



Kyndryl Resiliency Orchestration

Release Notes

Version 8.4.9.0



DISCLAIMER

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

COPYRIGHT

©Copyright Kyndryl, Inc. 2003, 2024.

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

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

TRADEMARK INFORMATION

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

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



CONTENTS

<i>Introduction</i>	4
<i>Acronyms</i>	4
<i>What's New</i>	6
Enhancements of RO Platform.....	6
Enhancement of the Purge feature	6
Enhancement in the Reports.....	6
Management Service Enhancements.....	7
Resiliency Block Replicator (RBR) based DR Solutions Enhancements.....	7
ROAD on Kubernetes solution enhancements	8
Zerto solution enhancement.....	8
VM Protection with VMware SRM (vSphere Replication) enhancement	8
Enhancements of Automated Discovery Deployment and Configuration (AD2C)	8
<i>Security</i>	9
<i>Customer Tickets</i>	10
<i>Compatibility Information</i>	12
Supported Platforms	12
Supported Browsers.....	12
Installing Resiliency Orchestration	12
Upgrading Resiliency Orchestration to the latest version.....	13
<i>Known Limitations</i>	14



Introduction

This document captures information on the new product features, new Disaster Recovery (DR) and Cyber Resiliency (CR) solutions supported enhancements and known limitations of Resiliency Orchestration software Service Pack version 8.4.9.0.

Acronyms

Acronym	Definition
ADC	Application Defined Continuity
AG	Application Group
API	Application Programming Interface
AWS	Amazon Web Services
CIR	Cyber Incident Recovery
CLI	Command Line Interface
COS	Cloud Object Storage
CR	Cyber Resiliency
DR	Disaster Recovery
DRaaS	Disaster Recovery as a Service
FO	Failover
FOTE	Failover Test Exercise
FQDN	Fully Qualified Domain Name
LPAR	Logical Partition
PIT	Point in Time
PR	Primary
RAL	Recovery Automation Library
RBAC	Roll-Based Access Control



RBR	Resiliency Block Replicator
RG	Recovery Group
RHEL	Red Hat Enterprise Linux
RO	Resiliency Orchestration
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RFR	Resiliency File Replicator
SB	Switchback
SO	Switchover
SP	Service Pack, Spectrum Protect
SR	System Replicator
UI	User Interface
VM	Virtual Machine



What's New

The Resiliency Orchestration (RO) 8.4.9.0 version can be installed fresh or upgraded from previous RO releases. The highlights of this release are mentioned below. This version is available in both English and Japanese languages.

Enhancements of RO Platform

The current version of RO is certified with the following Operating Systems, Database Platforms, Web Servers, and JDK:

O/S Platform	D/B Platform	Web Server	JDK
RHEL 9.3 (Plow)	Maria DB: <ul style="list-style-type: none"> 10.5.24 10.5.22 	Apache Tomcat: <ul style="list-style-type: none"> 9.0.86 9.0.85 9.0.84 	<ul style="list-style-type: none"> Azul Zulu JDK 8.0.402 OpenJDK Runtime Environment (build 1.8.0_392)

The certified combinations are mentioned in the table. This does not mean that the other combinations will not work for RO. For more information, refer to the Kyndryl Resiliency Orchestration Installation Guide.

Enhancement of the Purge feature

The purge feature has been enhanced to enable you to clean up the high volume of the purged data automatically.

Enhancement in the Reports

The following reports have been added:

- DR drill report:** A new report is now available under the Report section to obtain the DR Drills along with the status for a selected group and for a selected duration. The success percentage is also captured.
- Group summary report:** A new report is now available under the Report section to obtain the summary report for all activities and the status for a selected group and for a selected duration. The success percentage is also captured.



- **Test Summary Report:** A new report is now available under the Report section to obtain the Test summary and status for a selected group and for a selected duration. The success percentage is also captured.

For more information, refer to the Kyndryl Resiliency Orchestration Admin Guide.

Management Service Enhancements

Credential Label dropdown has been added to the Management Service, allowing users to select different group credentials for performing Test Credentials. Group Credentials can be modified.

Resiliency Block Replicator (RBR) based DR Solutions Enhancements

Resiliency Block Replicator (RBR) based DR solution has been enhanced with the following bug fixes:

- Removal of pair does not delete the virtual device entry in DMC.
- During VM onboarding under RBR, added validation for the maximum disk count which is supported.
- This solution has also been enhanced with new code to change recovery IP after starting FOTE.
- VIB version update at cluster level: Upgrading the VIB at cluster level is available to you by following the given steps, provided the VIB is manually installed at the host level.
- Introduced RHEL 8.8 support in NICRA.

