Protecting VMs to and from Oracle Private Cloud Appliance X9-2 with RackWare DR

Oracle and Rackware Inc - Tech Brief | May 2023

May, 2023, Version [1.0]

Table of contents

Introduction **3**

Environment **3**

Installing and Licensing RackWare Management Module (RMM) **4**

Installation 4

Licensing 7

RackWare GUI **8**

Protecting workloads using RackWare DR **8**

Architecture / Network Diagram 8

Prepare Origin and Target 9

Creating a wave 9

Adding Hosts to Wave 10

Wave options 11

Disaster Recovery with RackWare **11**

Available approaches: 11

Creating DR Policy 11

Applying DR Policy 12

Auto-Provisioning **13**

Creating a user on PCA 14

Registering Clouduser on RMM 14

Applying Cloud Configuration to Waves 15

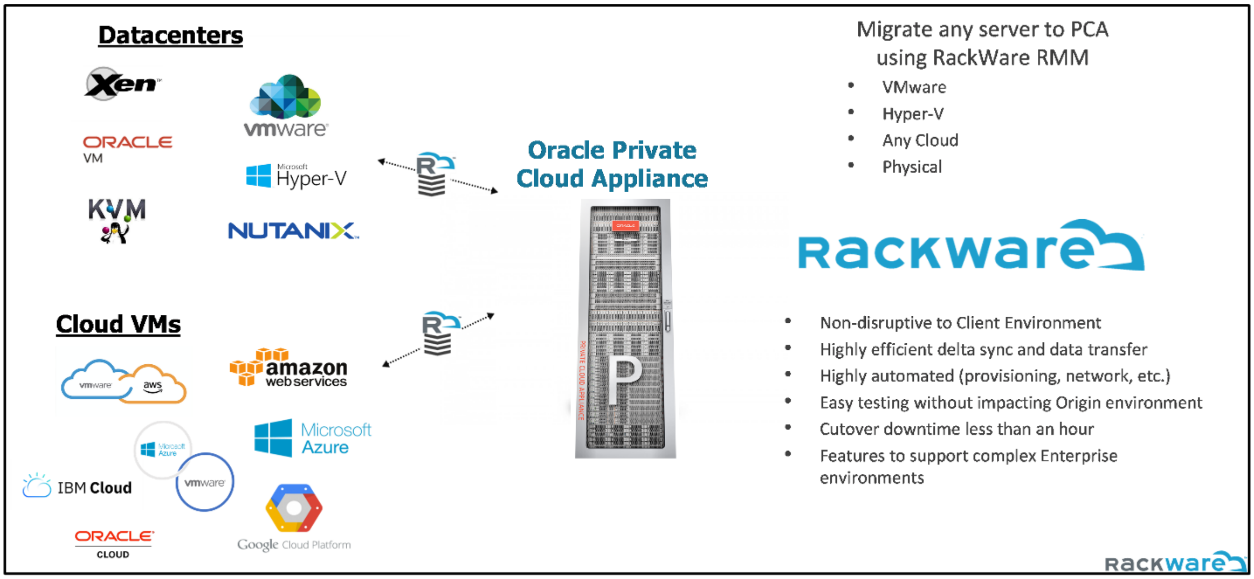
Additional features offered by RackWare RMM **17**

Introduction

RackWare's RMM (RackWare Management Module) is a comprehensive Hybrid Cloud Management solution that provides customers with utmost flexibility in their cloud adoption journey.

PCA X9-2, Oracle's latest in the Private Cloud Appliance product family, provides private cloud infrastructure and architecture consistent with Oracle Cloud Infrastructure (OCI).

RackWare with its true ANY-to-ANY migration, back-up, and disaster recovery capabilities, now allows users to move their workloads into PCA X9-2 from on-prem VMWare, OLCNE, Nutanix, Cloud (AWS, GCP, IBM Cloud, etc.) and older PCA generations. RackWare has also successfully demonstrated its capabilities to protect PCA workloads using Converged DR and Backup by replicating workloads to OCI, remote PCA(s) and other clouds.



