enter the target IP Address.
SBRROOT	Enter the SBRROOT path for Kyndryl Resiliency Orchestration server.
Volumes	Enter the volume name.

	To enter the multiple volume names, separate each name by a comma.

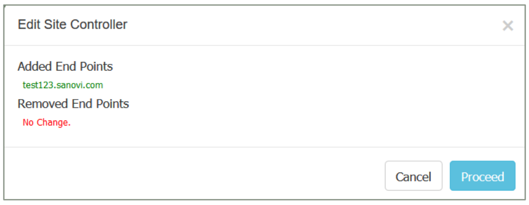
3. Click **Save** to save the entered details to complete protection scheme setup.

a.

Example – rhel1234.sanovi.com

2. Click **Save**. The changes are saved and a confirmation message is displayed.
3. Click **Proceed** to make the changes.

The IP addresses (list/range/CIDR) added and removed during the edit is displayed in the confirmation message as shown in the sample figure below.



Edit Site Controller

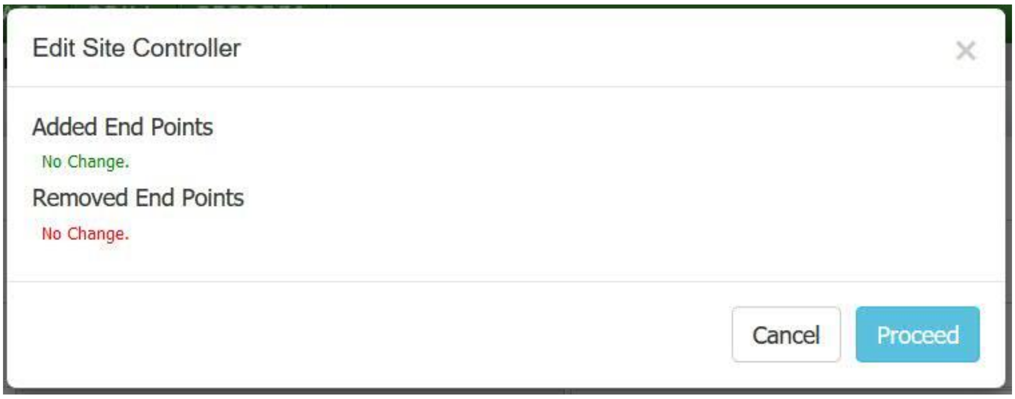
Added End Points

test123.sanovi.com

Removed End Points

No Change.

If there is no change in IP address list (neither added nor removed) during the edit, then a confirmation message stating the same is displayed as shown in the figure below.



Edit Site Controller

Added End Points

No Change.

Removed End Points

No Change.

When Site Controller mapping is modified, the changes are not reflected immediately. For the changes to take effect, the following steps needs to be followed:

1. Move the respective group to MAINTENANCE
2. Edit the component, change the component to Local Agent (by unchecking Server Managed Remotely) and save the component.

3. Again Edit the component, change the component to Remote Agent (by checking Server Managed Remotely and providing credentials) and save the component. This will take the latest Agent Node mapping configured.
4. You should not map Management service with Site Controller.
5. Before removing an IP from a Site Controller mapping, move the component to UNMANAGED. Then remove the IP (for procedure, refer Editing Site Controller) and then move the component to MANAGED. This is applicable only for Remote agents.

Removing Site Controller

You need to perform the following steps to remove Site Controller:

1. Log in to Kyndryl Resiliency Orchestration server with administrative privileges.
2. Select **Discover > Site Controller**. The **Site Controller Mapping** page is displayed
3. Click the delete icon 🗑 corresponding to the Site Controller mapping. The Site Controller mapping is deleted.

Converged

Converged infrastructure packages multiple information technology (IT) components into a single, optimized computing solution. Components of a converged infrastructure solution include servers, data storage devices, networking equipment and software for IT infrastructure management, automation and orchestration.

This chapter describes how to work with UCS Directors and UCS Director DR Map for DR.

UCS Directors

Cisco UCS Director unifies and automates end-to-end IT converged infrastructure management processes by abstracting the complexity of individual devices, hypervisors, and virtual machine.

UCS Directors section explains the following:

Adding UCS Directors

Modifying UCS Directors

Deleting UCS Directors

Listing UCS Directors

UCS Director DR Map for DR

Virtual Data Centre (vDC) Map for DR is used to configure Kyndryl Resiliency Orchestration on which vDC on the DR site should the resources be allocated for DR for a given VM on the primary. This map needs to be created for each vDC on the primary for which DR might be needed.

UCS Director DR Map for DR section explains the following:

Adding UCS Director vCD Map for DR

Deleting UCS Director vCD Map for DR

Listing UCS Director vCD Map for DR

UCS Directors

Adding UCS Directors

Refer **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

To add a new UCS director in the existing DR environment, perform the following steps:

1. Click **DISCOVER > Converged** tab on the navigation bar. The **Converged** page appears with the following configured values.
   - NAME
   - SITE
   - CREDENTIAL STATUS

   Click **Add UCS Director** link at the top right corner of the **Converged** page should navigate to 'Add UCS Director' page.

   Configure the following field elements.

Field	Description
Name	Provide a unique name to the UCS Director being created. This field is mandatory. **Note:** This field accepts up to 32 alphanumeric characters, spaces and underscores. The UCS Director name can start with an alphabet.
SITE	Select the Site from the drop-down list.

Field	Description
Access Key	To obtain the Access key: ▪ Login to CISCO UCS Director ▪ click on Admin link, select the User information window. ▪ Click on the **Copy key button** from the Advanced tab, to copy the access key. ▪ Paste the Access key in Kyndryl Resiliency Orchestration server's **Add** UCS director page.
SERVER IP	Provide the UCS Director IP Address.

2. Click on **Test Credentials** to test the credentials entered.
3. Click **Save** to add the UCS director account.

   OR
   Click **Cancel** to quit the current operation.
4. On successfully adding the UCS Director, a message box is displayed.
5. Click **OK** in the message box to return to the UCS Director List page.

Modifying UCS Directors

Refer **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges

To modify a UCS director, perform the following steps:

1. Click **DISCOVER > Converged** tab on the navigation bar. The **Converged** page appears with the following configured values.
   1. NAME
   2. SITE
   3. CREDENTIAL STATUS
2. Click ✎ icon corresponding to the UCS Director that you want to modify. This opens **Edit UCS Director** page. The UCS Director details cannot be modified by users with Operator privileges. Refer **Adding UCS Directors** for field description.

   Note:

   Site and UCS Director name cannot be modified.

3. Make the required changes in the relevant field.
4. Click **Save** to save the modifications.
   OR
   Click **Go Back** to return to the **UCS DIRECTOR LIST** page.
5. Click **OK** to return to the UCS Director List Page.

Management Service

Adding Management Service

.

Site controller support for vCenter and Zerto Management Service

Map the vCenter IP address and the Zerto IP address with the Linux Site Controller IP address (in Site Controller page, refer Site Controller Configuration) to run the vCenter and Zerto agent on that Site Controller, and then do the discovery of the vCenter/ Zerto Management Service.

This is only an option. You can continue to run the vCenter and Zerto agents on Resiliency Orchestration itself, by discovering vCenter and Zerto Management Service directly without mapping the vCenter and Zerto IPs to any Site Controller.

Ensure that the Site of both the Site Controller and the Management Services are the same.

Steps to create Management Service in Zerto

You need to perform the following steps to create a new Management service with service type VCenter in the existing DR environment:

In Kyndryl Resiliency Orchestration, vCenter can be discovered using their IP address or name (which could be a hostname or a fully qualified domain name (FQDN)).

Cred migration script to extend to support management service creds

```
[root@rhelagents58 installconfig]# cd ../bin/
[root@rhelagents58 bin]# ./PrivateCred2GroupCredMigrator.sh -help
This script will convert the private credential to named credential

Syntax: script-name

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

To convert the credential for specific/set of component(s) and it's dataset(s) &
service(s)/management services...
```

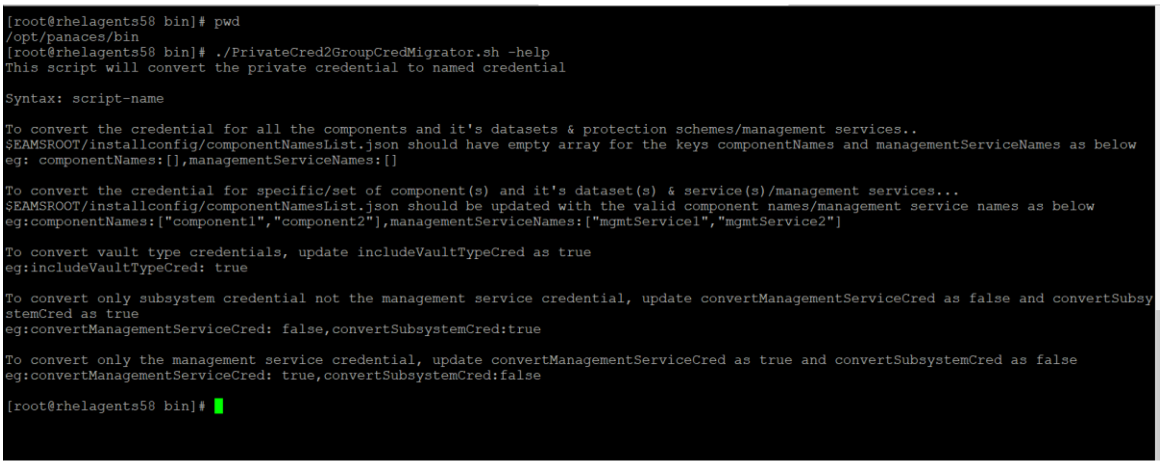
$EAMSROOT/installconfig/componentNamesList.json should be updated with the valid component names/management service names as below
eg:componentNames:["component1","component2"],managementServiceNames:["mgmtService1","mgmtService2"]

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

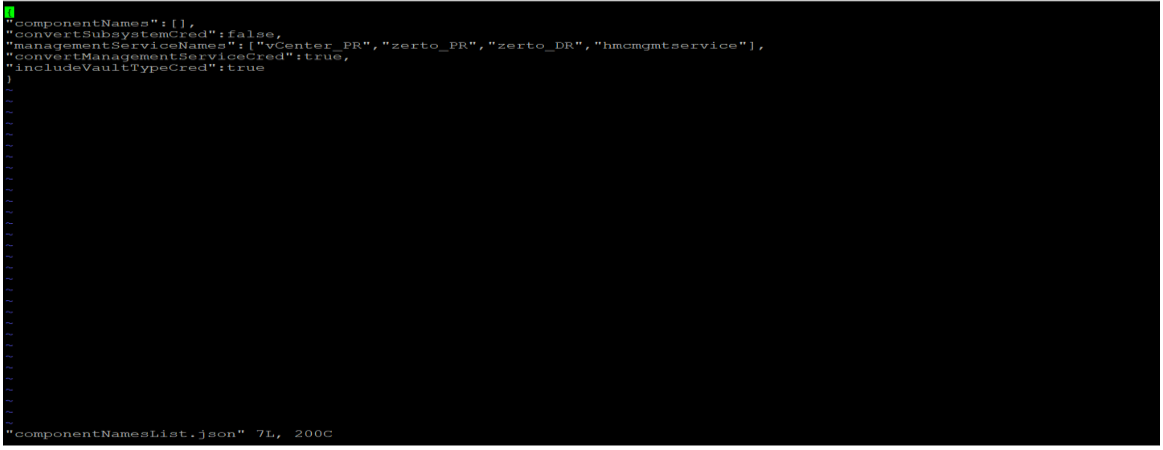
To convert only subsystem credential not the management service credential, update convertManagementServiceCred as false and convertSubsystemCred as true
eg:convertManagementServiceCred: false,convertSubsystemCred:true

To convert only the management service credential, update convertManagementServiceCred as true and convertSubsystemCred as false
eg:convertManagementServiceCred: true,convertSubsystemCred:false

```
[root@rhelagents58 bin]# pwd
/opt/panaces/bin
[root@rhelagents58 bin]#
```



```
[root@rhelagents58 bin]# pwd
/opt/panaces/bin
[root@rhelagents58 bin]# ./PrivateCred2GroupCredMigrator.sh -help
This script will convert the private credential to named credential

Syntax: script-name

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

To convert the credential for specific/set of component(s) and it's dataset(s) & service(s)/management services...
$EAMSROOT/installconfig/componentNamesList.json should be updated with the valid component names/management service names as below
eg:componentNames:["component1","component2"],managementServiceNames:["mgmtService1","mgmtService2"]

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

To convert only subsystem credential not the management service credential, update convertManagementServiceCred as false and convertSubsy
stemCred as true
eg:convertManagementServiceCred: false,convertSubsystemCred:true

To convert only the management service credential, update convertManagementServiceCred as true and convertSubsystemCred as false
eg:convertManagementServiceCred: true,convertSubsystemCred:false

[root@rhelagents58 bin]#
```



```
{
"componentNames":[],
"convertSubsystemCred":false,
"managementServiceNames":["vCenter_PR","zerto_PR","zerto_DR","hmcmgmtservice"],
"convertManagementServiceCred":true,
"includeVaultTypeCred":true
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"componentNamesList.json" 7L, 200C
```

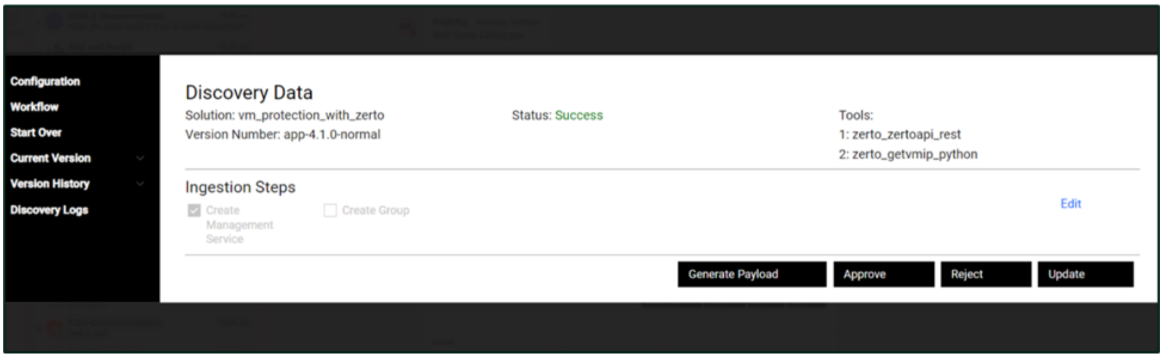
Management service

Discover the following services for primary and DR:

- vCenter Management service.
- Zerto Management service

Note: Ensure to register vCenter Management Service first and then Zerto Management Service to get the correct mapping between vCenter and Zerto.

1. Select the **Create Management Service** in the **Ingestion Steps** and click **Approve.**
2.



Discovery Data

Solution: vm_protection_with_zerto

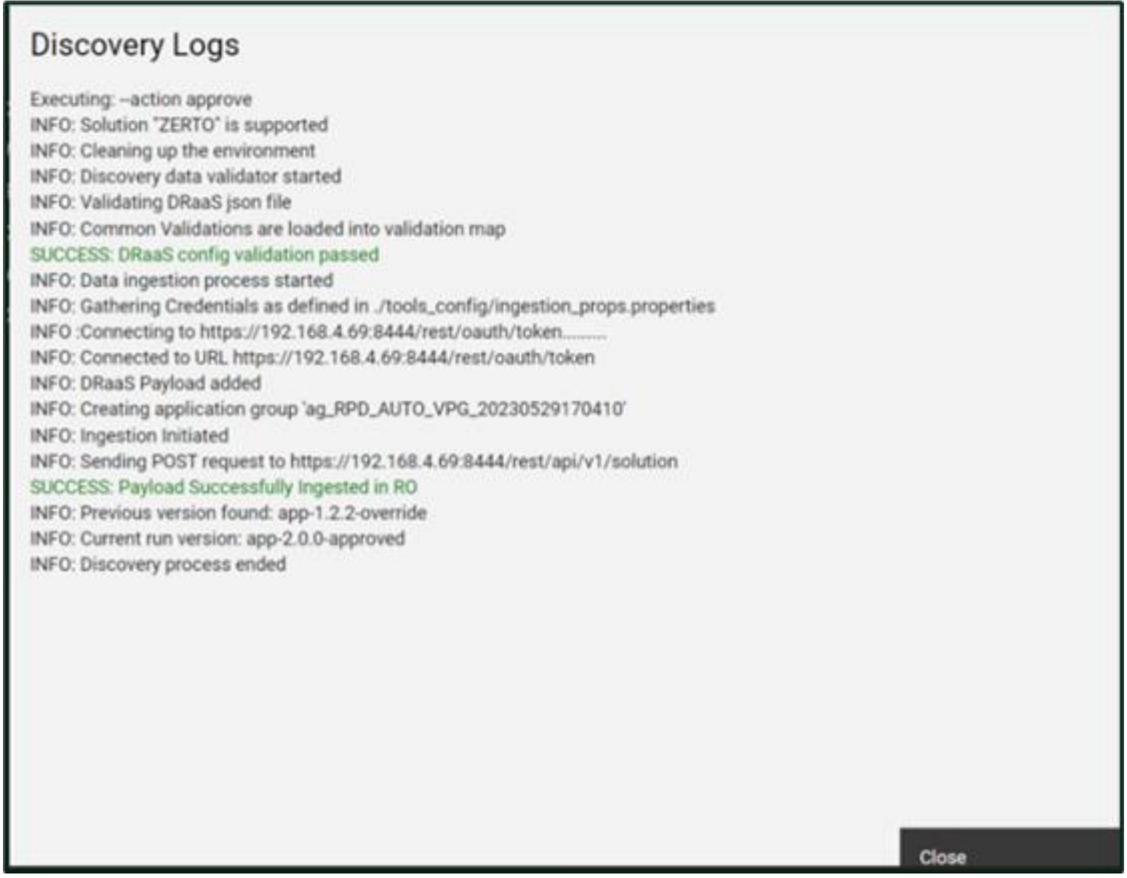
Version Number: app-4.1.0-normal

Status: Success

Tools:
1: zerto_zertoapi_rest
2: zerto_getvmip_python

Ingestion Steps

☑ Create Management Service ☐ Create Group



```
Executing: –action approve
INFO: Solution "ZERTO" is supported
INFO: Cleaning up the environment
INFO: Discovery data validator started
INFO: Validating DRaaS json file
INFO: Common Validations are loaded into validation map
SUCCESS: DRaaS config validation passed
INFO: Data ingestion process started
INFO: Gathering Credentials as defined in ./tools_config/ingestion_props.properties
INFO :Connecting to https://192.168.4.69:8444/rest/oauth/token.........
INFO: Connected to URL https://192.168.4.69:8444/rest/oauth/token
INFO: DRaaS Payload added
INFO: Creating application group 'ag_RPD_AUTO_VPG_20230529170410'
INFO: Ingestion Initiated
INFO: Sending POST request to https://192.168.4.69:8444/rest/api/v1/solution
SUCCESS: Payload Successfully Ingested in RO
INFO: Previous version found: app-1.2.2-override
INFO: Current run version: app-2.0.0-approved
INFO: Discovery process ended
```

Verify if the Management Service is created by navigating to Kyndryl RO and click **Close.**

The sequence of registering the Management Service is mandatory for the correct configuration of Zerto environment.

Site controller support for vCenter and Zerto management service

Map the vCenter IP address and the Zerto IP address with the Linux Site Controller IP address on the **Site Controller** page (refer to **Site Controller Configuration** topic in the Kyndryl Resiliency Orchestration Administrator's guide) to run the vCenter and Zerto agents on that Site Controller, and then do the discovery of the vCenter / Zerto Management Service.

This is only an option. You can continue to run the vCenter and Zerto agents on Resiliency Orchestration itself, by discovering vCenter and Zerto Management Service directly without mapping the vCenter and Zerto IPs with any Site Controller.

Ensure that the Site of both the Site Controller and the Management Services are the same**.**

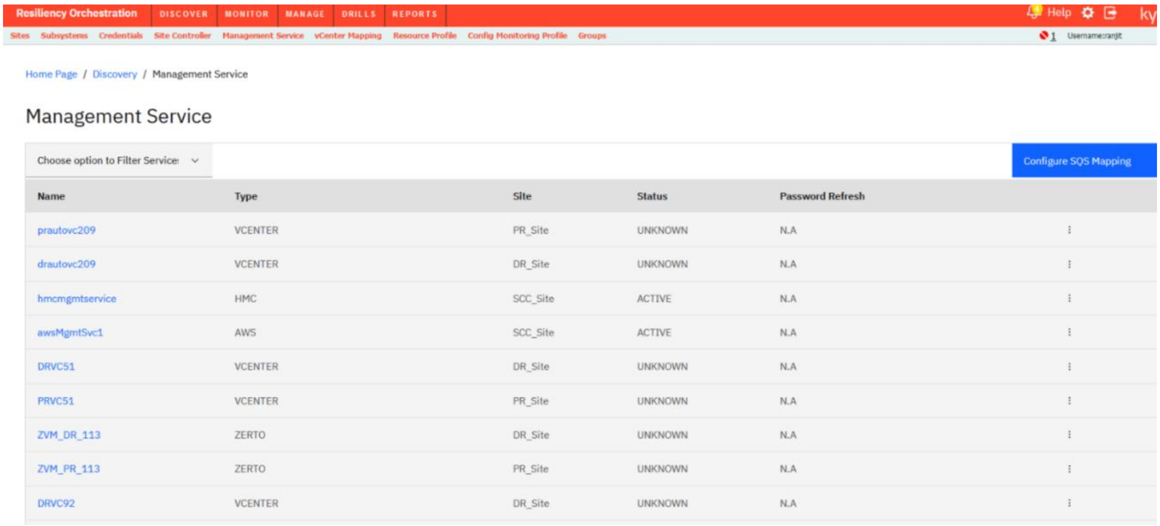
Deleting Management Service

Note: Now you can delete the Management Service through AD2C.