These are the appropriate versions for the current release:

- VIB IO Filter 3.4.9: ibmrbr-c_3.4.9-1.0.0000_233526552-package.zip
- DMC ISO 3.4.5: DMC_VS_17_149_82ee689_3.4.5.iso
- AIX 3.4.8: RBRIP-AIX61-03.04.0008.0000-DEV20240215035517.rs6000.tar.Z
- NICRA 3.4.9: Resiliency-Block-Replicator-ADB-3.4.9.0.0-20240304052827.x86_64.rpm
- RHEL 8.6 and RHEL 8.8



ROAD on Kubernetes solution enhancements

This solution has been enhanced to support the following versions of OS and Platforms:

- Kubernetes version: 1.28.2
- Master node: RHEL 8.8, RHEL 9.3
- Worker nodes: RHEL 8.8, RHEL 9.3
- OS where NFS Service is running: RHEL 8.8, RHEL 9.3
- Podman: 4.4.1
- Cri-o: 1.28.2
- Cert-manager: v1.12.0
- KEDA: 2.13.0
- MetallB: 0.14.3
- Helm: v3.14.2
- ActiveMQ Artemis: 2.27
- Mariadb(K8s): 10.6.5

Zerto solution enhancement

This solution has been enhanced to support Zerto version 10.

VM Protection with VMware SRM (vSphere Replication) enhancement

This solution has been enhanced to support SRM version 8.8.

Enhancements of Automated Discovery Deployment and Configuration (AD2C)

The Automated Discovery Deployment and Configuration (AD2C) has been enhanced with the following:

- The **RO Download Configuration** feature is now extended to Sites and Site Controllers.
- **Re-discovery** button on the Discovery page has been disabled.



- AD2C Custom Certificate generation capability is now available. The customer can generate their own security certificate.
- For the Zerto solution, the Solution_Configuration.csv file, which is used during the Discovery of the solution using the AD2C has been enhanced with the version column.

Security

Key security enhancements and updates have been added to this release.



Customer Tickets

The following table displays the customer tickets which are resolved/periodically are getting resolved.

Ticket	Description
INCNA11349571	There is an AD2C SSH credential connectivity issue.
INCNA11311704	Unable to delete Protection schema Using AD2C.
INCNA11227854	Random RepInfo scans are getting stuck.
INCNA11303805	RBR Clone VM failed to Obtain the IP Address.
TS010693011	Unit Agents Reg Entry gets changed.
INCNA11129109	Changing password credentials for service accounts.
TS014421097	Credential failing during dataset creation.
INCNA11193151	Users are unable to fetch the RPO Trend reports.
INCNA11101214	From the Anomaly Scan, the encrypted VMs are getting excluded.
INCNA11227300	While changing the Always On availability group an error is displayed "java.sql.SQLException: Incorrect syntax near '\-\'."
TS014498349	In Oracle RAC Archive logs with Dataguard, the discovery of RG with 8 primary nodes and 6 secondary nodes is failing.
INCNA11174112	Users are not able to create a Protection Schema for Oracle Data Guard using AD2C.
INCNA11008807	Issues have been observed with the large number of login attempts for OS users on Remote agents (ref. TS014469143)



INCNA11107135	RO allows RO application user to reset their password with old password.
INCNA11192784	DR group summary Report shows DR impaired although dependent RG is healthy and in DR ready state.
INCNA11190942	DR group summary Report is showing impaired.
INCNA11188504	DMZ Local agent connectivity issue has been found.
INCNA11008807	The issue has been found on a large number of login attempts for OS users on Remote agents.
INCNA11123825	Users are unable to login RO application.
TS013604987	Users are unable to migrate UniAgents from AgentNode to SiteController.
TS013506424	An error is displayed when you create groups in RO for AD2C.
INCNA11113714	An issue has been raised for the dependency on the Oracle DG solution.
INCNA11089904	Users are unable to delete component NETAPPTTESTDRMUM.
INCNA11008803	The .tar is getting failed to transfer files from DC-DR.
INCNA11106867	You are unable to delete protection scheme- insprac2_172.20.229.43_PR_inspcdb2
INCNA11039301	NetApp data RPO is not getting calculated.
INCNA10384735	You get the problem when you start agents after rebooting (automated) Windows SC.
INCNA11261156	Unable to compute RTO is displayed in RGs status.
INCNA10992784	You get a Username password error for the DR DataGuard Protection Scheme.