Migrate any server to PCA using RackWare RMM

- VMware
- Hyper-V
- Any Cloud
- Physical

- Non-disruptive to Client Environment
- Highly efficient delta sync and data transfer
- Highly automated (provisioning, network, etc.)
- Easy testing without impacting Origin environment
- Cutover downtime less than an hour
- Features to support complex Enterprise environments

Fig. 1 - Platforms supported by RMM to migrate and protect workloads to Oracle PCA

Connectivity to the source and destination environments is over inherently encrypted SSH protocol and RMM is also capable of cloud orchestration in the destination environment using REST APIs over Secure HTTP (HTTPS).

Environment

We can consider 3 scenarios:

	Source / Origin	Target / Destination
1	Cloud	PCA X9-2
2	Older PCA	PCA X9-2
3	PCA X9-2	Cloud

In all scenarios RackWare recommends that the RMM appliance resides in the Destination environment to safeguard against DR events.

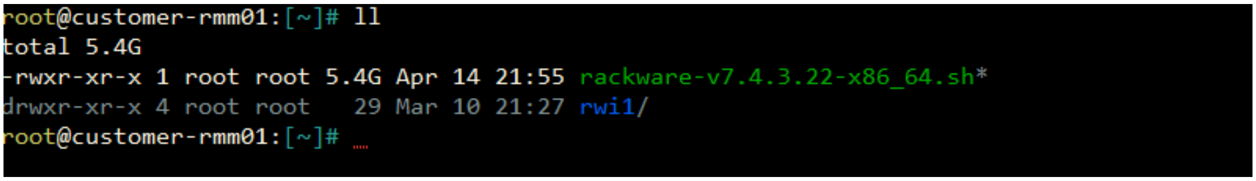
Installing and Licensing RackWare Management Module (RMM)

RackWare Management Module (RMM) software runs on any RHEL based 7.x Linux operating system. RackWare has marketplace listings on major clouds like Oracle Cloud Infrastructure, where users can deploy the instance with a single click and self-start migration activities.

On platforms, where such listings are not available, RackWare provides an installation file.

The RMM installer name takes the form: **rackware-<VERSION>-x86_64.sh**

Ensure that the permissions of this file allow for execution, and if not modify via chmod 755.



```
root@customer-rmm01:[~]# ll
total 5.4G
-rwxr-xr-x 1 root root 5.4G Apr 14 21:55 rackware-v7.4.3.22-x86_64.sh*
drwxr-xr-x 4 root root   29 Mar 10 21:27 rwi1/
root@customer-rmm01:[~]#
```

The RMM software is dependent on various libraries and utilities. The RMM installer checks for these dependencies, and automatically installs any that are missing. The simplest and safest option to ensure that all the correct packages are on the server is to have temporary access to the Internet for the server prior to running the installer. Specifically, ports 80 and 443 should be open in the outbound direction on the RMM and on any firewalls. Note that this step utilizes the standard distribution package manager and requires Internet access.

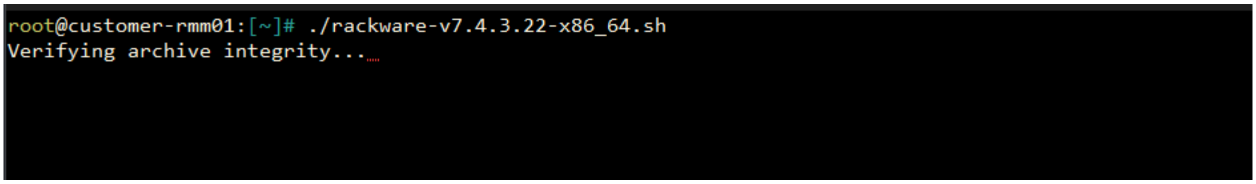
Internet access can be disabled immediately after installation.

Installing the RMM over an existing installation is supported and, in fact, is the mechanism for installing a new version. In this case there will be an existing CMDB, and by default the installation process retains that information. So, after installation all existing resources will continue to reside in the CMDB.