Management Service List

.

To view the Management Service created or available in a DR environment, click **DISCOVER > Management Service** on the navigation bar.



Management Service

Name	Type	Site	Status	Password Refresh
prautovc209	VCENTER	PR_Site	UNKNOWN	N.A
drautovc209	VCENTER	DR_Site	UNKNOWN	N.A
hmcmgmtservice	HMC	SCC_Site	ACTIVE	N.A
awsMgmtSvc1	AWS	SCC_Site	ACTIVE	N.A
DRVC51	VCENTER	DR_Site	UNKNOWN	N.A
PRVC51	VCENTER	PR_Site	UNKNOWN	N.A
ZVM_DR_113	ZERTO	DR_Site	UNKNOWN	N.A
ZVM_PR_113	ZERTO	PR_Site	UNKNOWN	N.A
DRVC92	VCENTER	DR_Site	UNKNOWN	N.A

The **Management Service List** page displays following details in a tabular form:

Field	Description
Name	Displays the name of the management service.
TYPE	Displays the type of the management service.
Site	Displays the name of the site.
Status	Displays the status of the site. Status can be ACTIVE, INACTIVE, UNKNOWN.

The **Discover Details List** page displays following details in a tabular form:

Discover Instance for AWS:

Field	Description
Instance Name	Displays the name of the AWS instance.
Instance ID	Displays the id of the AWS instance.
Instance PRIVATE IP	Displays the name of the site.

1. Select the check box.
2. Click **Save VM** to save the AWS Instances.
3. On successfully adding the AWS instance, a message box is displayed.
4. Click **OK** in the message box to return to the Management Service List page.

Discover Images for AWS: Amazon machine images.

Field	Description
AWS IMAGE Name	Select the image
AWS IMAGE ID	Enter the image id.
AWS IMAGE IP	Enter the image ip.

1. Click **Save image** to save the image.
2. On successfully adding the AWS image , a message box is displayed.
3. Click **OK** in the message box to return to the Management Service List page.

Note: If vCenter IP/Name is changed, all related groups must be deleted.

vCenter Mapping

vCenter mapping in Kyndryl Resiliency Orchestration is used to manage the mapping between the Primary and Destination (Disaster Recovery (DR)/Cyber Recovery (CR)) vCenters, including Data Centers, Clusters, ESX and Resource Pools. It also helps in defining the network ports and storage devices.

The resource mapping will be leveraged for finding out the resources to be leveraged for performing recovery and drill operation. The vCenter mapping will help user to define the mapping for DR & CR recovery purpose.

vCenter Mapping provides the following features under different tabs -

Cluster Mapping - This tab provides ability to map PR vCenter to Destination (DR/CR) vCenter and Data Center mapping. Based on the vCenter mapping, user can either define Cluster/ESX mapping. User can also define the Resource Pool mapping (non-mandatory) based on the cluster/ESX mapping.

Port group Mapping - This tab enables user to perform Network/port group mapping between the Primary and DR sites.

Placeholder Datastore - This tab helps user to assign the specific placeholder data stores to the vCenter and ESX.

This mapping is a mandatory pre-requisite for all VM based solutions ex. DR (VM to VM) & CR supported in Kyndryl Resiliency Orchestration.

Limitation - User can define one vCenter mapping for DR purpose and one vCenter mapping for CR purpose for the same PR vCenter. Each PR site can have only one DR mapping and one CR mapping. Adding second mapping of same purpose for the same PR vCenter has limitations.

The following snippet displays the logical mapping between vCenter Datacenter clusters:

(vCenter1-Datacenter1-Cluster1 [--->] vCenter2-Datacenter2-Cluster2)

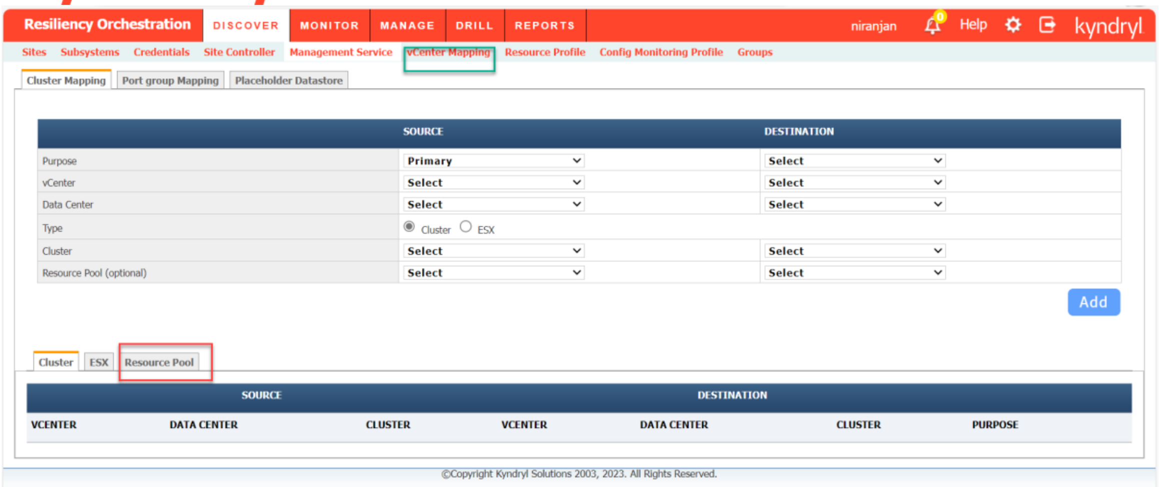
Note: The vCenter Management Service should have the permission to list the Clusters.

Resource Pool Mapping

Resource Pool mapping is the mapping between one side of vCenter-Datacenter-Cluster/ESX-Resource Pool to another side of vCenter-Datacenter-Cluster/ESX-Resource Pool.

The user needs to perform the following steps for resource mapping:

1. Login to the Kyndryl Resiliency Orchestration server.
2. Select **Discover → vCenter Mapping**. The Cluster Mapping page is displayed as shown in Figure 1.
3. Select **Purpose** in the Source and Destination. Source Purpose is always Primary, and Destination Purpose is either DR or CR.
4. Select the primary vCenter from the Source side vCenter drop-down list. The Data Centres are listed.
5. Select the data center from the Data Center drop-down list.
6. Select **Type** as Cluster (default) or ESX.
7. Select the Cluster or ESX from the Cluster or ESX IPs/Names listed for the selected Data center.
8. Select the Resource Pool from the drop-down list.
9. Repeat steps 4 to 8 for DR and then click **Add**. The resource pool is added, and the details are displayed in the **Resource Pool** tabbed section as shown in the following figure:



	SOURCE	DESTINATION
Purpose	Primary	Select
vCenter	Select	Select
Data Center	Select	Select
Type	● Cluster ○ ESX	
Cluster	Select	Select
Resource Pool (optional)	Select	Select

SOURCE			DESTINATION			
VCENTER	DATA CENTER	CLUSTER	VCENTER	DATA CENTER	CLUSTER	PURPOSE

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved.

The following snippet displays the logical mapping between vCenter datacenter clusters:

Primary vCenter-Datacenter-Cluster-Resource pool [--->] DR vCenter-Datacenter-Cluster-Resource pool

Note: The vCenter Management Service should have the permission to list the Resource Pool.

Port group Mapping

Port group mapping is a mapping between source and destination of vCenter-Datacenter-Cluster-Port Groups.

Salient features of Port group mapping are as follows -

- Port groups are per Network Adapter on a VM.
- Distributed virtual switch is at vCenter level. The Resiliency Orchestration server supports multiple port group per VM (Network Adapter during DR operations).
- The Resiliency Orchestration server supports multiple network mapping– Network adapter with port group in DR side. A virtual machine running on vCenter supports multiple virtual NIC.
- The Resiliency Orchestration server also supports vSphere Replication.

Note: Port group mapping is optional to configure through UI path **Discover** > **vCenter Mapping** > **Port group Mapping** if network adapter or available port group name is not configured.

The procedure for port group mapping is as follows:

1. Login to the Kyndryl Resiliency Orchestration server.
2. Select **Discover → vCenter Mapping**. The Cluster Mapping page displays.
3. Click the **Port group Mapping** tab. The Port group Mapping page displays.

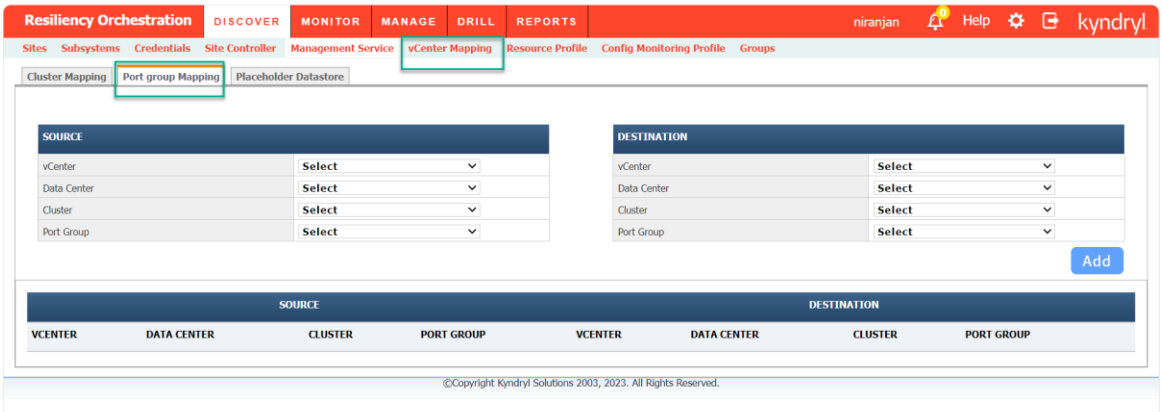
4. Select the primary vCenter from the **vCenter** drop-down list in the Source section. The Data Centres are listed.

5. Select the data center from the **Data Center** drop-down list. All clusters of the selected Data Center are listed.

6. Select the cluster from the **Cluster** drop-down list. All port groups of the selected cluster are listed in the Port Group list.

7. Select the Port Group.

8. Repeat steps 4 to 7 for Destination section and then click **Add**. The port group is added, and the details will be displayed as shown in the following figure:



SOURCE		DESTINATION	
vCenter	Select	vCenter	Select
Data Center	Select	Data Center	Select
Cluster	Select	Cluster	Select
Port Group	Select	Port Group	Select

SOURCE				DESTINATION			
VCENTER	DATA CENTER	CLUSTER	PORT GROUP	VCENTER	DATA CENTER	CLUSTER	PORT GROUP

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved.

Note: The vCenter Management service should have the permission to list the Port Group.

Placeholder Datastore

The user needs to select a datastore for each ESX, the server uses this datastore as the placeholder datastore.

To select the Placeholder Datastore, follow the steps listed below.

Login to the Kyndryl Resiliency Orchestration server.

Select **Discover → vCenter Mapping**. The Cluster Mapping page displays.

Click the **Placeholder Datastore** tab. The Placeholder Datastore page displays.

Select the primary vCenter from the **vCenter** drop-down list. All ESX of the selected vCenter are listed.

Select the ESX IP/Name from the **ESX** drop-down list. All placeholder datastores of the selected ESX are listed.

Select the placeholder datastore from the **Placeholder DataStore** list.

Click **Add**.:

Note:

1. In case of DR, one placeholder datastore is required for recovery purpose. In case of CR, add Placeholder Datastores required for recovery first and then the datastore required to perform drill.
2. If vCenter IP/Name is changed, all cluster mapping should be deleted and these should be recreated via remapping procedure.

Group Creation

Groups

You can view the summary of groups configured under various types in the dashboard. The **Groups** category displayed the number of groups configured against each type such as **Business Groups, 3 Site Groups**, **Application Groups**, and **Recovery Groups**. This section also displays the total of all the groups.

If the group is licensed, the following actions can be performed:

Changing the functional module for a group.

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click Recovery Group or Application Group tab, the respective Group listing page appears.
3. Click on the required group Name in the **Group Name** column and the **Group Details** page is displayed.
4. Click the Group Configurations tab.
5. Click the **License** tab. This tab will have an option to specify the licensed functional module "Recovery" and/or "Test" for that group.
6. The Licensed modules are shown as enabled for that Group.
7. The user can access the licensed modules for that Group. The disabled options cannot be accessed.
8. Click **Save**.

Note:

- The Save button is enabled only if the Group is in Maintenance/Unmanaged Mode. If the Save button is disabled, the user has to use the **Discover** >**Groups** link to move the group to Maintenance mode and to enable it.
- On clicking the Save button without any modules selected, a warning message "*At least one module has to be enabled for the group*" is displayed.
- On clicking the Save button with one or more modules selected, the group will be assigned with the selected modules and the user can perform any functionality related to that module.

The Kyndryl Resiliency Orchestration server will count the licenses appropriately as per the modules checked by the user.

Specifying the functional module for a group during group creation

1. Click Save after creating the Group. The Group Configuration page is displayed.
2. Click the License tab. The tab displays options to specify the licensed functional modules for that Group.
3. The licensed modules are enabled and the unlicensed modules are shown as disabled.

Note:

The "Enable" button will be enabled only if the group is in "Maintenance/Unmanaged mode". For a newly created group, the "Enable" button will be shown as enabled.

- On clicking the "Enable" button without any modules selected, a warning message "At least one module has to be enabled for the group" is displayed.
- On clicking the "Enable" button with one or more modules selected, the group will be assigned with the selected modules and user can perform any functionality related to that module.

The Kyndryl Resiliency Orchestration server will count the licenses appropriately as per the modules checked by the user.

Creating / Editing Groups

A Group is created / Edited by discovering Components, Datasets and Protection Schemes and by associating them to a site. Refer Adding Sites and Discovering Subsystem for more information.

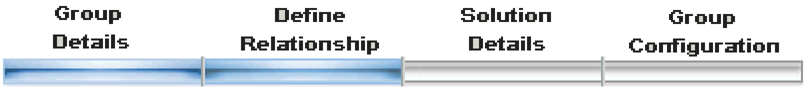
Refer **Kyndryl Resiliency Orchestration Server User Role Management** to see the privileges.

A Group is configured completely by performing following steps:

1. Group Details
2. Define Relationship
3. Provide Solution Details
4. Configure a Group
   - Configure RPO/ RTO/ Data Lag Objective
   - Configure Continuity Operations
   - Configure Events
   - Configure Drills
   - Configure Notifications
   - Configure SNMP
   - Configure Business Processes

- Configure Group License

Following diagram explains the Group creation / Editing process. This will be displayed on the BG, AG, and RG creation page.



🟦 Indicates that the respective step has been completed.

⬜ Indicates that the respective step has not been completed.

Navigate to Groups page by clicking **DISCOVER** > **Groups**. The **Groups** page appears. Select **Application Groups** or **Recovery Groups** and the respective Group Listing page appears which displays the list of Groups available with their status.

Note:

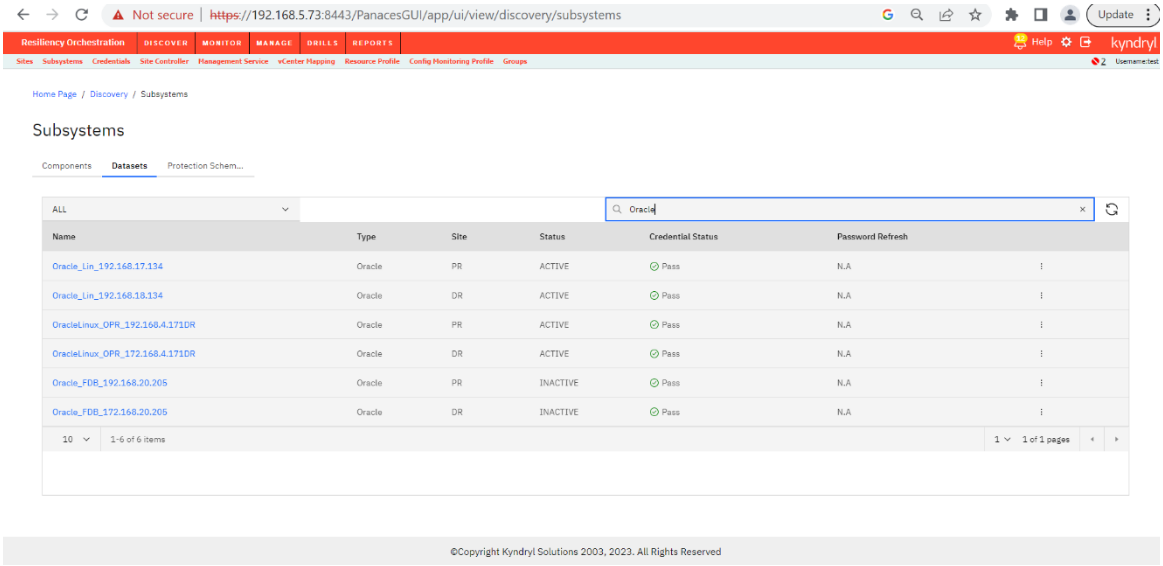
You can also view the details of a Group by clicking the respective link in the **Group Name** column.

Creating Recovery Groups

A **Recovery Group** (**RG**) is created to protect data. The data protection is done by binding the data to the associated Components and Protection Scheme present in the DR infrastructure.

Refer Kyndryl ***Resiliency Orchestration Server User Role Management*** to see the privileges.

- **Note**: RG can be created only after component, dataset, and protection scheme are discovered.
  When PFR is used for data replication and NormalFullCopy operation of Kyndryl Resiliency Orchestration is not used, you have to create a new fileset and associate it to the new Group. If the NormalFullCopy operation is performed by Kyndryl Resiliency Orchestration, then the filesets are created by Kyndryl Resiliency Orchestration itself.
- For more information on fileset creation, refer ***Add Fileset*** topic in PFR Online Help. The fileset creation is not applicable for other replication tools.
- You can create a Recovery Group for Disaster Recovery (DR) as well as for Cyber Recovery (CR) by performing the following steps. The procedure mentioned below is applicable for both DR and CR.



Subsystems

Name	Type	Site	Status	Credential Status	Password Refresh
Oracle_Lin_192.168.17.134	Oracle	PR	ACTIVE	✓ Pass	N.A
Oracle_Lin_192.168.18.134	Oracle	DR	ACTIVE	✓ Pass	N.A
OracleLinux_OPR_192.168.4.171DR	Oracle	PR	ACTIVE	✓ Pass	N.A
OracleLinux_OPR_172.168.4.171DR	Oracle	DR	ACTIVE	✓ Pass	N.A
Oracle_FDB_192.168.20.205	Oracle	PR	INACTIVE	✓ Pass	N.A
Oracle_FDB_172.168.20.205	Oracle	DR	INACTIVE	✓ Pass	N.A

10 1-6 of 6 items 1 1 of 1 pages

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

To create an RG:

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click **Discover Recovery Group** button on the right side of the page, the **Create Recovery Group** page appears.

Enter the following details.

Field	**Description**
Group Name	Enter a unique name for the Recovery Group. If the Group name already exists, a message is displayed prompting you to enter a different name for the Group. This field is mandatory. Note: Group name should not be empty. It can have a maximum of 32 characters that includes alphanumeric characters and underscore. It should start with an alphabet only and should not contain any blank spaces.
Description	Enter a description for the RG.

Field	Description
Group Priority	Choose the type of priority from the drop-down list to associate with the RG.
Solution Signature	Select the type of DR/CR Solution from the drop-down list. This field is mandatory. Refer to the **Advanced Group Configuration** topic for the respective DR/CR Solution available under DR Solutions Supported by Kyndryl Resiliency Orchestration or CR Solutions supported by Kyndryl Resiliency Orchestration. The **Include Redo Logs** checkbox is displayed, only if you select any of the Oracle DR Solutions from the drop-down list. Enable the **Include Redo Logs** checkbox if the DR Solution supports Redo Logs. **At present, Kyndryl Resiliency Orchestration supports Redo Log for Oracle Archive Logs with Hitachi Replication and Oracle Archive Logs with Other Replicator" only.** **Note**: If you select **Include Redo Logs** checkbox, ensure that you set up additional protection schemes for redo log protection on production and DR respectively.
Purpose	Select the Purpose of the group. The options available are **DR** and **CR**. By default, **Purpose** is set to **DR**, which means that a DR group will be created. Select **CR** if you would like to create a CR group.
Configured RPO/RTO	Enter the RPO/RTO values. You can configure the values in seconds, minutes or hours. This field is mandatory. **Note**: ▪ The RPO/RTO values are dependent on the DR Solution type selected. For an RG that does not have an impact on AG's RPO/RTO, its RPO/RTO values though configured, will be shown as N/A. ▪ **Configured RPO/RTO** will be disabled in Test License packages.

Field	Description
Configured Data Lag Objective	Enter the Data Lag Objective value. You can configure the value in KB/MB/ number of files. This field is mandatory. Note: ▪ The Data Lag Objective unit is dependent on DR solution type selected. If a PFR solution is selected, than the unit will be the number of files. ▪ **Configured Data Lag Objective** will be disabled in Test License packages.
This server is part of a Cluster	Select the checkbox, only if the DR Solution is supported on a cluster. If you select this checkbox, provide the **Cluster Timeout** time in seconds. Refer to Support for Cluster for more information.
Part of Flex pod.	Select the checkbox, only if it is a part of Flex Pod. **Note**: For more information go to Creating Flexi RG.