INCNA11303641	There is an error for the patch request to compute RTO (rp4vm/Oracle/MSSQL).
INCNA11250991	You cannot create Components, Group using AD2C.
INCNA11261072	The impaired status is displayed in the DR group summary Report.
INCNA11315231	Production Site Controllers are showing disconnected
INCNA11370092	VIT related to SSL Certificate Signed Using Weak Hashing Algorithm
INCNA11049950	Getting Snapshot Manager to report in email with the error message "Invalid URL found while preparing HTML message." No data available in the email content
INCNA11101214	During the Anomaly scan encrypted VMs are erroneously getting excluded <added>
INCNA11257525	Login is much slower than expected (Forward ported the fix provided to customer Anthem into the current branch) <added>

Compatibility Information

Supported Platforms

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

Supported Browsers

To know more about supported browsers, refer to the Resiliency Orchestration Installation Guide.

Installing Resiliency Orchestration

Refer to the Resiliency Orchestration Installation Guide for prerequisites, system requirements, and steps to install Kyndryl Resiliency Orchestration software and its components.



Upgrading Resiliency Orchestration to the latest version

Refer to the Resiliency Orchestration Upgrade Guide for prerequisites, system requirements, and steps to upgrade to the latest version of Resiliency Orchestration.



Known Limitations

This version of Resiliency Orchestration software has the following limitations:

Solution Name/ Component	Known Limitation	Workaround
RO	Data Lag, Data RPO and App RPO reports are not supported but are still available for AG groups.	User must not generate Data Lag, Data RPO and App RPO reports for AG groups.
	Active MQ console for Windows functionality is not working.	Navigate to \$EAMSROOT/installconfig/Sitecontroller.cfg > Add the IP address in PANACES_SITE_CONTROLLER_BIND_ADDRESS="Windows SC IP Address" Example- PANACES_SITE_CONTROLLER_BIND_ADDRESS=192.168.20.161.
	The new installation of RO/SC/agents will have new certificates. In case users have done a fresh installation in the agent but still have custom/old certs in RO/SC, the local agent will not get connected to the RO/SC.	Copy truststore from RO > Local Agents so that the Local Agents get connected to RO/SC. For more information, refer to the Installation Guide.
	The Third-Party Directory Server configuration in the Installer (both UI and Silent/Console mode) is not supported.	Resiliency Orchestration needs to be installed in Basic Authentication mode and then it needs to be switched to AD Authentication mode using DRMChangeUserMgmtMode.sh script for Single Organization mode. For Multiple Organization modes, this switch from Basic Authentication to AD needs to be done using CLI SubscriberManager.sh.
	zOS solution needs to be configured again in case Resiliency Orchestration is upgraded from 8.0 or older versions. It is not necessary to reconfigure if you are upgrading RO from 8.1 or higher versions.	zOS upgrade is not supported before RO 8.0. If the user upgrades RO, then he has to delete the existing group and rediscover the group.
	SRM RALs will not have the correct failure paths if the	1. Import workflow for standard workflows from \$EAMSROOT/workflows/VMwareSR



	<p>upgrade is done from version 8.3.3 to the latest version.</p>	<p>M/vSphere, and any customized workflow, export by using the workflow configurator tool add the failure path manually to the next RAL and import workflow, and then publish. OR 2. Import workflow for the standard workflows from \$EAMSROOT/workflows/VMwareSR M/vSphere, and any customized workflow, edit the workflow, add the failure path manually to the next RAL, and then publish.</p>
	<p>TEMP_DIR path is getting changed in the vmware_vcenter_service.properties file after the upgrade.</p>	<p>In the vmware_vcenter_service.properties file, edit the property WIN_TEMP_DIR = C:/LINUX_TEMP_DIR=/tmp to reflect it as: (should appear in two lines) WIN_TEMP_DIR = C:\ LINUX_TEMP_DIR=/tmp</p>
	<p>When both Jackrabbit HTTPS and Firewall are enabled in RO, the user will not be able to perform the Low-touch upgrade for Agent, and the following error message is displayed: <Date> <Time>: ROAGENT_UPGRADE_ERR OR: Resiliency Orchestration Agent Upgradation failed with the error message: Runtime Error : Please Retry later, Remark : REPOSITORY_ERROR: Unknown Repository error: java.rmi.ConnectIOException : Exception creating connection to: <IP Address>; nested exception is: java.net.NoRouteToHostException: No route to host</p>	<p>Tomcat chooses some dynamic port when Jackrabbit starts. The download of the binaries is picked up by that dynamic port. Though Jackrabbit repository UI is coming up and check-in of binaries is also happening the downloading of binaries to the local agent is failing. So, the user must enable the dynamic port in the RO. To identify the dynamic port, 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</p>