Installation

Step 1. Execute installer by running the following command as **root**:

root@ovh-rmm01:[~]# ./rackware-<VERSION>-x86_64.sh



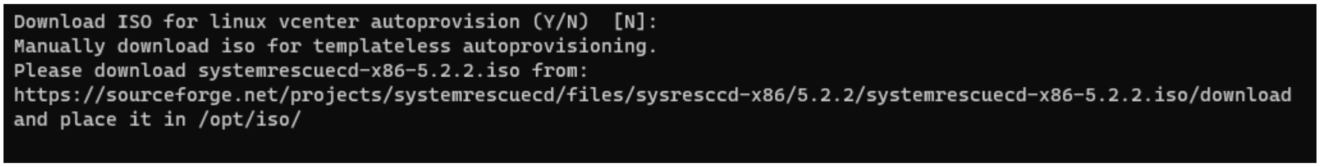
```
root@customer-rmm01:[~]# ./rackware-v7.4.3.22-x86_64.sh
Verifying archive integrity...
```

Step 2. Read and accept the EULA and the Microsoft licenses by entering "yes".

Step 3. Answer the prompts with default values [yes]:

a) perl-CGI
b) EPEL package installation
c) Modify iptables

Step 4. Download ISO for Linux vCenter Auto-Provision



```
Download ISO for linux vcenter autoprovision (Y/N)  [N]:
Manually download iso for templateless autoprovisioning.
Please download systemrescuecd-x86-5.2.2.iso from:
https://sourceforge.net/projects/systemrescuecd/files/sysresccd-x86/5.2.2/systemrescuecd-x86-5.2.2.iso/download
and place it in /opt/iso/
```

This file is needed when auto-provisioning Linux machines into a vCenter. If you are planning on using the RMM to auto-provision Linux machines into a vCenter, then answer ‘Y’. Otherwise, accept the default of ‘N’.

Step 5. Log Rotate

Maintains the sync job logs for a set number of days. Default is 15 days but can be set depending on the length of the project.