4 Click **Next** to proceed with the Define Group Relationship.

5 Define Group Relationship by configuring the following elements for Production and Remote sites. To configure these elements, you can either click the links available under **Configuration Process** section or on the respective pictorial representation.

- Server Component
- Application Dataset
- Data Protection
- Network Component

Note:

- After defining each of the elements as mentioned above, the pictorial representation of the respective icons becomes (tick mark icon) indicating that the elements have been set up.
- At any point during group configuration, click **Back** to go back to the previous page or click **Cancel** to abort the group configuration.

6 Click **Next**. A message box is displayed indicating the Group has been created successfully.

7 If Group creation fails, "**Group Details**" page of the create group will be shown with the error message.

8 Click **OK** to configure DR/CR Solution specific details.

For specific information on this configuration, refer to respective pages under **DR/CR Solutions Supported by Kyndryl Resiliency Orchestration**.

Perform any of the following:

- Click **Save** to create Recovery Group.
- Click **Reset** to set the previous values in the GUI.
- Click **Cancel** to quit the current window without saving changes.

Server Component

During the Group creation process, configure the server component.

To configure the server component, perform the following steps:

1. In the **Create Recovery Group** page, after entering the details for **Group Details**, click Next.
2. In **Define Relationship**, click **Server Component** from the **Configuration Process** section or click the 🖥 icon. The **Select Components** window is displayed. It displays the list of Primary and Remote components discovered during component discovery.
3. Select the component for Primary and Remote sites by clicking the respective check box from the **Primary Components** and **Remote Components** list. You can select more than one component at a time.
4. Click **Save** to save the changes.
5. Click **Close Window** to close the window.

Note:

The components that you select on the **Select Component** window will be saved and shown when you open this window next time.

Application Dataset

During the Group creation process, after configuring the Server component, user need to configure Application Dataset.

To configure the Application Dataset, perform the following steps:

1. In the **Create Recovery Group** page, after entering the details for **Group Details**, click Next.
2. In **Define Relationship**, click **Application Dataset** from the **Configuration Process** section or click the icon. The **Select Datasets** window is displayed. It displays the list of components discovered during dataset discovery on Primary and Remote sites for the respective solutions supported by Kyndryl Resiliency Orchestration.
3. Click the **Show all datasets** checkbox to display the datasets, even if these are already in use.
4. Select the dataset for Primary and Remote sites by clicking the dataset from the **Primary Dataset** and **Remote Dataset** lists. You can select only one dataset for Primary and Remote sites at a time.

   Note:

   The Dataset is unique for a Group.

5. Click **Save** to save the changes.
6. Click **Close Window** to close the window.

   Note:

   The dataset(s) that you select on the **Select Datasets** window will be saved and shown when you open this window next time.

Data Protection

To configure the data protection schemes, perform the following steps:

1. In the **Create Recovery Group** page, after entering the details for **Group Details**, click Next.
2. In **Define Relationship**, Click **Data Protection** from the **Configuration Process** section or click the icon. The **Select Protection Schemes** window is

displayed. It displays the list of components discovered during protection scheme discovery on Primary and Remote sites for the respective solutions supported by Kyndryl Resiliency Orchestration.

3. Select the protection scheme for Primary and Remote sites by clicking the protection scheme from the **Primary Protection** and **Remote Protection** lists. You can select only one protection scheme for Primary and Remote sites at a time. If you do not find a Protection Scheme, abort the operation and initiate discovery.

   Note:

   - Select at least one protection scheme from the list. The protection scheme selection is not available for Oracle RAC with PFR solution as Oracle RAC itself creates its own fileset based on the number of nodes configured.
   - The Protection Scheme should not be used in more than one Group. If used, replication might not happen for one or more Groups simultaneously.
   - If you enable redo log protections for any of the following solutions, ensure that you select additional protection schemes on primary and remote to protect redo logs:
     - Oracle Archive Logs with Veritas Volume Replicator
     - Oracle Archive Logs with SRDF
     - Oracle Archive Logs with Global Mirror

4. Click **Save** to save the changes.
5. Click **Close Window** to close the window.

   Note:

   The protection scheme(s) that you select on the **Select Protection Schemes** window will be saved and shown when you open this window next time.

Viewing Recovery Group Details

You can view the Recovery Group Details by performing the following steps:

1. Click **Discover** on **Navigation bar**.
2. Click **Groups** on the Sub-navigation bar. The Groups window is displayed.
3. Click **Recovery Group** tab, the **Recovery Group listing** page appears.
4. Click any Recovery group in the **Group Name** column. The Recovery Group Details window is displayed. This window provides the following tabs:

Group Details - Displays the following information:

- Name of the group
- Associated AG

- Brief description of the group
- Solution along with the type of replication selected for the group
- Configured RPO and RTO for the group along with the priority set for the group.

You can edit the group details by clicking the **Edit Group** button, if you have administrator privileges.

- **Relationship** - Displays the names of the datasets and components configured for the primary and the remote site with specific details about the chosen protection mechanism. You can view and configure each subsystem by clicking the corresponding subsystem icon on the pictorial representation of the relationship between the different subsystems. This opens the **Protection Details**, **Dataset Details**, or **Component Details** pane which displays the list of configured components, datasets or protection scheme.
- **Solution Details** - Displays the solution specific information. For example, in the case of Application subsystem with PFR solution this tab displays the custom script location and the critical process (es) which are resulting in **'Application Down'** status.
- **Group Configuration** - Displays the following options for group configuration:
  - **Continuity**- Displays the list of BCOs that can be performed on the group. Click each BCO link to configure the Workflow of the operation and add any custom action(s).
  - **RPO/ RTO**- You can configure the RPO/ RTO values for the RG.
  - **Drills**- Displays the drills that can be performed on the RG. Click each drill to link to configure the different actions of the drills or to add custom action(s).
  - **Events**- Displays the Events/ Events page for the group. Click each event ID to view the event details.
  - **SNMP**- You can add a new SNMP Trap Forwarder or select from the existing trap forwarder list for sending notifications to the RG.

You can also click the corresponding icon to modify the configured properties for each continuity operation.

Editing Recovery Group

A Recovery group can be edited only when it is in UNMANAGED or MAINTENANCE and in Normal Continuity mode. Group edit is not allowed during crashed states. When in these modes, Discovery Groups page will show "Edit Group" icon enabled/highlighted, disabled otherwise.

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

To edit a Recovery Group (RG):

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Click **Recovery Group** tab, the **Recovery Group listing** page appears.
3. Click on edit group ✎ icon for the group you want to edit. The Group Details page will be shown.

   Note: Go to Change Continuity 🛠 to change group to Maintenance Mode to enable the edit group option.

Field	**Description**
Group Name	The name of the group. This field is not editable.
Description	Description of the RG. This field is editable.
Solution Signature	Type of DR/CR Solution. This field is not editable.
Purpose	Purpose of Group is DR/CR. This field is editable.
Configured RPO/RTO	The RPO/RTO values. You can configure the values in seconds, minutes or hours. This field is editable. **Note**: The RPO/RTO values are dependent on the DR/CR Solution type selected. For an RG that does not have an impact on AG's RPO/RTO, its RPO/RTO values though configured, will be shown as N/A.
Configured Data Lag Objective	Enter the Data Lag Objective value. You can configure the value in KB/MB/ number of files. This field is editable. **Note**: ▪ The Data Lag Objective unit is dependent on DR solution type selected. If a PFR solution is selected, than the unit will be the number of files.

Field	Description
This server is part of a Cluster	Shown selected if the DR/CR Solution is supported on a cluster. The configured cluster timeout will also be displayed. This field is editable. Refer to Support for Cluster for more information.

4. Click **Next** to Define Group Relationship.
5. Define Group Relationship by configuring the following elements for Production and Remote sites.

To configure these elements, you can either click the links available under **Configuration Process** section or on the respective pictorial representation. "Application Dataset" cannot be configured during edit group.

- Server Component
- Data Protection
- Network Component

  Note:

  At any point during group configuration, click **Back** to go back to the previous page or click **Cancel** to abort the group configuration.

6. Click **Next** to configure DR/CR Solution specific details.

For specific information on this configuration, refer to respective pages under *DR/CR Solutions Supported by Kyndryl Resiliency Orchestration.*

If configuration fails, the "Group Details" page of the edit group will show an error message.

7. Perform any of the following:

- Click **Submit** to edit Recovery Group.

Note*:*

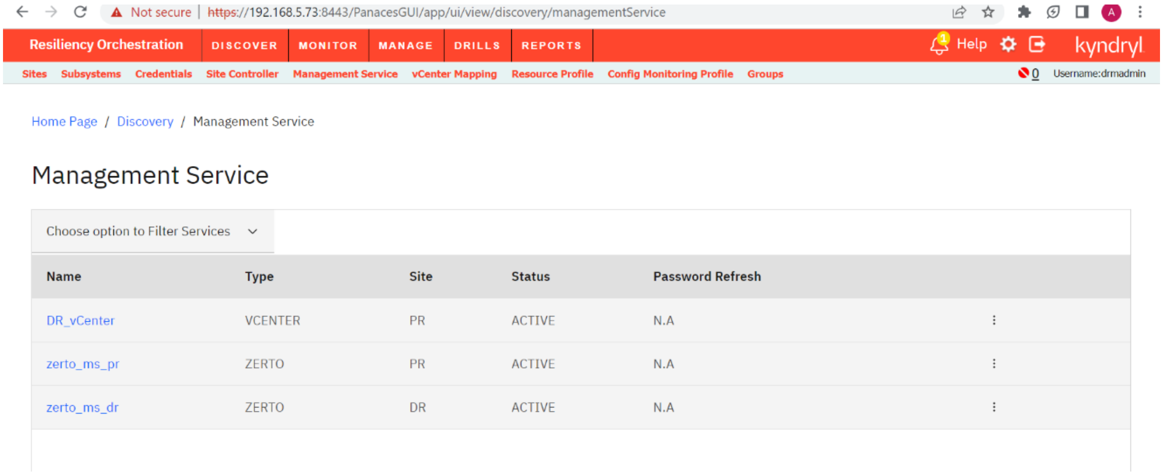
When the **Submit** button is clicked, a dialog window appears stating that certain workflows, such as **NormalCopy**, **SwitchOver**, **SwitchBack** etc. will be moved to the **Draft** state and that these workflows will need to be published before executing them. Click **OK** to accept and click **Cancel** to cancel this behaviour.

- Click **Reset** to set the previous values in the GUI.

- Click **Cancel** to quit the current window without saving changes.

8. If more than one data protection pairs have been added to the group, the workflows of the group need to be reviewed and customized to handle all the data protection pairs. The workflows that are pre-loaded/pre-packaged will handle only one pair of the data protection. If the group is of the type MSSQL Logs with PFR, Application SubSystem with PFR or Sybase Logs with PFR, then the workflows have to be completely removed by importing a new workflow XML and then needs to be customized.

"Configure SQS Mapping" button has been removed.



Management Service

Choose option to Filter Services

Name	Type	Site	Status	Password Refresh
DR_vCenter	VCENTER	PR	ACTIVE	N.A
zerto_ms_pr	ZERTO	PR	ACTIVE	N.A
zerto_ms_dr	ZERTO	DR	ACTIVE	N.A

Application Group Workflow Auto Generation

Application Group (AG) workflows are auto-generated based on the Recovery Group (RG) dependency. A user should make sure that all RGs are in proper state, before executing any of the workflows.

For example to start an AG level Fail-over, all the RGs under an AG should be in "Normal Inactive" state.

Points to remember:

AG Workflow auto-generation uses pattern base on the RG dependency and triggers one of the pre-defined RG workflow. User has to fill all those pre-defined RG workflows for proper execution of BCOs like Switch-over, Switch-back or Fail-over from AG. Requirement is that all the workflows are in "Published" state before triggering any AG BCOs.

The pre-defined RG workflows are:

- StartAppPR
- StopAppPR
- StartAppDR
- StopAppDR

- RoleSwitchToPR
- RoleSwitchToDR
- Recovery

It is recommended not to edit the auto-generated workflows of AG.

Network Component

To configure the network component, perform the following steps:

1. Click **Network Component** from the **Configuration Process** section or click the icon. The **Select Components** window is displayed. It displays the list of network components discovered during Component Discovery for Primary and Remote sites.
2. Select the component for Primary and Remote sites by clicking the respective checkbox from the **Primary Components** and **Remote Components** list. You can select more than one component at a time.
3. Click **Save** to save the changes.
4. Click **Close Window** to close the window.

Note:

The components that you select on the **Select Components** window will be saved and shown when you open this window next time.

Support for Cluster

Kyndryl Resiliency Orchestration supports Active-Passive and Active-Active clustering. Based on the type of clustering, its configuration differs. Kyndryl Resiliency Orchestration provides cluster support to the following solutions:

- Active - Passive Cluster Support
  - ***MSSQL with PFR***

    Cluster support for MSSQL-PFR requires Cluster Timeout interval to be configured at the time of Recovery Group creation. It also requires the virtual IP to be specified in the IBMAgentGeneric.cfg file for the cluster to work. The IP address must be specified against the parameter PANACES_SQLAGENT_DBNODE_ADDRESS. This parameter must be configured for MSSQL cluster. At the time of recovery after disaster, PFRconfig.bat file must be run to fail over the continuity to the cluster node. Automatic running of this file can be configured in the cluster.
  - Oracle True Copy with Veritas Cluster Support (VCS)

    Oracle True Copy being the block replication based solution requires only Cluster Timeout interval to be set at the time of Recovery Group creation. Groups must be configured with Virtual IP.
- Active - Active Cluster Support

- ***Oracle RAC***

  While creating a Group, Oracle RAC cluster support requires the Node and Dataset configuration to be done at Production and DR site. Protection scheme is automatically detected.

Note:

To use Kyndryl Resiliency Orchestration to support cluster, the replication volume must be on shared device to avoid data loss. For example, for MSSQL and Sybase, the `volume/directory` where the transactional logs are dumped by Kyndryl Resiliency Orchestration™ must be shared. For Oracle the archive log location must be on shared storage.

Perform following steps to enable Kyndryl Resiliency Orchestration to support Cluster. It is assumed that you have already installed cluster software on all the nodes.

1. Install required agents on all the nodes in a cluster. Refer to Kyndryl Resiliency Orchestration Installation Guide for information on Agent installation.
2. Configure cluster software so that it starts communicating to Kyndryl Resiliency Orchestration agents during cluster fail-over. Ensure that configuration of cluster software starts Kyndryl Resiliency Orchestration agents after the underlying software being managed by the agent is up and active.
3. If RG is part of the cluster, then refer to **Creating Recovery Group** for configuring the group on a cluster.
4. If you are using PFR as protection mechanism, refer to **PFR Online Help** for more information on configuring the cluster software.

Creating an Application Group

One or more Recovery Groups are grouped together to form an Application Group (AG). An AG can be created after RG's creation or RGs can be added later by editing the AG.

> **Note:** You can view only those AGs that are assigned to you, by assigning an AG to a user, all RGs under an AG will be automatically assigned to the user.

To create an AG, perform the following steps:

1. Click **DISCOVER** > **Groups** on the navigation bar. The **Groups** page appears.
2. Select Application Group tab, the Application Group listing page appears.
3. Click **Discover Application Group** button on the right side of the page, the **Create Application Group** page appears.

Enter the following details to create an Application Group.

Field	Description
Organization	If you are using Enterprise Resiliency Orchestration leave it with default value. **Note:** This is applicable to Cyber Resiliency Orchestration only.
Application Group Name	Enter a unique name for the AG. If the Group name already exists, a message is displayed indicating you to enter a different name for the Group. This field is mandatory. **Note:** Group name should not be empty. It can have a maximum of 32 characters that includes alphanumeric characters and underscore . It should start with an alphabet only and can contain blank spaces.
Description	Enter a description for the AG.
Application Group Priority	Enter a unique name for the AG. If the Group name already exists, a message is displayed indicating you to enter a different name for the Group. This field is mandatory. **Note:** Group name should not be empty. It can have a maximum of 32 characters that includes alphanumeric characters and underscore. It should start with an alphabet only and should not contain any blank spaces**.**
Purpose	Select the Purpose of the group. The options available are **DR** and **CR**. By default, **Purpose** is set to **DR**, which means that a DR group will be created. Select **CR** if you would like to create a CR group.

Field	Description
Select Recovery Groups	▪ To associate RG to an AG, select the RG from the left side multiple selection List box and click >> button. The selected RGs are added to the AG when they are moved to the right side List box. ▪ To deselect the associated RGs from the AG click << button to move the RG from the right side window to the left side window. The order of the RGs dependencies is taken from top to down in the order of selection i.e. the Group that is selected first (which appears at the last in the listing on right side box) will be failed over first and then the Group immediately above the last will be failed over next and so on. You can also establish relationship between Recovery Groups while associating them to the AG.

4. Click **Next** to create the Failover Dependency.

   You can drag RGs from **Move Recovery Groups** list box to **Failover Dependency** area to define the parallel or sequential relationship.

   The order of the RG dependencies is taken from top-down in the order of selection i.e. the Group that is selected on top will be failed over first and then the Group immediately below the first will be failed over next and so on.

   You can also establish a relationship between the RGs while associating them to an AG.

   AG level workflows like Switch-over, Switch-back and Fail-over will be generated automatically based on this Failover dependency.

5. Click **Next** to provide the AG details. Enter RTO value in seconds for an AG in the **Configured RTO** text boxes. The values can be given either in hours/minutes/seconds from the drop-down list.

   Note:

   - Actual RTO for AG will be calculated based on the auto-generated Fail-over workflow of the AG.
   - AG will support only RTO no RPO.

6. Perform any of the following:

- Click **Back** to go back to the previous page.
- Click **Finish** to save the changes.
- Click **Cancel** to quit the current operation.

Viewing Application Group details

You can view the Application Group Details by performing the following steps:

1. Click **Discover** on Navigation bar.
2. Click **Groups** on the Sub-navigation bar. The Groups window is displayed.
3. Click **Application Group** tab, the Application Group listing page appears.
4. Click any Application group in the Group Name column. The **Application Group Details** window is displayed.

Editing Application Group

An application group can be edited only when it is in UNMANAGED or MAINTENANCE.

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

To Edit an Application Group perform the following steps:

1. Click **DISCOVER > Groups** on the navigation bar. The **Groups** page appears.
2. Click **Application Group** tab, the **Application Group listing** page appears.
3. Click on edit group ✎ icon for the group you want to edit. The Group Details page will be shown. The Group details cannot be modified by users with Operator privileges.

   Note:

   You can edit AG only if AG is in Maintenance or Unmanaged mode.

   Go to Change Continuity ⚒ to change group to Maintenance Mode to enable the edit group option.

Field	Description
Organization	The organization to which the AG belongs. This field is not editable.
Group Name	The name of the group. This field is not editable.
Description	Description of the AG. This field is editable.
Application Group Priority	Select the type of priority from the drop-down list.
Purpose	Purpose of Group is DR/CR. This field is editable.
Select Recovery Groups	Recovery Groups can be added or removed in this field.

4. Make the required changes in the relevant field.

5. Click **Next** to proceed with Create Failover Dependency page.
6. Click **Next** to proceed with Application Group Details page.
7. Click **Back** to go back to previous page.
8. Click **Finish** to save the changes.
9. Click **Cancel** to quit the current window without saving changes.

Deleting a Group

To delete a Group, it must meet the following criteria:

- It must be either in Unmanaged or Maintenance mode.
- It must not be associated with any other Group.

For the groups that do not meet above criteria, the Delete icon 🗑 is disabled.

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

The Groups created can be deleted by performing the following steps:

1. Click **DISCOVER > Groups** on the navigation bar. The **Groups** page appears.
2. Click **Recovery Group** or **Application Group** tab, the respective **Group listing** page appears.
3. Click 🗑 icon corresponding to the Group that you want to delete. A message box is displayed confirming the deletion.

> Super Administrator has the privilege to create and delete a Group. Super Administrator can delete any group (created by him or by other user categories).
>
> However, the Administrator can delete only those Groups that are assigned to or created by him. When a Group is deleted, the fileset(s) corresponding to the Group should also be deleted.

Note:

- You need at least one RG to retain an AG. If you delete the last RG then that RG and its associated AG also gets deleted.
- You can delete AG only if it is in Maintenance or Unmanaged mode.

Deleting an Application Group (AG) created through wizard

In traditional application discovery, user can delete the application by deleting the AG place holder and delete the respective components and protection scheme discovered through traditional discovery process. These clean-up steps will not work if the AG and components are created through wizard.

To delete an AG created through wizard, it must meet the following criteria:

1. Using the delete option listed in the AG listing page, user can delete the AG as a whole not the individual RGs.
2. To enable the AG delete option, user needs to move the AG to maintenance mode
3. The pre-requisite to delete the AG is to move all underlying RGs into maintenance mode. RG can only be moved to maintenance mode if there are no running active workflows.

Clean-up process

1. The delete action will clean-up the AG, all RGs mapped to the AG, components, datasets and protection schemas which are auto created during AG creation.
2. In case the mapped components, datasets & protection scheme are part of another AG, then the AG deletion will not clean-up those shared subsystems (components, datasets & protection scheme) .
3. After deleting the AG, the Appstack that was used while creating the AG is also deleted automatically as a clean-up process. User can rediscover and create the same AG again.