	<p>(Host unreachable) Rollback successfully RO Agents version to <Version></p>	<pre>java 1577299 tomcatuser 243u IPv4 17815178 0t0 TCP *:<PortNumber> (LISTEN)</pre> <p>Add the port to the firewall exceptions using the following commands: <code>firewall-cmd --zone=public --add-port=<PortNumber>/tcp --permanent</code></p> <p><code>firewall-cmd --reload</code></p> <p>To verify the port after reloading the firewall, execute the following command: <code>firewall-cmd --list-all</code></p>
	<p>RO Base version failure:</p> <p>While upgrading the RO to the latest version, if it fails with pre-check, or with a wrong version format issue, the below error message displays.</p> <p>Error message: Base Kyndryl Resiliency Orchestration Version <version> format is not correct as per RO Versioning Standard.</p>	<p>Contact the RO Support team.</p>
	<p>Some Remote Agents are not visible on the Agents Page.</p>	<p>Every time you restart any or all the services, ensure that the Site Controller must start first and then start the Panaces service to resolve this issue.</p> <p>Otherwise, users need to go to SiteController and start all missing agents.</p> <p>Example: <code>./VcenterAgent.sh start 192.168.6.51 LINUXSERVER</code></p>
	<p>In the RO UI, the Notification bell icon reports an event count less than the actual number of the raised events.</p>	<p>Ignore the count.</p>
	<p>During the RO upgrade, after importing Database, when you try to import users.sql,</p>	<p>Delete all the queries involving panaces_goldencopy in the users.sql file and then import.</p>



	<p>the following error is displayed:</p> <p>ERROR 1146 (42S02): Table 'panaces_goldencopy.report_db2_continuity_details' doesn't exist</p>	
	<p>While configuring the email notification, the 'Use Mail Authenticator' check-box appears as checked by default. Even after unchecking the checkbox and clearing the 'User Account' details, and saving it, if you again open the same dialog box, the check-box appears as checked again with the filled up details of the 'User Account'.</p>	RO supports email authentication only.
Validation Manager	PDF reports display incomplete information.	
App subsystem with any replicator	Dataset Events are not getting polar canceled.	Manually close the open Events which are not polar canceled.
App PFR	<p>Fallback operation failing with 'PFR Fallback callback failed-SFR-OPR-0003: Create fileset error: Got SocketTimeoutException while reading from socket : java.net.SocketTimeoutException: Read timed out. (for Linux App PFR)</p>	<p>Note: Default value of this "PFR_REQUEST_TIMEOUT" is 3 minutes. Step1. Changed the PFR_REQUEST_TIMEOUT to 10 minutes in at \$SFRROOT\installconfig\PFRConfiguration.cfg file in both PR and DR side machines. 2.Restart the SFR Services 3.Perform the Fallback to check it is in success state.</p>
Site controller mapping	CIDR Range discovery with same IP, different sites and different SCs are supported, but CIDR Range discovery with same IP, same site with different SC is not supported	Not Applicable
Oracle, MSSQL	The feature of converting DB credentials into named credentials by using the	This means this feature is not supported for other solutions.



	PrivateCred2GroupCredMigrator.sh script is supported only for the Oracle and MSSQL solutions.	
	Users are not able to see the RALs in SO/SB workflows in MySQL SR when these are viewed after importing the workflow.	Import workflow again to display the RALs.
RBR	Local writes are not visible in the NICRA post SO, SB and FallbackResynch <Added>	<ol style="list-style-type: none"> 1. Before execution of SO/SB Drill workflows 2. Edit the SO/SB Workflows for RGs level mentioned below and publish the Workflow Go to Reconfiguring the Network for Remote Virtual Machine RAL -> Go to Action Properties -> Execution Mode - Select -Manual Mode 3. Start SO execution once workflow reaches Awaiting Input for the Reconfiguring the Network for Remote Virtual Machine RAL - requires user input Execute below command on DR Nicra and note down the port number and VMDK path of each disk DR-Nicra> dtcresetport -d Execute below esxcli commands in DR ESXi with VM in powered off state for each VMDK path DR-ESXi> /bin/vmkfstools --iofilters ibmrbr:enable_cbt=1:nicraServerPortNumber =<port-no> <vmdk-path> 4. Then RO side go to RG SO drill for the AwaitingInput RAL mentioned Step2 just click continue button and wait for the execution complete for remaining SO RALs. 5. Verify the local writes using cmd dtcmonitortty in DR NICRA. 6. Before execution of SB Edit the SB WF RGs level as mentioned in Step 2. Start SB execution once workflow reaches Awaiting Input for the Reconfiguring the