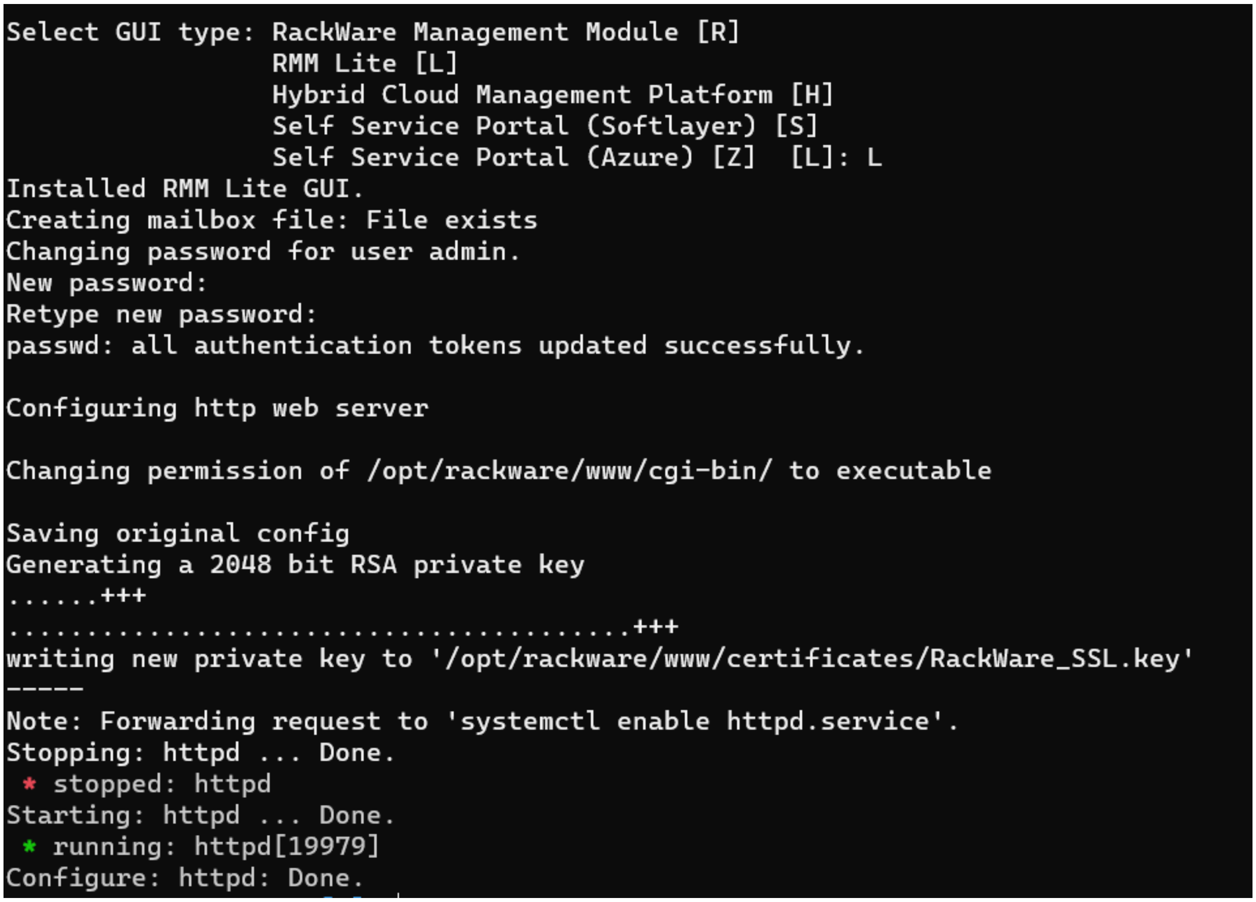
Step 6. RMM-Hub

Unless you are using the RMM-Hub feature, accept the default of N for this prompt.

Step 7. GUI Selection and Configuration:

When prompted for the RMM GUI type, select [L] (default) for RMM Lite.

User will be required to provide and confirm a password for the ‘admin’ user, which is the default user for the GUI.



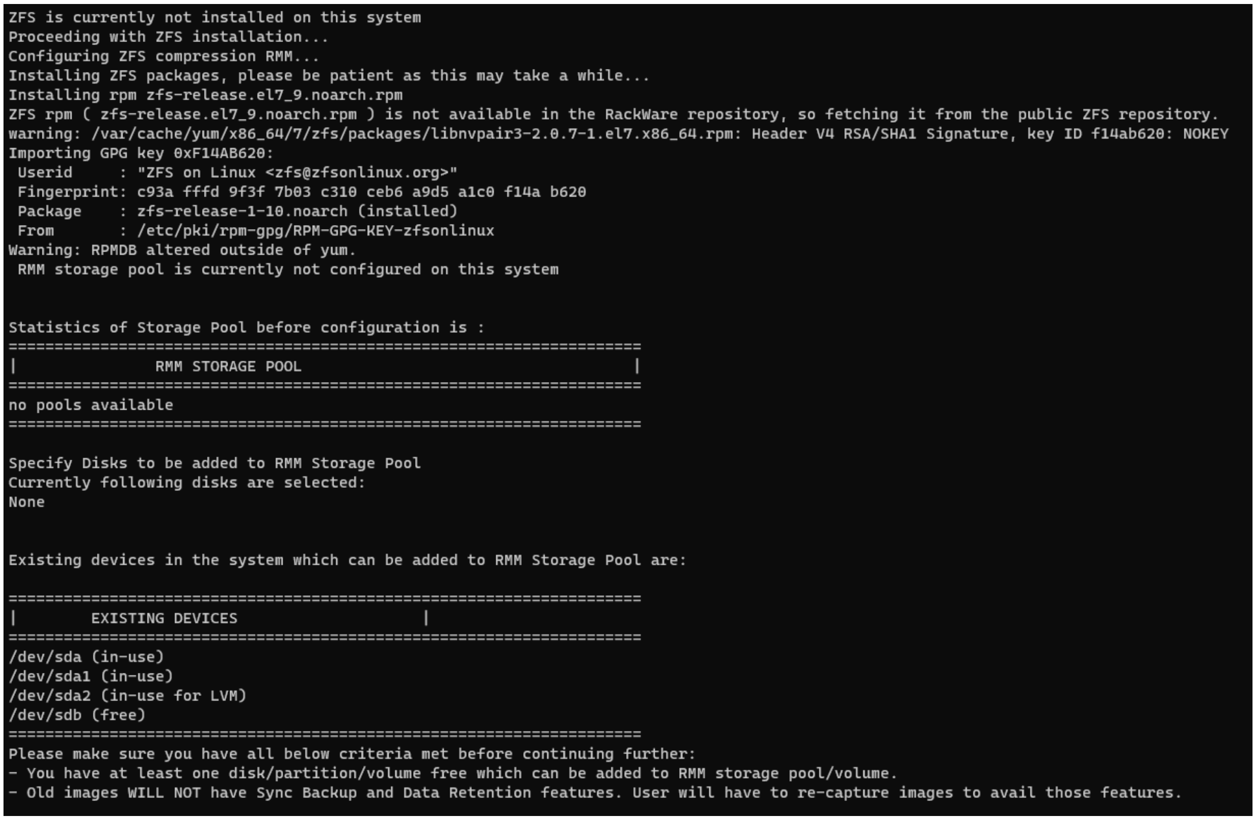
```
Select GUI type: RackWare Management Module [R]
                 RMM Lite [L]
                 Hybrid Cloud Management Platform [H]
                 Self Service Portal (Softlayer) [S]
                 Self Service Portal (Azure) [Z]  [L]: L
Installed RMM Lite GUI.
Creating mailbox file: File exists
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Configuring http web server

Changing permission of /opt/rackware/www/cgi-bin/ to executable

Saving original config
Generating a 2048 bit RSA private key
......+++
........................................+++
writing new private key to '/opt/rackware/www/certificates/RackWare_SSL.key'
-----
Note: Forwarding request to 'systemctl enable httpd.service'.
Stopping: httpd ... Done.
 * stopped: httpd
Starting: httpd ... Done.
 * running: httpd[19979]
Configure: httpd: Done.
```