For the groups that do not meet the above criteria, the Delete icon 🗑 is disabled.

Refer ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

The Groups created through wizard can be deleted by performing the following steps:

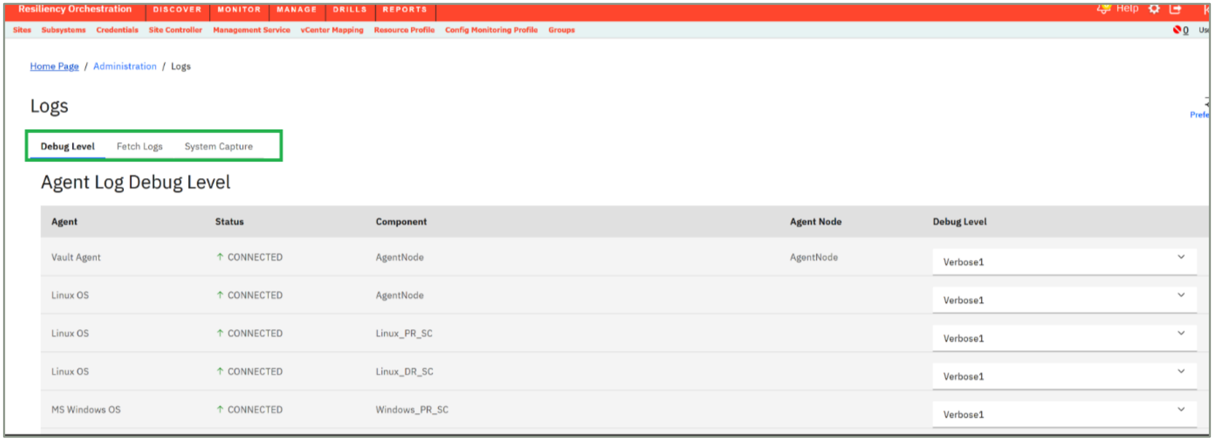
1. Click **DISCOVER > Groups** on the navigation bar. The **Groups** page appears.
2. Click **Application Group** tab, the respective **Group listing** page appears.
3. Click 🗑 icon corresponding to the Group that you want to delete. A message box is displayed confirming the deletion.

Note: If vCenter IP/Name is changed, all cluster mapping should be deleted and these should be recreated via remapping procedure.

Resiliency Orchestration Logs

Working with Logger

To perform all configurations related to logs, click **Admin** on the navigation bar. The **Administration** page appears. Scroll down to the **Logs Summary** and click **Log Info**. The **Resiliency Orchestration Logs** page appears as displayed in the image below:



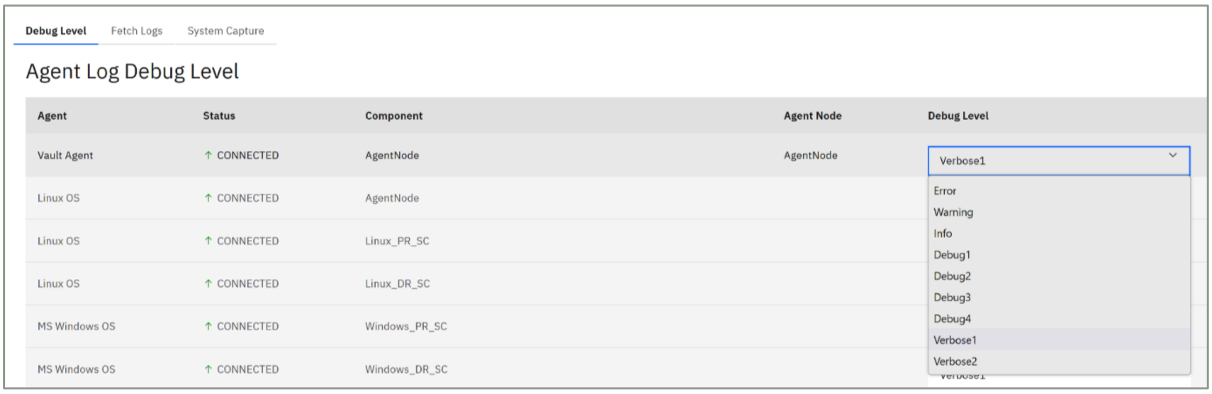
Logs

Agent Log Debug Level

Agent	Status	Component	Agent Node	Debug Level
Vault Agent	↑ CONNECTED	AgentNode	AgentNode	Verbose1
Linux OS	↑ CONNECTED	AgentNode		Verbose1
Linux OS	↑ CONNECTED	Linux_PR_SC		Verbose1
Linux OS	↑ CONNECTED	Linux_DR_SC		Verbose1
MS Windows OS	↑ CONNECTED	Windows_PR_SC		Verbose1

Resiliency Orchestration Logs page appears with the following information:

Column	Description
Debug Level	Provides the debug level drop-down list. You can see the debug level drop-down list only if the agent is connected to the Resiliency Orchestration server. If the agent is not connected to the Resiliency Orchestration server, you see **Unavailable** in the Debug level column.
Fetch logs	Allows you to retrieve a log file from a corresponding site to Resiliency Orchestration Server.
System Capture	Allows you to capture and view system details corresponding to the Resiliency Orchestration Server.



Agent Log Debug Level

Agent	Status	Component	Agent Node	Debug Level
Vault Agent	↑ CONNECTED	AgentNode	AgentNode	Verbose1
Linux OS	↑ CONNECTED	AgentNode		
Linux OS	↑ CONNECTED	Linux_PR_SC		
Linux OS	↑ CONNECTED	Linux_DR_SC		
MS Windows OS	↑ CONNECTED	Windows_PR_SC		
MS Windows OS	↑ CONNECTED	Windows_DR_SC		Verbose1

Column	Description
Agent	Displays the list of agents connected to Resiliency Orchestration Server.
Status	Displays the status of agents to indicate whether the agent is Connected or Disconnected
Component	Displays the component where the agent has been installed.
Agent Node	Displays the agent node for the agent.
Debug Level	Provides the debug level drop-down list. You can see the debug level drop-down list only if the agent is connected to Resiliency Orchestration server. If the agent is not connected to Resiliency Orchestration server, you see **Unavailable** in the Debug level column.
Fetch logs	Allows you to retrieve a log file from a corresponding site to Resiliency Orchestration Server.
System Capture	Allows you to capture and view system details corresponding to Resiliency Orchestration Server.

You can set the following preferences for log files on the right pane of the Logs page:

- View the complete path of the log files stored on the server in the **Retrieved Logs will be stored on the Server at the following location** text box.
- Set the debug level for the RO server log by selecting the debug levels from the **Server Debug Level Selection** drop-down list. Refer to Setting Debug Level for more information.
- Set Resiliency Orchestration server and Agent Log Retention period. Refer to the Retaining Log for more information.
- Set the Server log file size limit on the Resiliency Orchestration server. Refer to Setting Log File Size for more information.

Logger Overview

The **Logger** maintains a periodic log of Resiliency Orchestration operations. The log files are created for the following modules of Resiliency Orchestration:

- Resiliency Orchestration GUI
- Resiliency Orchestration Server
- Log file per Agent per Server

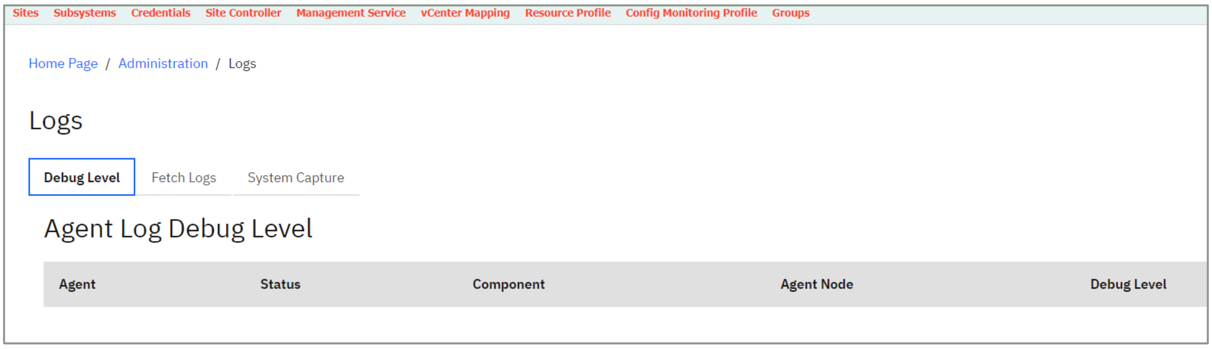
The naming format of the log file is a module name followed by that day's date with '.log' as an extension.

The logger has the following configurable options:

- Agent Debug Level
- Resiliency Orchestration Server Debug Level Selection
- Server Log Retention Period
- Agent Log Retention Period
- Log File Size

You can also retrieve log files and filter log files by making specific choices.

To perform all configurations related to logs, click **Admin** on the navigation bar. The **Orchestration Administration** page appears. Scroll down and click **Logs Summary**. The **Resiliency Orchestration Logs** page appears with the following information:



Logs

Agent Log Debug Level

Agent	Status	Component	Agent Node	Debug Level

Column	Description
Agent	Displays the list of agents connected to Resiliency Orchestration Server.
Status	Displays the status of agents to indicate whether the agent is Connected or Disconnected

Component	Displays the component name where the agent has been installed.
AGENT NODE	Displays the agent node of the agent.
Debug Level	Provides the debug level drop-down list. You can see the debug level drop-down list only if the agent is connected to Resiliency Orchestration server. If the agent is not connected to the Resiliency Orchestration server, you see Unavailable in the Debug level column.

You can set the following preferences for log files in the right pane of the Resiliency Orchestration Logs page:

- View the complete path of the log files stored on the Resiliency Orchestration server in the **Retrieved Logs will be stored on the Resiliency Orchestration Server at the following location** text box.
- Set the debug level for the Resiliency Orchestration server log by selecting the debug levels from the **Server Debug Level Selection** drop-down list. Refer to Setting Debug Level for more information.
- Set Resiliency Orchestration server and agent log retention period. Refer to the Retaining Log for more information.
- Set the log file size limit on the Resiliency Orchestration server. Refer to Setting Log File Size for more information.

Setting Debug Level

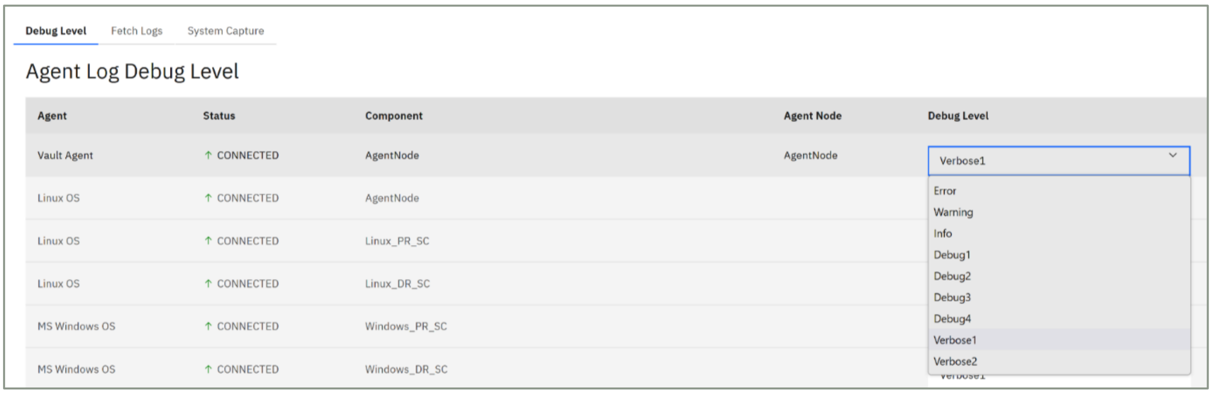
The Debug Level is the minimum severity level of the entries to be made into the log file. The log files are created every midnight, and the entry will actually be entered into the log file, if it is at least as severe as the current debug level of the logger.

For example, if a module makes a log entry with severity level VERBOSE, but the current debug level is INFO, then this entry will not be written into the log file because VERBOSE is not as severe as INFO. Therefore, the Debug Level decides how many entries will be written to the log file. These log files are created every midnight.

Click *Resiliency Orchestration Server User Role Management* to see the privileges.

You can set the debug level for the log files by performing the following steps:

1. Click **Admin** on the navigation bar. The **Resiliency Orchestration Administration** page appears. Scroll down to the **Logs Summary** and click. The **Resiliency Orchestration Logs** page appears.



Agent Log Debug Level

Agent	Status	Component	Agent Node	Debug Level
Vault Agent	↑ CONNECTED	AgentNode	AgentNode	Verbose1
Linux OS	↑ CONNECTED	AgentNode		
Linux OS	↑ CONNECTED	Linux_PR_SC		
Linux OS	↑ CONNECTED	Linux_DR_SC		
MS Windows OS	↑ CONNECTED	Windows_PR_SC		
MS Windows OS	↑ CONNECTED	Windows_DR_SC		

2. Each module can be configured with a debug level. There are nine debug levels to record an ongoing process of Resiliency Orchestration, ranging from ERROR to VERBOSE 2. The debug levels control the information logged into the log file.
3. The following table explains the purpose of each debug level:
4.

Debug Level	Description
ERROR	Logs all the errors that occurred or occurring in the system. This is the minimal debug level. In a real-time environment, generally, it would be sufficient to log errors. In such cases, the debug level has to be set to ERROR and only errors occurring will be logged.
WARNING	This debug level forecasts the problem.
INFO	Keeps the user informed about the operation being performed.

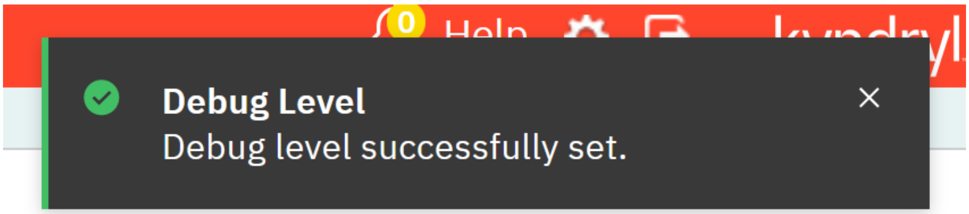
Debug Level	Description
DEBUG 1 DEBUG 2 DEBUG 3 DEBUG 4	Provides info on the cause of the error that has occurred. Typically, this will help the support team and engineers to zoom into the actual problem.
VERBOSE 1	Logs information on all the activities that happen on the system.
VERBOSE 2	Logs every happening in the system. Typically, threaded executions use this level to avoid the creation of huge log files. For example, if RPO and RTO is not being computed, then this level needs to be set to debug the problem.

5. The entries to the log file are maintained in a unique format, which is <time stamp>::<thread name> ::< severity level> :: <module name> :: <sub module name> :: <message>
6. For example, 07/23/2004 06:50:37 PM :: RPORTOHandlerThread::VERBOSE :: SERVER :: ACPAgentManagement :: no events from any agent at this moment.

2. The Debug Level Selection can be done for Agents and Resiliency Orchestration Server one at a time. The entries are made into the respective log file based on the debug level.

3. To select the debug level for **Agents**, perform the following steps:

   1. In the **DEBUG LEVEL** column, select the debug level from the drop-down list adjacent to the Agents on the **Resiliency Orchestration Logs** page. A message box is displayed indicating the successful modification of the debug level.



Debug Level

Debug level successfully set.

Note:

The debug level information for Resiliency Orchestration Server and Agents is stored along with the preceding level information into the log file. For example, If the selected debug level is WARNING for the SERVER module then the severity levels information logged into the log file are 'ERROR' and 'WARNING'. If the selected debug level is VERBOSE, then it logs all the preceding severity level information into the log file.

Log Preferences

Resiliency Orchestration automatically purges the agent and server log files based on the following:

- Size of the log file directory
- Days specified to retain log files.

As the log files are created every midnight, they accumulate and occupy the server space. To free up the server space the old log files are deleted.

The log files are retained depending upon the retention period specified in ‘Days’ and the log files are purged based on the size and the retention period.

In Days- Specifies the time period in the number of days to retain the latest log files, after which Resiliency Orchestration deletes the oldest log files.

In size- Specifies the maximum size of the log file directory, where the Resiliency Orchestration server and agent log files reside. Resiliency Orchestration starts purging the oldest log files when the directory size exceeds the maximum limit.

To purge the log file, Resiliency Orchestration considers size as the primary factor and the number of the days as the secondary factor. When the size of the log file directory exceeds 100 MB, Resiliency Orchestration deletes the oldest log file one by one till the directory size goes below 100 MB.

When the size of the log file directory is lesser than 100MB, then Resiliency Orchestration considers the number of days specified (i.e. 5) to retain the log files of the past five days and to delete the oldest log file one by one in descending order.

Click Resiliency Orchestration Server User Role Management to see the privileges.

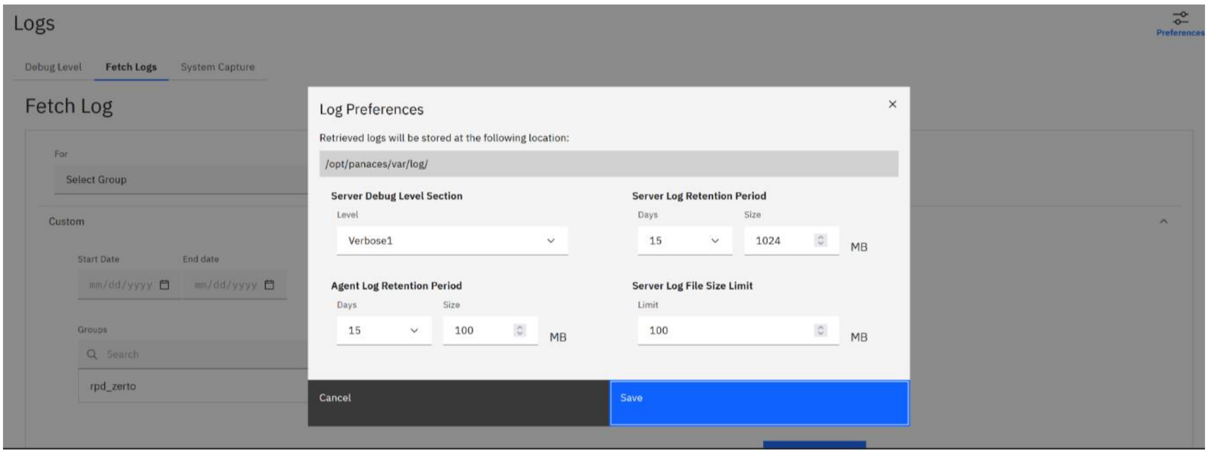
To select a log retention period, perform the following steps:

1. Click Admin on the navigation bar. The Resiliency Orchestration Administration page appears. Scroll and click Logs Summary. The Resiliency Orchestration Logs page appears.

   On the right pane, set the **Server Log Retention Period** and **Agent Log Retention Period** by performing the following steps under the respective sections:

- Select **Log Retention Period** from the **Days** drop-down list box. The log retention period can be given only in the number of days. The minimum number of days is 1 and the maximum number of days is 30.
- Enter the size of the log files in MegaBytes (MB) in the **Size** field. The size in MB is the threshold limit of the log file directory, beyond which the log files are purged by Resiliency Orchestration at a stipulated time (usually at midnight).

2. Click **Save** button.



Log Preferences

Retrieved logs will be stored at the following location:

/opt/panaces/var/log/

Server Debug Level Section
Level: Verbose1

Server Log Retention Period
Days: 15
Size: 1024 MB

Agent Log Retention Period
Days: 15
Size: 100 MB

Server Log File Size Limit
Limit: 100 MB

Operational History

Resiliency Orchestration server will automatically purge (delete) the metadata and retain the required data for the retention period configured by the user. Data available for reports is influenced by the metadata maintained by Resiliency Orchestration server.

Purging happens between 00:00 AM to 01:00 AM automatically based on the configuration.

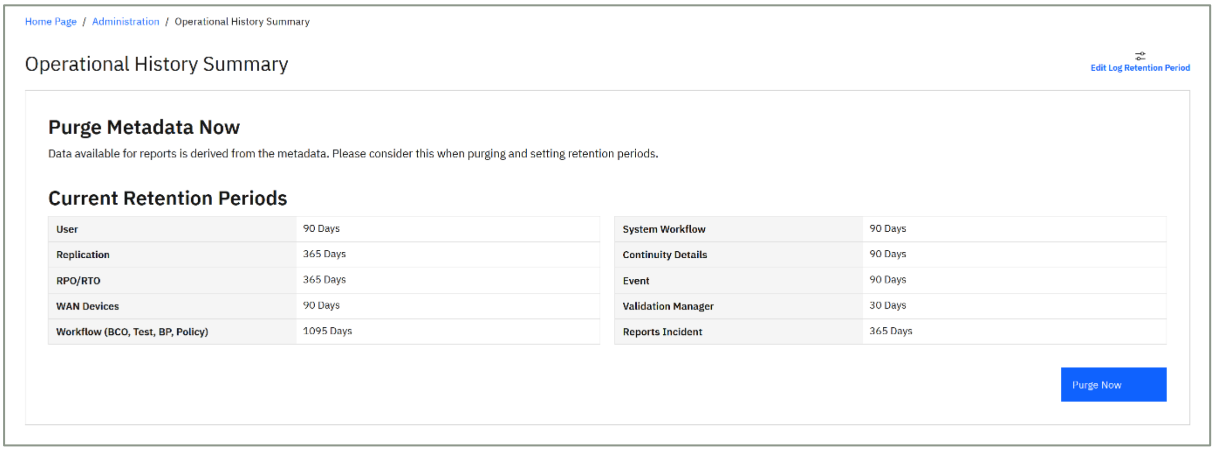
Resiliency Orchestration Server User Role Management to see the privileges.