		<p>Network for Remote Virtual Machine RAL - requires user input</p> <p>Execute below command on Primary Nicra and note down the port number and VMDK path of each disk</p> <p>PR-Nicra> dtcresetport -d</p> <p>Execute below esxcli commands in DR ESXi with VM in powered off state for each VMDK path</p> <p>PR-ESXi> /bin/vmkfstools --iofilters ibmrbr:enable_cbt=1:nicraServerPortNumber =<port-no> <vmdk-path></p> <p>7. Then RO side go to RG SB drill f for the AwaitingInput RAL mentioned Step2 just click continue button and wait for the execution complete for remaining SO RALs.</p> <p>8. Verify the local writes using cmd dtcmonitortty in PR NICRA.</p> <p>Note: If KRO admin user have already executed FO and would like to Execute FB WF then KRO user must follow below steps</p> <p>1. Edit the FBR WF for RG level Go to Reconfiguring the Network for Remote Virtual Machine RAL -> Go to Action Properties -> Execution Mode - Select -> Manual Mode</p> <p>2. Start the FB workflow AG level and user proc with the FBR workflow execution - once workflow reaches Awaiting Input for the Reconfiguring the Network for Remote Virtual Machine RAL - requires user input Execute below command on Primary Nicra and note down the port number and VMDK path of each disk</p> <p>3. PR-Nicra> dtcresetport -d</p> <p>4. Execute below esxcli commands with VM in powered off state for each VMDK path</p> <p>PR-ESXi> /bin/vmkfstools --iofilters ibmrbr:enable_cbt=1:nicraServerPortNumber =<port-no> <vmdk-path></p> <p>5. Then RO side go to FBR WF for the AwaitingInput RAL mentioned Step2 just click continue button and wait for the execution complete for remaining FBR RALs.</p>
--	--	---



		6. Verify the local writes using cmd dtcmonitortty in PR NICRA.
	In this solution, FOTE VMs are not recommended to be kept for more than 72 hours.	If the customer performs the test for more than 72 hours, it is recommended to monitor the data store space where the VMs reside.
	If the VM hostname has a DOT(.) then IP customization will fail.	Remove DOT(.) from the VM Hostname.
	For the AIX IBMPcloud RBR solution, after FOTE is successful, the Group remains in Tracking mode.	Run the dmc cmd for a smart refresh for the group - cmd: "command group LaunchRefresh " then you can see the group turns Tracking to Normal/connected state.
	Simultaneous addition/removal of multiple disks is not supported for a Single VM as NICRA/VIB does not support multiple disk additions.	If you would want to add/remove multiple disks, then you will need to provide disk path key value for one disk at time and then execute ProtectNewVirtualDisk /UnprotectNewVirtualDisk workflow.
	An independent build for AIX 7.2 is not provided for the current release due to an internal build-level challenge.	Build image for AIX 6.1 can also be used for AIX 7.2 without any changes.
OpenShift Protection with Velero and Cloud Native solutions	These solutions are not supported in the current version of RO. These solutions are supported till RO 8.3.9.	Not Applicable.
Veeam	Veeam agent stays in UNKNOWN status.	Update the genericagent-common.bat file available in <Install directory>\bin of site controller, and uncomment the set COMMON_CLASSPATH variable by removing REM at the beginning of the comment line.
MySQL SR	Mysql SR Protection scheme discovery fails with error.	Protection is getting created if "IsCustomReplicator" is set to "true" or "TRUE", if the format of the cell in xls is text. By default, it is not in text format. To make it in text format, right-click on the column> Format Cells > Number tab> Select Text as Category > Click OK.
Application Group (AG)	Deletion of an Application group also results in the	Before deleting AG disassociate underline RG's.



	deletion of standard Recovery groups (RG).	
DS8K	The SCB session field is missing from the snapshot list under the Pending Data tab in the RO UI for the DS8K solution.	This is a known limitation of this solution.
MSSQL Logshipping	This solution is not supported in this release.	Not applicable.