To manage purging of the metadata, perform the following steps:

1. Click **Admin** on the navigation bar, and the **Resiliency Orchestration Administration** page appears.
2. Scroll down to the Operational History Summary and click Go to Operational History. The Resiliency Orchestration Server Operational History Management page appears. There are two-tab options:
   - **Purge Log Now**
   - **Edit Log Retention Period**

Purge Log Now

This tab shows the default retention period configured. The default values for the **Retention Period** are given below:


Home Page / Administration / Operational History Summary
Edit Log Retention Period
Purge Now

Operational History Summary

Purge Metadata Now

Data available for reports is derived from the metadata. Please consider this when purging and setting retention periods.

Current Retention Periods

User	90 Days	System Workflow	90 Days
Replication	365 Days	Continuity Details	90 Days
RPO/RTO	365 Days	Event	90 Days
WAN Devices	90 Days	Validation Manager	30 Days
Workflow (BCO, Test, BP, Policy)	1095 Days	Reports Incident	365 Days

Log Information	Retention Period in Days
User	90 (3 months)
Replication	365 (1 year)

Log Information	Retention Period in Days
RPO/RTO	365 (1 year)
Workflow (BCO, Test, BP, Policy)	1095 (3 years)
System Workflow	90 (3 months)
Continuity Details	90 (3 months)
Event	90 (3 months)
Validation Manager	30 (1month)

Note: You can change the retention period for each Log Information parameter to up to 1825 days (5 years).

Clicking on **Purge Now** button will purge the metadata. This is useful when the retention interval is altered and the metadata needs to purged immediately.

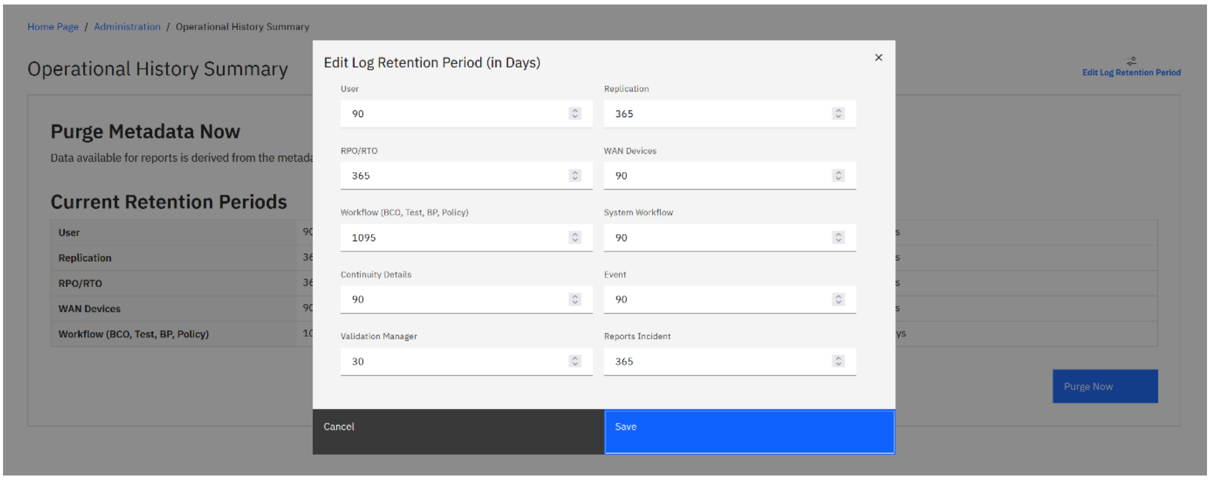
Depending on the installed licenses, the following logs are available for purging, as given in the below table.

Purge Log Now options	Test License	Recovery License	Recovery and Test License
User Log	✓	✓	✓
Replication	✗	✓	✓
RPO/RTO	✗	✓	✓
Internal Workflow	✓	✓	✓
Continuity	✗	✓	✓
Events	✓	✓	✓

Purge Log Now options	Test License	Recovery License	Recovery and Test License
Workflow Log ▪ BCO ▪ BP ▪ Policy ▪ Test	✓ ✓ ✓ ✗	✗ ✗ ✗ ✓	✓ ✓ ✓ ✓
Validation Manager	✓	✓	✓

Edit Log Retention Period

Provide retention period in days for each log. Click **Save Configuration** to save. This configuration will be effective only from the next automatic purge cycle. However, to purge immediately, refer **Purge Log Now** above.


Home Page / Administration / Operational History Summary
Operational History Summary
Purge Metadata Now
Data available for reports is derived from the metada
Current Retention Periods
User
Replication
RPO/RTO
WAN Devices
Workflow (BCO, Test, BP, Policy)
Edit Log Retention Period
Purge Now
×
Cancel
Save

Edit Log Retention Period (in Days)

User 90
Replication 365
RPO/RTO 365
WAN Devices 90
Workflow (BCO, Test, BP, Policy) 1095
System Workflow 90
Continuity Details 90
Event 90
Validation Manager 30
Reports Incident 365

Offline Purge Utility for Workflow Executions

Workflow executions, over time, increases the size of the database and this utility is provided to delete records from the database for any given workflow.

The steps to execute the utility are as follows:

- Ensure to stop the services on the RO server before executing this utility. The database replication to the secondary server should also be stopped.

- We can purge/delete the workflow execution history data from the database and preserve the last N days of history which is also called the retention days.
- The script takes only two parameters i.e., the number of days (retention days) and the Workflow name.
- Execute the following script:

  `$EAMSROOT/tools/purge/PurgeWorkflowHistory.sh` by providing the arguments.

  For example, `./PurgeWorkflowHistory <no of days> <Workflow name>`
- Once script execution is completed successfully, the following message is displayed:

  ```
  Purged rows: <no of rows>
  ```

  ```
  Purge Workflow history done for...<workflow name>
  ```

  The following message is displayed on failure:

  ```
  Got Exception in purgeExecutionLog method. Possible reason :: <reason/err massage>
  ```
- If the first parameter is given the wrong value, the following error message will be displayed:

  ```
  date: invalid date ‘’
  ```
- All the stopped services can be brought up now.

Setting Log File Size

You can limit the size of the server and agent log file to have better manageability over the log files created during various operations. The maximum size of a log file is defined by providing the size in megabytes. When the log file reaches the specified size, Resiliency Orchestration saves the log file with the module name and a sequence number for better identification.

The file naming convention is shown below:

Format: Module NameDateHH:MM_Sequence number.Log

For example:PanacesServer07-23-0404:55_1.log

PanacesServer07-23-0404:55_2.log

These log files are saved under a directory and are purged or retained by providing the retention period and size of the directory on the **Log Retention** page.

For more information on this refer to the ‘Log Retention Period’ section in this guide.

Click Resiliency Orchestration Server User Role Management to see the privileges.

To set Log File Size, perform the following:

1. Click Admin on the navigation bar. The Resiliency Orchestration Administration page appears. Scroll down to the Logs Summary. The Resiliency Orchestration Logs page appears.
2. In the right pane, click Preferences and enter the **Server Log File Size Limit** in Mega Bytes (MB) in the **Log File Size Limit** area. When the size of the log file exceeds the specified limit, Resiliency Orchestration saves the log file and provides a sequence number. The sequence number is used to refer to the log file.
3. Click **Save**.

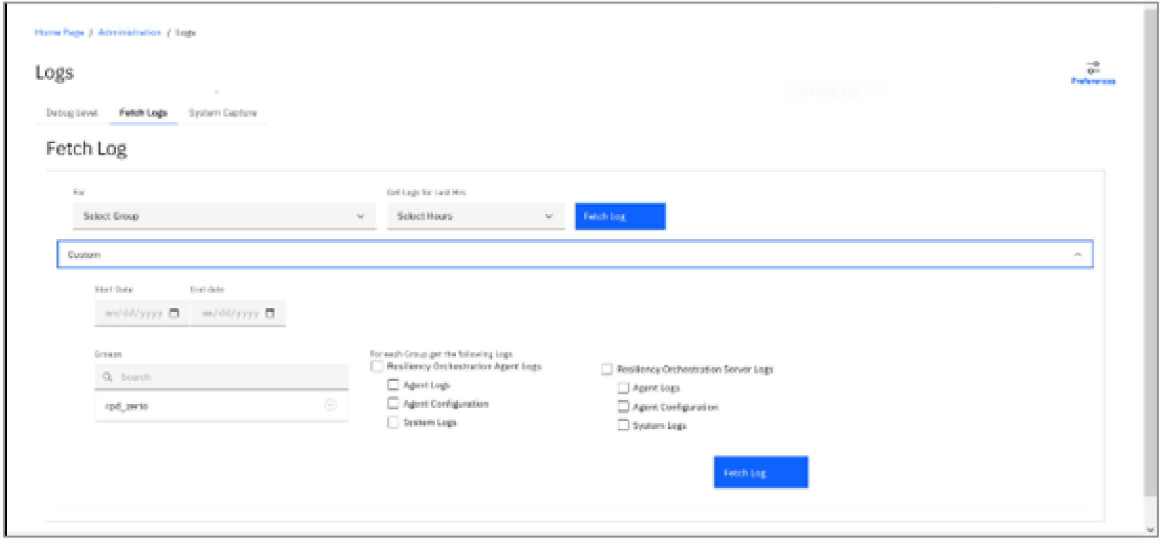
Fetch Log

This option allows you to retrieve a log file from a corresponding site to Resiliency Orchestration Server.

Click *Resiliency Orchestration Server User Role Management* to see the privileges.

To retrieve a log file, perform the following steps:

1. Click **Admin** on the navigation bar. The **Resiliency Orchestration Administration** page appears. Scroll down to the **Logs Summary** and click **Go to Logs**. The **Resiliency Orchestration Logs** page appears. Click the **Fetch Logs** tab.



2. Provide the necessary inputs for the following fields:

Field	Description
For	Select the group from the drop-down list for which you want to fetch logs.

get logs for last Hrs	Select the time duration in hours for which you want to fetch the logs.

3. Click the **Fetch Log** button. This opens a dialog box on windows to save the log file.

Note:

To learn how to fetch log files using Resiliency Orchestration command line tool, see Fetching Log files using Resiliency Orchestration log CLI tool.

Note:

When the panaces is running with non-root, the system logs will not be 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 etc.).

Custom

To filter Logs and perform Advanced Log Fetching:

1. Click **Admin** on the navigation bar. The **Resiliency Orchestration Administration** page appears. Scroll down to the **Logs Summary** and click. The **Resiliency Orchestration Logs** page appears. Click the **Fetch Logs** tab.
2. Provide the necessary inputs for the following fields:

Field	Description
Step 1: Choose Date/Time Duration	
Start Date/Time	Click 📅 and select the start date/time of the log occurrence.
End Date/Time	Click 📅 and select the end date/time of the log occurrence.
Step 2: Choose Log Source	
Choose Group	Select the group(s) for which you want to fetch logs from the list box. Hold down the "Ctrl" key to select more than one group.
For each Group get the following Logs	
Resiliency Orchestration Agent Logs	Select the checkbox to fetch Agent Logs.

Field	Description
	Selecting this checkbox automatically selects **Agent Logs**, **Agent Configuration**, and **System Logs** checkbox(es) which the user can clear, if required.
Resiliency Orchestration Server Logs	Select the checkbox to fetch Server Logs. Selecting this checkbox automatically selects **Server Logs**, **Server Configuration**, and **System Logs** checkbox(es) which the user can clear, if required.

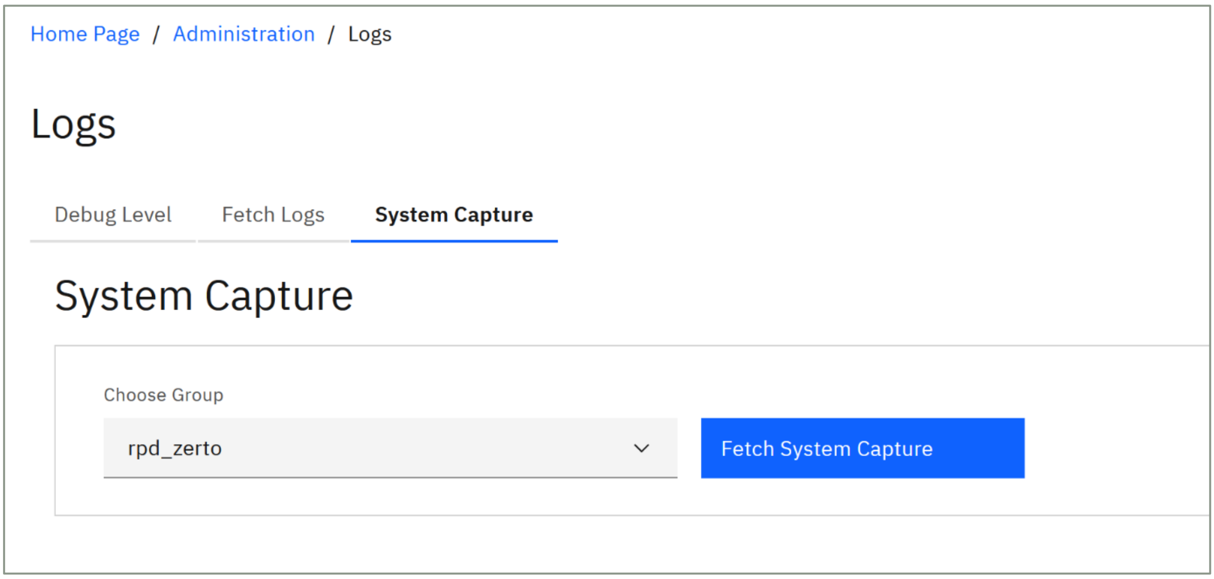
4. Click the **Fetch Log** button. This opens a dialog box on Windows to save the log file.

System Capture

This option allows you to capture and view system details corresponding to Resiliency Orchestration Server.

To retrieve a log file, perform the following steps:

1. Click Admin on the navigation bar. The Resiliency Orchestration Administration page appears. Scroll down to the Logs Summary and click Go to Logs. The Resiliency Orchestration Logs page appears. Click the System Capture tab.



2. Provide the necessary inputs for the following fields:

Field	Description
Choose Group	Select the group from the drop-down list for which you want to fetch logs. ▪ Select 1 group from the list assigned to the user.

3. Click the **Fetch System Capture** button. This opens a dialog box on windows, with a zip folder.
4. Extract the folder and open ***the system capture html page*** with the latest time stamp.

The Resiliency Orchestration System Capture html page contains the following details:

Field	Description
Group Details	Group Details Group Details contains the following information: ▪ Group configuration details ▪ Group Name ▪ Relationship ▪ Subsystems ▪ Component Subsystem ▪ Database Susbsystem ▪ Protection Scheme Subsystems Solution Signature RPO configuration RTO configuration DataLag configuration **Private details**(This provides the replication details of the group) Notifications Notifications contains the following information: ▪ Notification list

Field	Description
	- BCO Test Exercises Test Exercises contains the following information: - Test Name, its description and the test schedule in a tabular column. Business Process Integration Business Process Integration contains the following information: - Business Process Name, Business Process Description, Frequency and Schedule in a tabular column. Events: Events contains the following information: - Event Name, Event Description, Event Severity, Notification Status, and Event Impact in a tabular column. License details: License details contains the following information: Modular Name, Enabled in a tabular column. Active Workflows: Active Workflows details contains the following information: Current Workflow name, Status, Start time in a tabular column. Continuity Details Agent List

Listing Log Files

Click *Resiliency Orchestration Server User Role Management* to see the privileges.

To list the log files, perform the following steps:

1. Click **Tools** menu.
2. Click **Logs**.
3. Select **Operations**. The **User Operations** window is displayed.

This window displays the log files for all the actions performed. The operations search is based on the following:

- Timestamp
- Object
- Status

These options are used to optimize the search and are not mandatory. The operation performed so far can be retrieved irrespective of the search options by clicking the **All operations** button present at the bottom of left frame.

To retrieve the operations performed based on timestamp, perform the following:

1. Click the **Timestamp** radio button in the left frame of the window.
2. Enter From and To timestamp in Select Timestamp & enter data in 2004-12-21 10:42:12.0' format fields in the format specified.
3. When any one of the options is selected, the search button at the bottom of the left frame gets activated.
4. Click **Search** to search the operations based on the selected option.

Note:

All three options (Timestamp, Objects and Status) cannot be selected at a time.

The following table lists the details of an operation:

Field	**Description**
Time	This gives the exact time of the operation.
Module	This gives the name of the module on which the operation has been performed.
Object	This gives the name of the object on which the operation has been performed.
Operation	The gives the name of the operation performed.

Field	Description
Status	The status of the performed operation is given here.
Description	This field describes the operation.

To retrieve the information of the FAILED operations, perform the following steps:

1. Click the **Status** radio button on the left frame.
2. Enter the status of the operation in **Select Status & enter status** field.
3. Click the **Search** button to retrieve the operation based on the specified status. This retrieves the 'Failed' operations.

To view the operations performed on a specific object, perform the following:

1. Click the **Object** radio button in the left frame.
2. Enter the name of the object in **Select Object & enter object name** field.
3. Click the **Search** button to retrieve the required information. This retrieves the user operations performed on that object.
4. If you click the **All Operations** button, the **User Operations** window displays log details of all the operations.

Filtering Log Files and Advanced Log Fetching

The log file fetching can be narrowed down by specifying the date/time period (both start date/time and end date/time) of the log occurrence and Log Source.

Click *Resiliency Orchestration Server User Role Management* to see the privileges.

To filter Logs and perform Advanced Log Fetching:

3. Click **Admin** on the navigation bar. The **Resiliency Orchestration Administration** page appears. Scroll down to the **Logs Summary** and click **Go to Logs**. The **Resiliency Orchestration Logs** page appears. Click the **Fetch Logs** tab.
4. Click the **Advanced** link. The **Advanced Log Fetch** section appears.
5. Provide the necessary inputs for the following fields:

Field	Description
Step 1: Choose Date/Time Duration	

Field	Description
Start Date/Time	Click 📅 and select the start date/time of the log occurrence.
End Date/Time	Click 📅 and select the end date/time of the log occurrence.
Step 2: Choose Log Source	
Choose Group	Select the group(s) for which you want to fetch logs from the list box. Hold down the "Ctrl" key to select more than one group.
For each Group get the following Logs	
Resiliency Orchestration Agent Logs	Select the checkbox to fetch Agent Logs. Selecting this checkbox automatically selects **Agent Logs**, **Agent Configuration**, and **System Logs** checkbox(es) which the user can clear, if required.
Resiliency Orchestration Server Logs	Select the checkbox to fetch Server Logs. Selecting this checkbox automatically selects **Server Logs**, **Server Configuration**, and **System Logs** checkbox(es) which the user can clear, if required.

5. Click the **Fetch Log** button. This opens a dialog box on Windows to save the log file.

Note:

To learn how to fetch log files using Resiliency Orchestration command line tool, see Fetching Log files using Resiliency Orchestration Log CLI tool.

Fetching Log files using CLI tools

Resiliency Orchestration Log Fetching / Extracting

Prerequisites:

The user that logs on to the system to run the tool should have read/write/execute permissions (recursive) on EAMSROOT folder (This is Resiliency Orchestration server software installation directory).

Log fetching:

Click *Resiliency Orchestration Server User Role Management* to see the privileges.

The drmlogs.sh provides a Command line utility that can be invoked on the Resiliency Orchestration server to collect the Resiliency Orchestration software logs. The logs are created as zip file on the Resiliency Orchestration server.

The following command line options are provided for:
drmlogs.sh

[--user=<User>]

[--password=<password>]

1.
   - The user is a Resiliency Orchestration user name.
   - It should have the administrator privileges.
   - The user is an optional parameter and defaults to 'panaces' if the user option is not given.
   - The password is an optional parameter and it prompts for password if password option is not given.

{ <--time =dd/mm/yyyy,hh:mm , --duration=N > }

1.
   - Logs from time given as --time option and up to duration of 'N hours' are collected (provided both are given).
   - If duration option is not given, it means logs from –-time to current time.
   - If only --duration option is given, it means last 'N hours' of logs from current time.
   - One of --time and --duration option must be provided.
   - The time is taken as local time of the server from where the logs are collected. If there is a time drift between the Resiliency Orchestration server and the agents, then the logs collected may not be consistent between the server logs and the agent logs.

[--server=[logs] [,config] [,system]]

[--server-other=<comma separated file paths>]

[--agent=[logs] [,config] [,system]]

[--agent-other=<comma separated file paths>]

- --server and –-agents options specify the list of information to be collected from the Resiliency Orchestration server and the agents systems. The list of information to be collected is specified as comma separated values.

- ‘logs’ keyword specifies Resiliency Orchestration logs to be collected. These are files under Resiliency OrchestrationROOT/var/log/*, Resiliency OrchestrationROOT/panacesFileReplicator/filesets/*
- ‘config’ keyword specifies Resiliency Orchestration configuration files. These are files under Resiliency OrchestrationROOT/installconfig/*.
- --server-other and –-agent-other option is any arbitrary file. Full file path needs to be given. This file will be retrieved only if the user has permission to that file.
- If none of the server and agent option is given, it defaults to agent and server logs.

[--group =<group name> [--c] [--d] [--p]]

[--component =<cname1>[,<cname2]*]

[--dataset =<datasetname>[,<datasetname>]*

[--protection =<protectionScheme> [,<protectionScheme>]*

- Either –group or combination of -component,-dataset,-protection needs to be provided.
- Group option specify group name for which to collect logs. This should be a functional group and cannot be an application group. If specified that a group name does not exist, then an appropriate message is shown.
- If no other option [like --c or --d or --p] is present, then for the given group, all the logs of dependent subsystem are collected. Dependent subsystem include dataset/protection/component from both primary and dr site. If –c, --d or -–p options are given, only components or dataset or protection, depending on an option given, would be retrieved.
- --component, --dataset, --protection specifies comma separated list of names for which to collect log files.

--filename <filename>

- Filename is the name of the output file. The filename should be a complete path name, otherwise it is the current directory. If this option is not given, a file is generated in $EAMSROOT/var/log. The name of the generated file will be displayed as **“<user-name>_Logs-uniqueNumber.zip."**

For Example: PanacesServer.log_01-10-2023_08-04-54.gz

Extracting logs:

drmlogs.sh can also be used to extract the log files from zipped log file, when files cannot be extracted using other unzip utilities. This utility can extract archive files up to 4GB size created by Kyndryl log fetcher only. The utility is supported for RHEL Version 5 LINUX (and later versions) running Java Runtime Environment 1.5 (and later versions).

This can be invoked as follows:

```
$EAMSROOT/bin/drmlogs.sh {--extract=<absolute-path-of-zip-file> --
destination=<destination-dir>} [--buffer-size=<N-bytes>]
```

The placement of the command line parameters should exactly match as per the CLI usage presented above i.e. The user can use this CLI with the following commands only (e.g.):

- $EAMSROOT/bin/drmlogs.sh --extract=/opt/mycreatedzipfile.zip --destination=/opt/zipcontent
- $EAMSROOT/bin/drmlogs.sh --extract=/opt/mycreatedzipfile.zip --destination=/opt/zipcontent --buffer-size=10000

Any other format of the CLI will not extract the zip file and will be considered for fetching Resiliency Orchestration logs. Following options are provided.

--extract:

The value should be the absolute path of the zip file which needs to be extracted. The command invoking user should have the required permissions to open the file. This is a mandatory parameter.

--destination-dir:

The value should be the absolute path of the directory to which the extracted files have to be written. The command invoking the user should have the required permissions to create, open, read and write files and directories in this directory recursively. This is a mandatory parameter.

--buffer-size:

The value should be a positive integer between 1 and 33554432 (i.e. 32MB). This is an optional parameter. This is the size of page read/written during extraction of the zip file. In the event of user not specifying the option, the default 2MB buffer is used. User specifying a value greater than 32MB, a buffer size of 32MB will be used. Any invalid value defaults to 2MB. (***Note:*** This is a performance tuning parameter and should be used with care).

Resiliency Orchestration Log Admin

Resiliency Orchestrationlogadmin.sh

Log collection CLI can be used to retrieve any files from the customer server as long as the user with which the agent is running has privilege to access those files. To give control to the user to determine which files outside of Resiliency Orchestration Installation folder, is allowed to be retrieved by log collection tool, an admin tool is provided. Using admin cli, the user can enable or disable certain path or the ability to collect system log files. By default, only collection of system logs (like /var/log/message on Linux or oracle alert logs etc) are enabled that are outside of Resiliency Orchestration Installation folder. Any other files outside of Resiliency Orchestration Installation folder cannot be accessed until user adds the paths.

Click *Resiliency Orchestration Server User Role Management* to see the privileges.

The following command line options are provided:

[--user <User>]

[--password <password>]

- The user is a Resiliency Orchestration user name.
- It should have Super administrator privileges.
- The user is an optional parameter and defaults to 'panaces' if user option is not given.
- The password is an optional parameter and it prompts for password, if password option is not given.

[--list]

- Lists the current configuration. It lists the files or logs that are allowed to be collected. By default system log files are allowed.

[--add-file=CompName:FilePath [, CompName2:FilePath2]..]

Value of this option is a list of comma separated string of "CompName:FilePath1". CompName is name of component where the file path "FilePath1" is allowed to be accessed by log cli.

[--add=system_logs]

To add allowing collection of system log. By default this is enabled.

[--remove-file= CompName:FilePath [, CompName2:FilePath2]..]

Removing file path from the list of allowed file paths.

[--remove=system_logs]

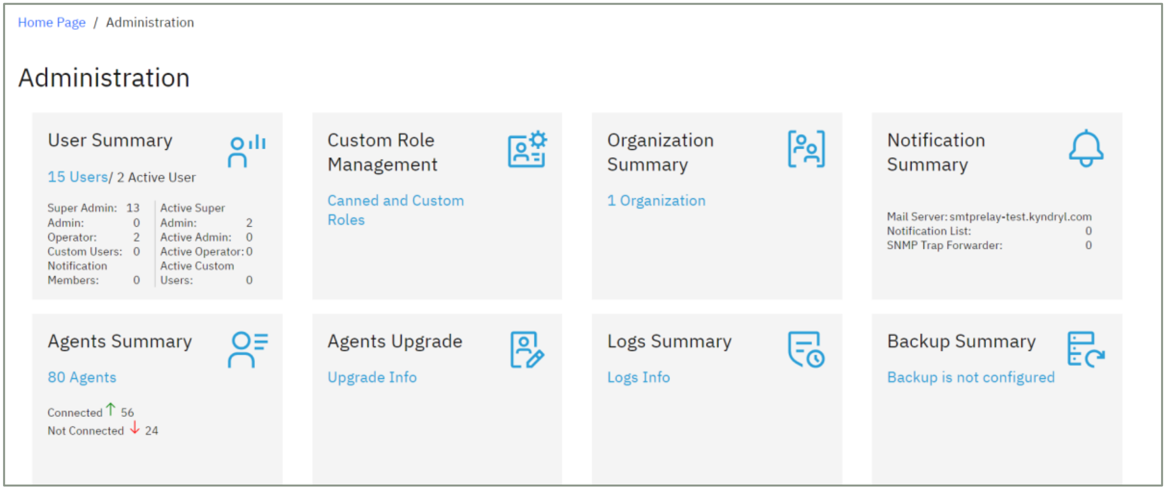
Removing collection of system logs.

Admin Tasks

Find information about the Tasks you can perform as an Administrator in the Kyndryl Resiliency Orchestration application.

Administration Summary

You can perform the following tasks as an Administrator:



Home Page / Administration

Administration

User Summary

15 Users/ 2 Active User

Super Admin: 13
Admin: 0
Operator: 2
Custom Users: 0
Notification Members: 0

Active Super Admin: 2
Active Admin: 0
Active Operator: 0
Active Custom Users: 0

Custom Role Management

Canned and Custom Roles

Organization Summary

1 Organization

Notification Summary

Mail Server: smtprelay-test.kyndryl.com
Notification List: 0
SNMP Trap Forwarder: 0

Agents Summary

80 Agents

Connected ↑ 56
Not Connected ↓ 24

Agents Upgrade

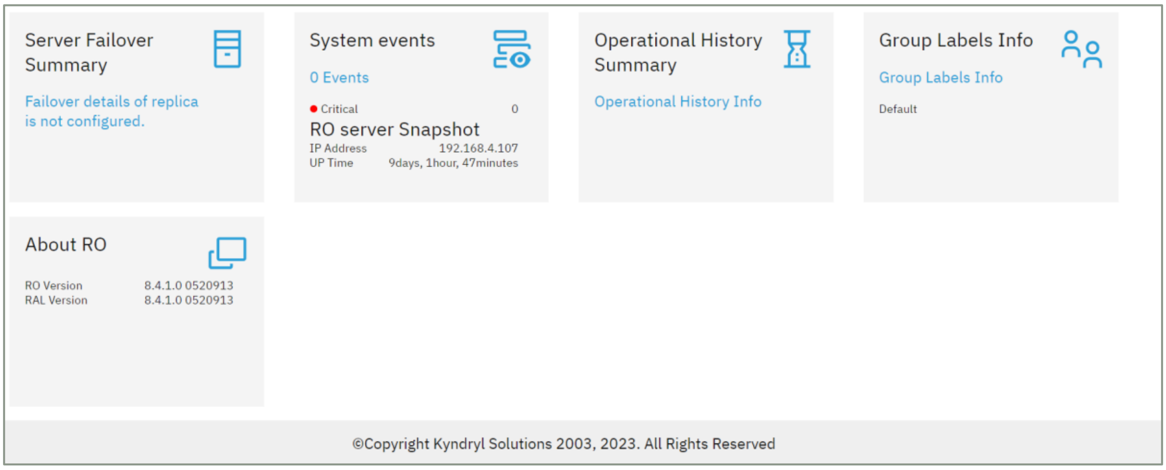
Upgrade Info

Logs Summary

Logs Info

Backup Summary

Backup is not configured



Server Failover Summary

Failover details of replica is not configured.

System events

0 Events

● Critical 0

RO server Snapshot

IP Address 192.168.4.107
UP Time 9days, 1hour, 47minutes

Operational History Summary

Operational History Info

Group Labels Info

Group Labels Info

Default

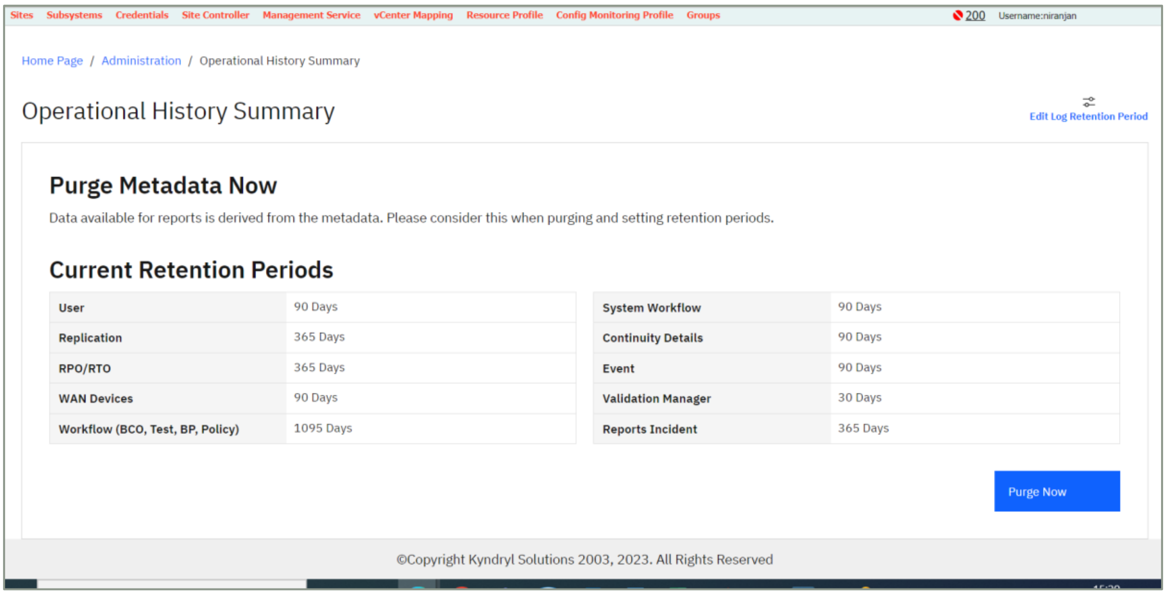
About RO

RO Version 8.4.1.0 0520913
RAL Version 8.4.1.0 0520913

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

- Users Summary
- Custom Role Management
- Organization Summary
- Notification Summary
- Agents Summary
- Agents Upgrade
- Logs Summary
- Backup Summary
- Server Failover Summary
- System events
- Manage Groups
- Operational History Summary
- Group Labels Summary
- About RO

A Operational History Summary



Home Page / Administration / Operational History Summary

Operational History Summary

Purge Metadata Now

Data available for reports is derived from the metadata. Please consider this when purging and setting retention periods.

Current Retention Periods

User	90 Days	System Workflow	90 Days
Replication	365 Days	Continuity Details	90 Days
RPO/RTO	365 Days	Event	90 Days
WAN Devices	90 Days	Validation Manager	30 Days
Workflow (BCO, Test, BP, Policy)	1095 Days	Reports Incident	365 Days

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

Cyber Incident Recovery

Protecting and Recovering Resiliency Orchestration Software from Cyber Attacks

It is critical to protect Resiliency Orchestration Software from cyber-attacks. During a cyber-attack, Resiliency Orchestration needs to be recovered so that business applications being protected from cyber-attacks can be recovered by Resiliency Orchestration Software.

Resiliency Orchestration Software has High Availability capabilities. However, to recover from cyber-attacks, you should perform the following steps:

1. Configure the Resiliency Orchestration’s metadata backups to WORM storage (such as COS).

   Note: In case, the WORM storage is not always available, you can take the metadata backups on a disk/storage and move it to WORM storage when it is available.

2. Set up a retention policy in WORM storage if it is supported by the storage vendor so that a minimum of 30 days of metadata backups are available. You can use the metadata dumps to recover Resiliency Orchestration. However, the recommended procedure is to try to recover the Resiliency Orchestration on the standby server before recovering it from the metadata backups.

Air Gap for CR Incident Recovery

For Air Gap for CR Incident Recovery information, refer to the Air Gap for CR Incident Recovery user guide.

Cyber Incident Recovery for Platform

For information on Cyber Incident Recovery for Platform, refer to the Cyber Incident Recovery for Platform user guide.

Cyber Incident Recovery for Data

For information on Cyber Incident Recovery for Data, refer to the Cyber Incident Recovery for Data user guide.

Server

Kyndryl Resiliency Orchestration comes with the following mechanisms to protect itself from any disasters:

- Kyndryl Resiliency Orchestration Crash Recovery
- Kyndryl Resiliency Orchestration Metadata Recovery
- Kyndryl Resiliency Orchestration Server Recovery

If Kyndryl Resiliency Orchestration server processes or hardware crashes during execution, it can recover automatically from the operations that were being executed at the time of crash.

Kyndryl Resiliency Orchestration server obtains a backup of the meta-data at regular intervals and stores the meta-data. When Kyndryl Resiliency Orchestration server crashes, the meta-data is lost from the time it has been backed up last to the time of server crash. In this case, we need to recover from the last backed up information.

When Kyndryl Resiliency Orchestration server crash occurs during execution of any continuity operation, Test Exercise operation or an Event Management operation, the server recovers from these operations and provides an option to resume the operation after the server is restarted.

During an Application Group crash recovery, first an attempt is made to recover all its Functional Groups and then the Application Group is recovered. During this process one or more Recovery Groups might fail leading to an inconsistent state of Application Group and its Recovery Groups. All further operations performed on the Application Group might not succeed.

When the HA feature is licensed, GUI will enable the following:

- Admin > Go to Server Failover Summary > Configuration
- Admin > Go to Server Failover Summary > Status

HA System events is displayed in System Events page.

Continuity Operation Recovery

If a Group is in the middle of a continuity operation, Kyndryl Resiliency Orchestration moves the continuity state of the Group to SHUTDOWN upon startup of Kyndryl Resiliency Orchestration server.

For example, if the current operation is Failover TRANSIT and the server crashes, the continuity operation on the Group would be moved to Failover SHUTDOWN state.

Continuity Recovery

If the server has been stopped or crashed in the middle of the workflow execution you can resume the actions.

To recover actions in a workflow, select any one of the following workflow resumption:

1. Click **Manage > Recovery group** on the navigation bar.
2. The **Recovery group listing** page appears. This page lists all groups assigned to the current user.
3. Click desired Group from the **GROUP NAME** column. The **Recovery Groups** page appears.
4. Click **Recovery Group** to do one of the following:
    - ***Initiate NormalCopy***

This operation is specific to each Recovery Group and involves periodic extraction of data from Primary and application of changed data on DR. The Replication mechanism copies incremental log files from the primary to DR.

Field	Description
Current BCM	Displays the current Business Continuity state.
Continue to Initiate the DR Operation?	Select this check box if you want to initiate the DR operation.

- ***Initiate Failover***

This operation allows Primary server to be brought down and the DR server to be made available for all business applications.

Field	Description
Current BCM	Displays the current Business Continuity state.
Continue to initiate the DR Operation	Select this check box if you want to initiate the DR operation.

Or Use ***Change Continuity State***() icon from **Discover > Groups List View.** A dialog box is displayed based on the selection.

This operation lets you move the Business Continuity State of a Group from the current to a new Business Continuity State. This operation is possible only when the Group is not executing any continuity operations currently.

Field	Description
Current BCM	Displays the current Business Continuity state.
Select Target State	Select the target state that you want to move from the current state. The available options are: Normal RESET, Normal INACTIVE, Failover ACTIVE and Fallback ACTIVE.
Continue to Initiate the DR Operation	Select this check box if you want to initiate the DR operation.

5. Enter the appropriate details in the dialog box.
6. Click **Continue** to proceed with the resumption OR click **Abort** to abort executing the workflow.

Note:

If an action in Action Group was executing at time of crash then the Action Group execution is started from the first action in the Action Group.

To recover a workflow that has recurring actions (even in Action group), executing at the time of system crash, then workflow from the first action is restarted automatically.

Event Management Recovery

The Event recovery page during Group recovery gives an opportunity for the user to recover at individual event and corresponding policy level. All the events that are in the middle of execution, at the time of Kyndryl Resiliency Orchestration Server going down or at the time of Metadata backup is being taken, would be listed during the recovery. The user can browse through this list and selectively close or resume these events or corresponding policies from where they have stopped. The user can also close all the open events in one go by a click of a button, which is applicable if the recovery is from older metadata backup.

Drills Recovery

If a Group is in the middle of a Drills, Kyndryl Resiliency Orchestration moves the drill state to SHUTDOWN, upon startup. Along with this, the Drills page provides a resume operation button called **Resume** to resume the stopped drill.

Kyndryl Resiliency Orchestration Meta Data Recovery

Kyndryl Resiliency Orchestration server can be recovered using a backup copy on the production server itself or using the replicated copy on the DR server. In both cases, the recovery procedures are similar and performed using the Recovery Wizard.

To use this option, the Backup Manager must be configured to take regular backups at the desired intervals so that a recent copy of the metadata is available for recovery.

To enforce recovery, the Kyndryl Resiliency Orchestration Server needs to be started in recovery mode after completing the metadata restores procedure or recovery procedure. To bring up Kyndryl Resiliency Orchestration Server in recovery mode, execute following command:

```
$(command prompt) IBM recover
```

Once Kyndryl Resiliency Orchestration Server comes up in recovery mode; all the configured availability Groups will be marked for recovery forcing you to complete the recovery process before doing any normal activity with that Group. An AG can be marked for recovery only if it has at least one RG associated with it. However an AG will be in Maintenance mode if it has no RGs associated with it. There is no Recovery for BG.

Each Group needs to be recovered independently. The recovery starts by clicking on that particular Group. The recovery process involves 3 different steps as shown below:

1. Group Status Recovery

During this part of the recovery, you can recover Group status.

The Group Status Recovery page displays the Group status as per the metadata copy and lets the user to set the correct Group status that represents the current environment. The Group status selected for an AG will be applicable for all its associated RGs. In other words, the AG and its RGs possess the same group status after this “Group status recovery step”.

2. Continuity Mode Recovery

Once the Group status is selected, the continuity mode recovery lets you recover to the right mode based on the chosen Group status.

During this process, Group’s continuity mode is recovered to the mode that represents the environment. Similar to the Group status, for an AG the chosen BCM state is used for its RGs also.

3. Event Policy Recovery

During the Event policy recovery, you can view the policies that are being executed at the time of the crash. This lets you close all the executing policies or keep them open for later selective closure or resumption of these policies.

If there are no policies executing for corresponding Group then there will be nothing shown in ‘Event Manager Recovery’ box in the above page will be empty. If an AG is being recovered, then all policies that are in executing state for all the associated FGs will be displayed in the above page. To know in detail about the event, click on the respective event name link on the above page. This opens a page describing the event. Click on the policy link on the above page to view the corresponding Workflow status details page.

Once the recovery process is complete a page displaying 'successful completion of the operation is shown. Click **Done** to close the page.

Kyndryl Resiliency Orchestration Server Recovery

Resiliency Orchestration Server Failover

When Kyndryl Resiliency Orchestration Primary Server goes down, the control is transferred to the Kyndryl Resiliency Orchestration Standby server.

If primary server is configured with AD server, the standby server should also be configured with AD so that the failover is seamless.

Note: To configure AD in Kyndryl Resiliency Orchestration server, refer to the topic Configuring AD.

Click ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

When you bring up the standby server during the primary server failover, perform the following steps:

1. Stop MySQL replication. Run the following command.
   ```
   stop slave;
   ```
   Note: The following is applicable only for Remote Agents.
2. In the $EAMSROOT/installconfig/PanacesAgentGeneric.cfg file, set PANACES_MASTER_SERVER_IP=<Slave Server IP>
3. Run the following update statement on 'panaces' database.

   In the below statements, replace Server IP as follows:

   <Primary RO Server IP> to IP address of primary server which is in failover state.

   <Standby RO Server IP> to IP address of the standby server.

   Use panaces;

   update component set c_ipaddr='<Standby RO Server IP>' where c_id=5;

   update component set c_display_ipaddr='<Standby RO Server IP>' where c_id=5;

```
update agent_csa set ac_connectorIP='<Standby RO Server IP>' where ac_connectorIP ='<Primary RO Server IP>';

update agent_csa set ac_anode_ip='<Standby RO Server IP>' where ac_anode_ip='<Primary RO Server IP>';

update agent_csa set ac_displayIPaddress='<Standby RO Server IP>' where ac_displayIPaddress='<Primary RO Server IP>';

update agent_csa set ac_ipaddress='<Standby RO Server IP>' where ac_ipaddress='<Primary RO Server IP>’;

update component_OSServer set cos_mgmt_ipaddr=’<Standby RO Server IP>’ where cos_mgmt_ipaddr=’<Primary RO Server IP>’;
```

4. While transferring the control to the standby server, ensure that the Kyndryl Resiliency Orchestration services on the standby server are started.
5. Manually start Kyndryl Resiliency Orchestration services on the standby server. Once the services are started, the agents automatically establish connection with the standby server.

Note: Enable SSL variable if you get error while starting panaces server.

Refer to the section ‘**Security Configuration**’ in the Installation Guide for the steps to enable the SSL variable.

Troubleshooting the Access Error

```
MariaDB [(none)]> drop user panaces@localhost;

Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> create user 'panaces'@'localhost' identified by
'<Password[1]>';

Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO
'panaces'@'localhost' IDENTIFIED BY '<Password[1]>' WITH GRANT OPTION;

Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> flush privileges;

Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> exit

[sprreoau001@cgvprliroap001 log]$ sudo /binaries/panaces/bin/panaces
status

Active MQ server is running

Panaces server is running
```

```
Tomcat server is running

Jackrabbit repository service is running

Agent Node is running
```

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

Resiliency Orchestration Server Fallback

After recovering the Kyndryl Resiliency Orchestration primary server, perform the following steps before starting the Kyndryl Resiliency Orchestration services on the Kyndryl Resiliency Orchestration primary server:

1. Stop the Kyndryl Resiliency Orchestration services on the standby server.
2. Run the enableEncryptionOnTables.sh script under $EAMSROOT/bin in the Kyndryl Resiliency Orchestration production server

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

   Check for below table decryption confirmation message.

   ```
   Executing the alter ddl statements.

   Decrypted
   ```

   For Example –

   ```
   /opt/panaces/bin/enableEncryptionOnTables.sh "dec" <Password>
   ```
3. In the $EAMSROOT/installconfig/PanacesAgentGeneric.cfg file, set PANACES_MASTER_SERVER_IP=<Primary Server IP>
4. Take the MySQL metadata dump on the standby server using the following command:

   ```
   mysqldump -u root --databases panaces pfr –routines=true --triggers > panaces_dump.sql
   ```
5. Copy the dump to the primary server.
6. Drop the Kyndryl Resiliency Orchestration MariaDB database on the production server by executing the following command at the command prompt:

   ```
   mysql>drop database panaces;
   mysql>drop database pfr;
   ```
7. Load the MySQL dump that is copied from standby server to primary server by issuing the following command:

   a. command from the terminal:

   b. mysql -u root < panaces_dump.sql
8. Run following update statement on ‘panaces’ database.

   In the above statements, replace the Server IP as follows:

   <Primary Ro Server IP> to IP address of actual primary server.

<Standby RO Server IP> to IP address of the actual standby server.

```
Use panaces;

update component set c_ipaddr='<Primary RO Server IP>' where c_name='AgentNode' and c_ipaddr='<Standby RO Server IP>';

update component set c_display_ipaddr='<Primary RO Server IP>' where c_name='AgentNode' and c_display_ipaddr='<Standby RO Server IP>';

update agent_csa set ac_connectorIP='<Primary RO Server IP>' where ac_connectorIP='<Standby RO Server IP>';

update agent_csa set ac_anode_ip='<Primary RO Server IP>' where ac_anode_ip='<Standby RO Server IP>';

update agent_csa set ac_displayIPaddress='<Primary RO Server IP>' where ac_displayIPaddress='<Standby RO Server IP>';

update agent_csa set ac_ipaddress='<Primary RO Server IP>' where ac_ipaddress='<Standby RO Server IP>;

update component_OSServer set cos_mgmt_ipaddr='<Primary RO Server IP>' where cos_mgmt_ipaddr='<Standby RO Server IP>';
```

9. Start Kyndryl Resiliency Orchestration services on the primary server.

Once the services are started, the agents automatically establish connection with the primary server.

Kyndryl Resiliency Orchestration Server Failover configured for UCS Director

When Kyndryl Resiliency Orchestration Primary Server goes down, the control is transferred to the new Kyndryl Resiliency Orchestration.

Click ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

When you bring up the new server during the Primary Server failover (High Availability), the following needs to be done:

1 **Login** to UCS Director UI.

- In **Physical tab**>>**Compute**

2 **Select** Default Pod>>**Go to** Kyndryl Continuity tab > Click ✎ icon corresponding to the UCS Director account and provide the new IP address for Kyndryl Resiliency Orchestration.

3 Click **Save** to save the modifications.

- Go to **Administration**, **Physical Accounts**>

4 Select the Kyndryl Resiliency Orchestration account.

5 Click on Test connection.

Note:

During Kyndryl Resiliency Orchestration fallback, the above changes needs to be undone.

Monitoring Server Recovery

Kyndryl Resiliency Orchestration server continuously monitors the metadata replication that is setup for high availability of Kyndryl Resiliency Orchestration Server.

Click ***Kyndryl Resiliency Orchestration Server User Role Management*** to see the privileges.

The current status of the replication can be seen by doing the following:

1. Click **Admin** on the navigation bar. The **Kyndryl Resiliency Orchestration Administration** page appears.
2. Scroll down to the **Server Failover Summary** and click **Go to Server Failover**. The **Server Failover** page appears.

The **Status** tab displays the following details:

Field	**Description**
Replication Information	
Replication Status	Displays the replication status. The Status are: ▪ **ON**: Replication is happening. ▪ **OFF**: Replication is not happening. ▪ **FAILED**: Replication is not happening, due to an error encountered during replication.
Last Dumped Log File	Displays the name of the last dumped log file.
Position	Displays the position within the last dumped log file.
Last Applied Log File	Displays the name of the last applied log file.
Last Applied Log File Position	Displays the position within the last applied log file.
Slave State	Displays the current status of the standby. The states are: ▪ Waiting for master update- The initial state before Connecting to primary. ▪ Connecting to master- The thread is attempting to connect to the primary. ▪ Checking master version- A state that occurs very briefly, after the connection to the primary is established. ▪ Registering slave on master- A state that occurs very briefly after the connection to the primary is established.

Field	Description
	▪ Requesting binlog dump- A state that occurs very briefly, after the connection to the primary is established. The thread sends to the primary a request for the contents of its binary logs, starting from the requested binary log file name and position. ▪ Waiting to reconnect after a failed binlog dump request- If the binary log dump request failed (due to disconnection), the thread goes into this state while it sleeps, then tries to reconnect periodically. The interval between retries can be specified using the CHANGE MASTER TO statement or the --master-connect-retry option. ▪ Reconnecting after a failed binlog dump request- The thread is trying to reconnect to the primary. ▪ Waiting for master to send event- The thread has connected to the primary and it is waiting for binary log events to arrive. This can last for a long time if the primary is idle. If the wait lasts for slave_net_timeout seconds, a timeout occurs. At that point, the thread considers the connection as broken and makes an attempt to reconnect. ▪ Queueing master event to the relay log- The thread has read an event and is copying it to the relay log so that the SQL thread can process it. ▪ Waiting to reconnect after a failed master event read- An error occurred while reading (due to disconnection). The thread is sleeping for the number of seconds set by the CHANGE MASTER TO statement or --master-connect-retry option (default 60) before attempting to reconnect. ▪ Reconnecting after a failed master event read- The thread is trying to reconnect to the primary. When connection is established again, the state becomes Waiting for master to send event. ▪ Waiting for the slave SQL thread to free enough relay log space- You are using a nonzero relay_log_space_limit value, and the relay logs have grown large enough that their combined size exceeds this value. The I/O thread is waiting until the SQL thread frees enough space by processing relay log contents so that it can delete some relay log files. ▪ Waiting for slave mutex on exit- A state that occurs briefly as the thread is stopping.
Last Error Number	Displays the last error number.
Last Error	Displays the detailed description of the last error.
Configuration Information	

Field	Description
Master Replication Log Buffer Size	Displays the buffer size of the primary replication log.
Master Replication Type	Displays the type of the primary replication.
Master Server ID	Displays the server ID of the primary.
Slave Server ID	Displays the server ID of the standby.
Master IP	Displays the IP address of the primary.
Master User	Displays user name of primary server.
Master Port	Displays the port ID of the primary.
Connect Retry	Displays the number of seconds after which the primary tries to reconnect. The default value is 60.

3. Click the **Configuration** tab. The **Failover Configuration** page appears. This is used to configure Kyndryl Resiliency Orchestration server for monitoring the metadata replication.

Field	Description
Slave Server Host Name/ IP	Enter hostname or IP address of the configured MySQL standby server.
MySQL Details on Standby Server	
User Name with Admin Privileges	Enter the user name with administrator privileges to log on to MariaDB database.
Password	Enter the password to log on to MariaDB database.
Port number	Enter the port number on which the MySQL standby server is listening.

4. Enter appropriate information in the relevant fields. Click **Save.**

Events

Kyndryl Resiliency Orchestration server also raises an event when the metadata replication state changes. These events can be seen from the events page and will categorized under System Events.

The following are the Events related to High Availability of Kyndryl Resiliency Orchestration:

Event	Impact	Description	Criticality
HASystemEvent001	High Availability of Kyndryl Resiliency	Replication of Kyndryl Resiliency Orchestration	INFO

	Orchestration software resumed	data to failover site has started.	
HASystemEvent002	High Availability of Kyndryl Resiliency Orchestration software stopped	Replication of Kyndryl Resiliency Orchestration data to failover site has stopped.	SERIOUS
HASystemEvent003	High Availability of Kyndryl Resiliency Orchestration software encountered an error	Error encountered while replicating Kyndryl Resiliency Orchestration data to failover site.	SERIOUS

Metadata Replication using Automated Script

MariaDB replication works in a Primary-Standby mode where a server acts as primary, while one or more servers act as standby. Resiliency Orchestration presently supports one standby process communicating to one primary. Any changes made to the files on the primary server are written to the binary log. The binary log files are updated with the latest changes and the server maintains an index of the files to keep track of log rotation. A replication process from the standby communicates to the primary to read the binary log and applies the changes to its own database.

Prerequisites for High Availability Configuration

- The RO, Tomcat, MariaDB versions must be the same on Production server and Remote RO server.
- Open the required port, for example, 3306.
- Ensure that the Remote server root password is still operational and not expired. You must use **sudo** to run scripts on the Remote server. So, if the sudo account is expired, then an error occurs.
- Create a directory on Production server and Remote servers with the required permissions to store log files and dump files.

Procedure for High Availability Configuration using Automated Script

Perform the following steps to configure High Availability using automation script.

1. Ensure that the script HAConfigure_Production.sh is available under the EAMSROOT/bin/HA_Scripts folder in the RO server.

2. Execute the `HAConfigure_Production.sh` script from the Production server.

3. Enter the following set of parameters on execution of the `HAConfigure_Production.sh` script:

Parameter	Description
Enter the path of Directory in production/remote server where DB dumps and logs can be placed. Directory should have the necessary permissions to save these files.	Enter the Directory path in the Production Server/Remote Server where DB dumps and logs can be placed. The directory must have the necessary permissions to save the relevant files. Then enter the directory to store log files/dump files (for example, /tmp, /opt, and so on).
Enter the IP Address of the current Production Server.	Enter the IP address of the Production server.
Enter the IP Address of Current Remote Server.	Enter the IP address of the Remote server.
Enter username to login Current Remote Server	Enter the username used to connect to the Remote server (for example, rouser or any other user).
Enter EAMSROOT of Current Production Server.	Enter the EAMSROOT of the Production server (for example, /opt/panaces).
Enter EAMSROOT of Current Remote Server.	Enter the EAMSROOT of remote server (for example, /opt/panaces).
Enter username to login to Production DB.	Enter the username to log in to the MariaDB database of the Production server.
Enter user password to login to Production DB.	Enter the MariaDB database password of the Production Server.
Enter username to login to Remote DB.	Enter the username to log in to the MariaDB database of the Remote server.
Enter user password to login to Remote DB.	Enter the MariaDB database password of the Remote Server.

Parameter	Description
Enter Replication username to be granted with required privileges.	Enter any username which the script will create and grant privileges (this user will be used in RO UI while configuring HA from the Admin page).
Enter Replication user password to be granted with required privileges.	Enter any password for the replication user.
Enter the path of Directory in production server where DB dump can be placed. Directory should have the necessary permissions to save the dump.	Enter the Directory path where dump can be stored (like /opt/backup or /tmp. If not default folder, then create the folder and grant the necessary permissions.

4. After the input parameters are provided, a warning appears to check the disk space. If there is enough disk space in both Production server and Remote server to take the dump successfully and copy to remote, then the user can enter **Y** to continue. If not, you can provide **N** and exit. Clean up the space and then retry executing the script.

5. The Production server and Remote server database credentials are validated before continuing with the main execution of the script. If the credentials are not correct, an error message appears and will not be able to continue.

   Note: The commands to be executed on Remote server are part of another script **HAConfigure_Remote** which will be called by default from the **HAConfigure_Production** script.

6. Once the script execution is completed, you can log in to the Production RO and configure HA from **Admin -> Server Failover** page.
7. If any errors appear during script execution, you must clean up the log/dump files and re-execute the script once the errors are fixed.

Note:

When the script is executed, log files called **HAConfiguration_Prod.txt** and **HAConfiguration_Remote.txt** are generated under the user specified folder in Production and remote servers respectively.

Preliminary Configuration

It is mandatory that the following entries are added in the file ‘PanacesAgentGeneric.cfg’ (available in $EAMSROOT/installconfig) on both primary and DR agents.

```
PANACES_MASTER_SERVER_ADDRESS=<IP address of  Resiliency Orchestration
master server>
PANACES_MASTER_SERVER_CONNECTIONATTEMPTS_BEFORE_FAILOVER=10
PANACES_MASTER_SERVER_RECONNECT_INTERVAL=25
PANACES_SLAVE_SERVER_ADDRESS=<IP address of Resiliency Orchestration
slave server>
PANACES_SLAVE_SERVER_CONNECTIONATTEMPTS_BEFORE_FAILOVER=10
PANACES_SLAVE_SERVER_RECONNECT_INTERVAL=40
```

High availability Switchover/Switchback/Failover Using automated Scripts

Prerequisites

- Production RO (Resiliency Orchestration) should be running, and Remote RO should not be running.
- HA should be configured.
- Production and Remote servers should have the relevant my.cnf, my.cnf_production and my.cnf_remote files under /etc.

  (my.cnf_production is the copy of my.cnf of production server, my.cnf_remote is the copy of my.cnf of remote server, also copy my.cnf_production to remote RO server and copy my.cnf_remote to production RO server under /etc.)

Note:

The following configurations should be available for SC and local agents:

a) PanacesAgentGeneric.cfg and Sitecontroller.cfg files under $EAMSROOT/installconfig of SC should be properly configured with both Production and Remote RO IPs.
So the SC can connect to the Remote RO when the Production RO is down.

b) In PanacesAgentGeneric.cfg, in agents

PANACES_MASTER_SERVER_ADDRESS=<IP address of Resiliency Orchestration production server>
PANACES_MASTER_SERVER_CONNECTIONATTEMPTS_BEFORE_FAILOVER=10
PANACES_MASTER_SERVER_RECONNECT_INTERVAL=25

PANACES_SLAVE_SERVER_ADDRESS=<IP address of Resiliency Orchestration remote server>
PANACES_SLAVE_SERVER_CONNECTIONATTEMPTS_BEFORE_FAILOVER=10
PANACES_SLAVE_SERVER_RECONNECT_INTERVAL=40

Steps to execute Switchover Script

HA_SwitchOver.sh is used for the switchover making original PR to DR and original DR to PR

1. Go to the EAMSROOT/bin/HA_Scripts folder in the original production server (i.e original Production server) and execute the HA_SwitchOver.sh script with the below command:
   ./HA_SwitchOver.sh

2. On triggering the script user will be asked to enter the below parameters:

Enter IP Address of Original Production RO Server ---> Original Production server IP

Enter IP Address of Original Remote RO Server ---> Original Remote server IP

Enter EAMSROOT of Original Production RO Server ---> Eamsroot of original Production server like /opt/panaces

Enter EAMSROOT of Original Remote RO Server ---> Eamsroot of original Remote server

Enter username to login to Current Remote RO Server --- > OS username to login to remote RO like rouser

Enter ROOT password to login to Production RO DB

Enter ROOT password to login to Remote RO DB

3. During script execution user will be asked to enter the password of remote server to execute secondary script HA_Remote_SO.sh in remote server.

4. Once script execution is completed successfully, user can login to the original DR server and go to server failover page. Change the slave server Ip to original production RO Ip and verify the replication status.

Steps to execute Switchback Script

HA_SwitchBack.sh is used for the switchback operation making original PR as PR again and original DR as DR again.

Go to the EAMSROOT/bin/HA_Scripts folder in the original remote server (i.e original Remote server or current production after SO) and execute the HA_SwitchBack.sh script with the below command:

```
./HA_SwitchBack.sh
```

On triggering the script user will be asked to enter the below parameters:

Enter IP Address of Current Production RO Server ---> Current Production is the original Remote server.

Enter IP Address of Current Remote RO Server ---> Current Remote is the original Production server.

Enter EAMSROOT of Current Production RO Server ---> Eamsroot of original Remote server like /opt/panaces

Enter EAMSROOT of Current Remote RO Server ---> Eamsroot of original Production server.

Enter username to login to Current Remote RO Server --- > OS username to login to current remote RO like rouser.

Enter ROOT password to login to Production RO DB

Enter ROOT password to login to Remote RO DB

During script execution user will be asked to enter the password of current remote server to execute secondary script HA_Remote_SB.sh in current remote server (current remote is the original production)

Once the script execution is successful, the user can login to the original PR server and go to server failover page. Change the slave server Ip to original remote RO Ip and verify the replication status.

Steps to execute Failover Script

HA_FailOver.sh is used for making the original DR as PR. This script is used only when Primary RO is down and hence Secondary RO should be brought up as Primary RO.

Go to the EAMSROOT/bin/HA_Scripts folder in the original remote server (i.e original Remote server) and execute the HA_FO.sh script with the below command:

./HA_FailOver.sh

On triggering the script, the user will be asked to enter below parameters:

Enter Original Production Server IP ---> Original Production server IP.

Enter Original Remote Server IP ---> Original Remote server IP.

Enter EAMSROOT of Original Remote Server ---> Eamsroot of original Remote server like /opt/panaces

Enter ROOT password to login to Original Remote RO DB

Metadata Replication with Manual Steps

MariaDB replication works in a Primary-Standby mode where a server acts as primary, while one or more servers act as standby. Kyndryl Resiliency Orchestration presently supports one standby process communicating to one primary. Any changes made to the files on the primary server are written to the binary log. The binary log files are updated with the latest changes and the server maintains an index of the files to keep track of log rotation. A replication process from the standby communicates to the primary to read the binary log and applies the changes to its own database.

Check the Prerequisites and perform the following configurations to recovery the Kyndryl Resiliency Orchestration server during failover:

Preliminary Configuration

Before doing server Failover, it is mandatory that the following entries are added in the file ‘PanacesAgentGenericConf.cfg’ (available in $EAMSROOT/installconfig) on both primary and DR agents.

```
PANACES_MASTER_SERVER_ADDRESS=<IP address of Resiliency Orchestration
master server>
PANACES_MASTER_SERVER_CONNECTIONATTEMPTS_BEFORE_FAILOVER=10
PANACES_MASTER_SERVER_RECONNECT_INTERVAL=25
```

```
PANACES_SLAVE_SERVER_ADDRESS=<IP address of Resiliency Orchestration
slave server>
PANACES_SLAVE_SERVER_CONNECTIONATTEMPTS_BEFORE_FAILOVER=10
PANACES_SLAVE_SERVER_RECONNECT_INTERVAL=40
```

After server Failover is complete, the Kyndryl Resiliency Orchestration should be started on the standby server. At this point, it is mandatory that the primary server should not be running.

At any point of time, the Kyndryl Resiliency Orchestration server should not run on both primary and standby servers simultaneously.

Note - Source of the below instructions is https://mariadb.com/kb/en/library/setting-up-replication/, please refer for more details.

Primary Server Configuration

The following are the details of MySQL configuration on primary server. If there is no password to access MySQL application, then the part of commands in italics need not be entered.

- Stop the Kyndryl Resiliency Orchestration server by entering the following command

```
# /opt/panaces/bin/panaces stop
```

- Add or modify the following entries in /etc/my.cnf at the primary site. If the file does not exist, create one.

```
[mysqld]
innodb_log_buffer_size=8M
innodb_flush_log_at_trx_commit=1
max_binlog_size=20M
max_allowed_packet=16M
max_connections=750
log_bin=panacespri_binlog
binlog-do-db=panaces
binlog-do-db=pfr
server-id=1
datadir=/var/lib/mysql
binlog-format=ROW
log_warnings=1
```

Note: Any changes in my.cnf needs mysql stop and start to take effect

- Set up Replication privilege:

  Log in to the primary server and issue the following commands

```
# MySQL -u root -p
```

```
mysql> grant replication slave on *.* to root@<IP address of slave>
-> identified by <'slave mysql password'>;
mysql> grant all on *.* to root@<IP address of slave>
-> identified by < 'slave mysql password'>;
```

- Get the primary server's Binary Log Co-ordinates

  Note: Below commands must be run in one session and session must not be exited. Exiting will remove the lock. Exiting may be done only after mysqldump is complete.

  ```
  mysql> flush tables with read lock;
  mysql> show master status;
  ```

  ```
  +--------------------------+----------+--------------+------------------+
  | File | Position | Binlog_Do_DB | Binlog_Ignore_DB |
  +--------------------------+----------+--------------+------------------+
  | panacespri_binlog.000080 | 173717 | panaces | |
  +--------------------------+----------+--------------+------------------+
  ```

  Note down the file name and the position values. If binary log is not already enabled, the output will be empty. In that case the File name should be noted as "empty string '' and the position as 4.)

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

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

  Check for below table decryption confirmation message.

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

  For Example –

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

- Take a dump of the panaces and pfr databases using the following command:

  ```
  mysqldump --routines=true --triggers -u <user> -p --databases panaces pfr
  > panaces_dump.sql
  ```

- Once the data dump has been taken, you can release the lock on the primary by running below command

  ```
  UNLOCK TABLES;
  ```

- FTP/SCP the sql file to the standby server under /tmp directory

- Start the Kyndryl Resiliency Orchestration server

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

Standby Server Configuration

The following are the details of MySQL configuration on Standby server. If there is no password to access MySQL application, then the parts of commands in italics need not be entered.

- If MySQL is already running on the standby server, shut it down.
  ```
  # mysqladmin -u root -p shutdown
  ```
- Add or modify the following entries in /etc/my.cnf on standby server. If the file does not exist, it can be created.
  ```
  [mysqld]
  innodb_log_buffer_size=8M
  max_allowed_packet=16M
  max_connections=750
  server-id=2
  log_warnings=1
  ```
- Restart the MySQL server.
  ```
  # service mysql start
  ```

  If primary and standby mysql – have different passwords, then login using primary password, and change password to standby password using command
  ```
  set password for 'root'@'localhost'=password('slave mysql password');
  ```
- Apply the database dump taken on the primary server previously
  ```
  mysql -u <user> -p < panaces_dump.sql
  ```
- Log on to the MySQL server and execute the following command to start the replication.
  ```
  mysql> change master to master_host=<'IP address of master'>,
  -> master_user='root', master_password=<'slave mysql password'>,
  -> master_log_file=<'file name noted down in step 1'>,
  -> master_log_pos=<position noted down in step 1>;
  mysql> start slave;
  ```
- Check the status by issuing the following command.
  ```
  mysql> show slave status;
  # Grant access to mysql from the master server for monitoring the
  replication
  mysql> grant all on *.* to root@<IP address of master>
  -> identified by < 'slave mysql password'>;
  ```

Kyndryl Resiliency Orchestration server running remote Agents

1. Install PFR on both the Resiliency Orchestration Servers.
2. Create a fileset using PFR GUI to replicate the remote agent configuration and scripts

   i. Fileset Name: Resiliency OrchestrationHA

   ii. Source IP : Primary Resiliency Orchestration Server

   iii. Target IP : Standby Resiliency Orchestration Server

iv. Replication Interval: Recommended is 30 minutes.

v. Symbolic link option: Replicate symbolic link only

vi. Setup source and targets

a. Source Dir/File : $EAMSROOT /remote (on Primary Kyndryl Resiliency Orchestration)

b. Target Dir/File: $EAMSROOT/remote (on Standby Kyndryl Resiliency Orchestration)

c. Source Dir/File : $EAMSROOT /work (on Primary Kyndryl Resiliency Orchestration)

d. Target Dir/File : $EAMSROOT/work (on Standby Kyndryl Resiliency Orchestration)

Note -

If any other directories are used to keep custom developed/customer scripts those have to be added to the replication source and target.

3. Enable Replication: Enable
4. Exclude the libraries and log directories from replication

a. Exclude var directory

i. Source Folder: $EAMSROOT/remote

ii. File/Folder: var

iii. Select Directory

iv. Select case sensitive

v. Select recursive

b. **Exclude mssql directory**

i. Source Folder: $EAMSROOT/remote

ii. File/Folder: mssql

iii. Select Directory

iv. Select case sensitive

c. **Exclude oracle directory**

i. Source Folder: $EAMSROOT/remote

ii. File/Folder: oracle

iii. Select Directory

iv. Select case sensitive

5. Sync Delete Files: Uncheck
6. Synchronization: Uncheck
7. Large File Support: Uncheck
8. After Fileset creation, start PFR on Primary and Standby Resiliency Orchestration.
9. Replication can be monitored using PFR GUI

Replication User Password Change

1. Primary password got changed:

   Execute the following SQL on standby:

   stop slave

   change master to master_password='<new-master-password>';

   grant all on *.* to root@<IP address of master>

   -> identified by < ‘slave mysql password’>;

   start slave

2. Standby Password got changed:

   Execute the following SQL on master:

   grant replication slave on *.* to root@<IP address of slave>

   -> identified by <’slave mysql password’>;

   GRANT FILE ON *.* TO

   <slave-user>@<slave-ip-address> IDENTIFIED BY '<new-slave-password>';

3. Both the passwords changed:

   i. Follow (1)

   ii. Follow (2)

Preferably, you can also reset the system and start the replication all-over again. Following are the steps to perform the action.

i. Execute 'stop slave' on standby m/c.

ii. Execute 'reset slave' on standby m/c.

iii. Execute 'reset master' on primary m/c.

Note:

- If the user(s)/password(s) of Kyndryl Resiliency Orchestration Databases (panaces, pfr) are changed on Primary Server then ensure that the same is configured on Standby Server Installation. Refer to Installation Guide ("Configuring Kyndryl Resiliency Orchestration Server section") for how to configure user/password for Kyndryl Resiliency Orchestration Databases.
- This deletes the binlog files generated at primary and not yet applied on standby m/c.

4. Use the HA setup document to setup high availability again.

Clean and Reset the panaces MariaDB database on Standby server

Follow these steps to clean/reset the Kyndryl Resiliency Orchestration metadata on the standby server before establishing communication between the two servers. These commands should be executed on the Kyndryl Resiliency Orchestration standby server.

```
# mysql –u root –p

mysql> stop slave;

mysql> reset slave;

mysql> drop database panaces;

mysql> drop database pfr;

mysql> exit

# mysqladmin -u root –p shutdown

# cd /var/lib/mysql

# /var/lib/mysql> rm ib* *relay*
```

Note:

Restart the standby server after clearing the Kyndryl Resiliency Orchestration metadata by executing following command:

```
# service mysql start
```

Backup

About Backup and Restore Mechanisms

Backup Mechanism

Backup mechanism is a procedure using which backup of configured data is taken on a configured server.

Restore Mechanism

Restore mechanism is a procedure using which backup of configured data is performed on a configured server.

Kyndryl Resiliency Orchestration supports following backup and restore mechanisms:

Backup Mechanism	Restore Mechanism	When to use?
Kyndryl Resiliency Orchestration Internal Backup	Kyndryl Resiliency Orchestration Internal Restore	Select this mechanism to take a full backup or restore of the configured database with the help of Kyndryl Resiliency Orchestration.
Backup using user supplied Command	Restore using user supplied Command	Select this mechanism to provide your own backup or restore commands to perform a full backup or restore of the configured database.
External backup mechanism	External restore mechanism	Select this mechanism to perform a full backup or restore of the configured database with the help of the third party backup or restore software.

You can configure the backup and restore mechanisms during NormalFullCopy and Fallback operations configuration.

Backup Manager

Kyndryl Resiliency Orchestration Backup Manager provides the protection mechanism for server Metadata, which contains all the server configuration information. Backup Manager provides online backup of the metadata automatically using a pre-configured schedule. In addition, on demand backup of the metadata can be done manually by clicking **Backup Now** button on the Backup Manager page. Ensure that the Backup is configured before taking the backup. All the backup copies go to a pre-configured location on the server. Thus Backup Manager reduces the unplanned downtime for Kyndryl Resiliency Orchestration Server by recovering from the latest copy of metadata.

Click *Kyndryl Resiliency Orchestration Server User Role Management* to see the privileges.

Note: Backup destination directory should have write permission before configuring the backup.

Example, chmod 755 <Backup destination directory>

Backup Manager Configuration

Kyndryl Resiliency Orchestration supports the following backup configurations and must be configured before taking any backup.

To configure the backup, perform the following:

1. Click **Admin** on the navigation bar. The **Kyndryl Resiliency Orchestration Administration** page appears. Scroll down to the **Backup Summary** and click **Go to Backup**. The **Backup Manager** page appears.
2. In the right pane, under **Configure Backup** provide information for the following:

Field	Description
Destination path	Provide the location of the backup file to be saved.
Backup at	Select the time slot (24 hrs time scale) of backup from the drop-down list.
Frequency	There are two types of frequency backup: ▪ Daily – Backup is fired daily at a configured time in **Backup At** field. For example, if the configured time is 15:00 hrs, then the backup is taken at 15.00 hrs every day. ▪ Weekly – In this case backup is fired weekly on the mentioned day at a specified time. For example, if the day mentioned is Sunday, and the time of backup is 15.00 hrs, then on every Sunday the files are backed up at 15.00 hrs.
Active Copies	This displays the number of active copies and about the availability of number of latest generated backup copies in that path.

3. Click **Save** to save the backup details.

Listing Backup Manager Information:

To view the configured backup information, perform the following steps:

1. Click **Admin** on the navigation bar. The **Kyndryl Resiliency Orchestration Administration** page appears. Scroll down to the **Backup Summary** and click **Go to Backup**. The **Backup Manager** page appears.
2. This page provides the configured backup information (refer to the above table) along with the following additional details of the backup file:
    - Backup Destination Path
    - Frequency of Backup
    - Frequency of Backup Day
    - Scheduled Backup time
    - Number of Active Copies
    - Size of Backup in Kb
    - Time of Last Backup
    - Backup File name

Kyndryl Resiliency Orchestration backup software supports online backup, which is independent of the backup schedule.

Server Memory Management

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

Following are the recommended values:

- No change is required for less than 20 groups.
- Configuration with more than 20 groups but less than 50: -Xmx512m is recommended.
- Configuration with more than 50 groups but less than 100: -Xmx1024m is recommended.
- Configuration with more than 100 groups: -Xmx4096m is recommended.

Note

You must stop Kyndryl Resiliency Orchestration server before trying to edit this setting. Restart the server after the setting is done.

Troubleshooting Agents

Windows Site Controller Agents

Perform the following steps to resolve the below error in the Windows site controller for agents like Veeam, Oracle, and Uniagent.

Error:

```
UncaughtExceptionHandler::Exception:java.lang.OutOfMemoryError: Metaspace
```

Note:

- The following steps are for the Generic Agent on Windows (Veeam).
- Similar steps can be performed for other agents also.

1. Move the Veeam group to maintenance mode.
2. Navigate to the agent listing page on the RO GUI and click on the Stop link under the Status column of the Veeam agent.
3. Login using Remote Desktop to the site controller mapped with the Veeam agent and keep a backup of SITECONTROLLER_HOME/bin/GenericAgent.bat
4. Modify the file GenericAgent.bat by updating the following line:

   ```
   set PR_JVMOPTIONS=-Duser.language=DE;-Duser.region=de;-
   XX:+HeapDumpOnOutOfMemoryError;-XX:HeapDumpPath=%EAMSROOT%;-
   XX:MetaspaceSize=30m;-XX:MaxMetaspaceSize=512m;-
   Dsun.reflect.inflationThreshold=2147483647;-
   XX:+UnlockDiagnosticVMOptions
   ```

5. Right-click on the service name "Kyndryl RO GenericAgent GENERIC_AGENT_n" and properties view to search for the service name of the stopped generic agent.

   The service name looks like, `IBMROGenericAgent_GENERIC_AGENT_n`

   Where “n” is the relevant number.

6. Execute the service deregistration script to delete the service from the site controller. Open the command prompt and navigate to folder SITECONTROLLER_HOME/bin and execute the following command;

   `.\deregisterAgent.bat IBMROGenericAgent_GENERIC_AGENT_64` (assuming n=64)

7. You can take the backup of the folders SITECONTROLLER_HOME\remote\GENERIC_AGENT_64 and SITECONTROLLER_HOME\remote\<Veeam_Management_Service_IP> and then delete them.

8. Navigate to the management service listing page in RO UI and edit the Veeam management service. Click on the Edit Credentials link and re-enter the password and test the credentials. Click on Save if successful.
9. Go to the Agent listing page on the RO UI and start the Veeam agent. The agent connects in a while and waits for the management service to show an Active status.
10. Move the Veeam group to the managed mode and make sure the next run of the replication workflow is successful.

Linux Operating System Site Controller Agents

Perform the following steps to resolve the meta space issue in the Linux Site controller for all the types of agents like Uniagent, Oracle agent, etc.

Note: Before performing the following steps, take the backup of the file SITECONTROLLER_HOME/bin/common.sh

1. Stop the agent from the RO UI front.
2. Edit the common.sh file by adding the below java option.

```
-Dsun.reflect.inflationThreshold=2147483647
```

3. The max metaspace size for the uniagents is 128m and 64m for the other agents.
4. Start the agent from the RO UI front.
5. Make sure all the basic functionalities are working in good condition.

3rd Party Integration

Kyndryl can notify 3rd party applications using the following services:

E-mail Notification

Email Integrations allows you to send your data to third-party applications via Email. To configure Email Notification, click Configuring Email Server.

SMS Notification

SMS Integrations allows you to send your data to third-party applications via SMS, refer to SMS Notification.

SNMP Notification

SNMP Integrations allows you to send your data to third-party applications via SNMP trap through SNMP Notification. To configure SNMP Notification click Configuring SNMP Trap Forwarder.

Panaces DB Optimization Procedure

This section is mainly created for one of the customer requirements where the Panaces database space is to be released for optimal performance. The disk space is not reduced even after deleting the old records and therefore Kyndryl recommends performing the following steps to release disk space from Panaces DB tablespace to OS.

Current Scenario and Known Issues

The following are some of the known issues related to Panaces DB optimization:

- Many CRO customers are facing disk space issues for /var/lib/mysql/panaces directory.
- Even though older DB records are deleted from tables, disk space is not being released to OS disk space.
- This issue occurs as Maria DB will not release free space to OS. So, there are many empty fragments in DB that is not released to OS.

Workaround

You must execute the optimize table <table_name> DB command for the following Panaces Tables such as:

- incident_log
- action_log
- action_execution_log_detail
- protection_log
- reports_incident_log

Pre-requisites

The following are the prerequisites before performing this procedure:

1. Check the diskspace before performing any optimization operations:

```
 prompt>> cd /var/lib/mysql/panaces

  prompt>> du -sh * | sort -hr | head
```

2. Note down the Panaces DB username and password in advance.

Note: Perform the following procedures during no dryrun execution time and with less network traffic.

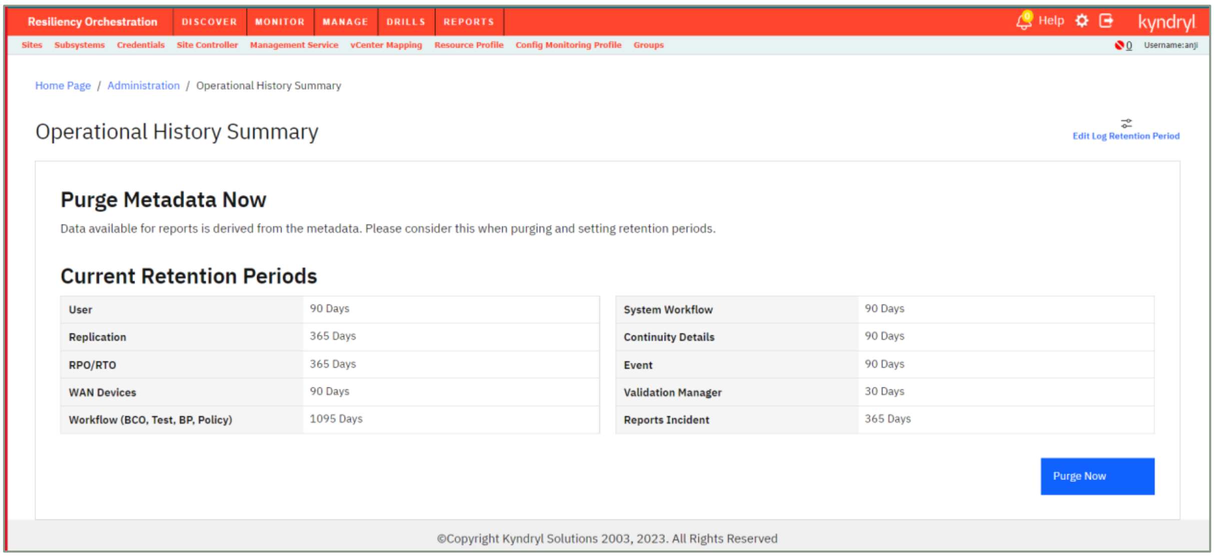
Panaces DB Optimization Procedure

Perform the following steps to release the disk space on PanacesDB:

1. Take a backup of PanacesDB by executing the following commands:

```
mysqldump --single-transaction --skip-disable-keys -uroot -
p<Password> --databases panaces --triggers --routines >
/var/lib/mysql/Panaces_DB_DUMP.dmp
```

2. Navigate to Kyndryl Resiliency Orchestration Server Operational History Management page and click Purge Now option.



Operational History Summary

Purge Metadata Now

Data available for reports is derived from the metadata. Please consider this when purging and setting retention periods.

Current Retention Periods

User	90 Days	System Workflow	90 Days
Replication	365 Days	Continuity Details	90 Days
RPO/RTO	365 Days	Event	90 Days
WAN Devices	90 Days	Validation Manager	30 Days
Workflow (BCO, Test, BP, Policy)	1095 Days	Reports Incident	365 Days

©Copyright Kyndryl Solutions 2003, 2023. All Rights Reserved

3. Stop the Panaces services.

4.Optimize the following tables by executing the following commands:

```
o  MariaDB [panaces]> optimize table incident_log;
o  MariaDB [panaces]> optimize table action_log;
o  MariaDB [panaces]> optimize table
   action_execution_log_detail;
o  MariaDB [panaces]> optimize table protection_log;
o  MariaDB [panaces]> optimize table reports_incident_log;
```

- Check the diskspace after optimizing the tables:

```
prompt>> cd /var/lib/mysql/panaces

prompt>> du -sh * | sort -hr | head
```

5. Start the Panaces services.

Post Validation Step

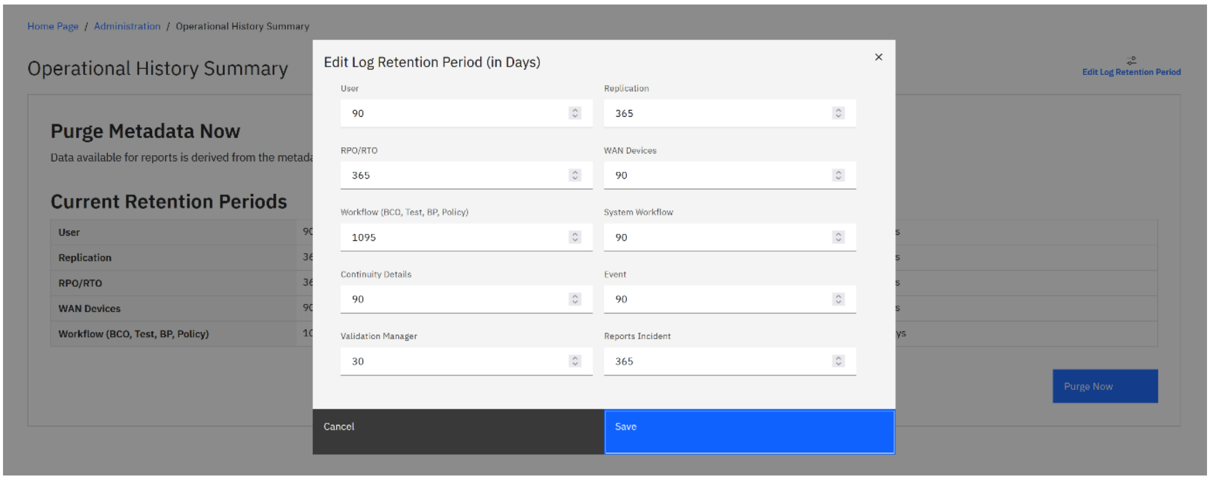
As part of post validation step, you can log in to CRO UI page and verify if all CRO pages has the required data.

Rollback Procedure

If there are any errors during execution or if something goes wrong, you can restore Panaces DB from the already taken backup file.

```
mysql -uroot -p<Password> < /var/lib/mysql/Panaces_DB_DUMP.dmp
```

Edit Log Retention Period(In Days)


Home Page / Administration / Operational History Summary
Operational History Summary
Edit Log Retention Period
Purge Metadata Now
Data available for reports is derived from the metada
Current Retention Periods
User
Replication
RPO/RTO
WAN Devices
Workflow (BCO, Test, BP, Policy)
Purge Now
×
Cancel
Save

Edit Log Retention Period (in Days)

User: 90	Replication: 365
RPO/RTO: 365	WAN Devices: 90
Workflow (BCO, Test, BP, Policy): 1095	System Workflow: 90
Continuity Details: 90	Event: 90
Validation Manager: 30	Reports Incident: 365