Step 8. Passphrase

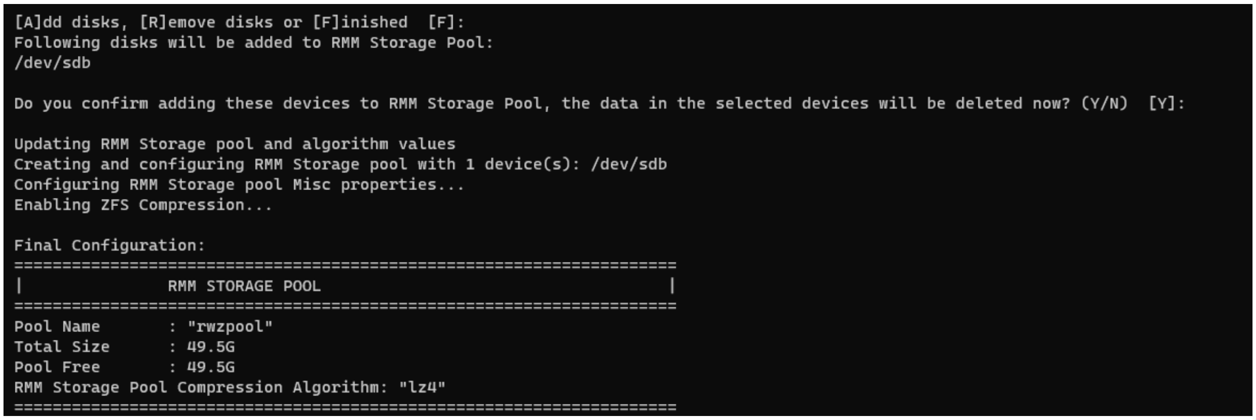
RMM requests users to input a passphrase to encrypt the onboard CMDB using 128-bit AES.

Step 9. Configuring a Storage Pool using ZFS

RackWare uses unformatted / unpartitioned block devices attached to the RMM to configure its storage pool using ZFS.



```
ZFS is currently not installed on this system
Proceeding with ZFS installation...
Configuring ZFS compression RMM...
Installing ZFS packages, please be patient as this may take a while...
Installing rpm zfs-release.el7_9.noarch.rpm
ZFS rpm ( zfs-release.el7_9.noarch.rpm ) is not available in the RackWare repository, so fetching it from the public ZFS repository.
warning: /var/cache/yum/x86_64/7/zfs/packages/libnvpair3-2.0.7-1.el7.x86_64.rpm: Header V4 RSA/SHA1 Signature, key ID f14ab620: NOKEY
Importing GPG key 0xF14AB620:
 Userid     : "ZFS on Linux <zfs@zfsonlinux.org>"
 Fingerprint: c93a fffd 9f3f 7b03 c310 ceb6 a9d5 a1c0 f14a b620
 Package    : zfs-release-1-10.noarch (installed)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-zfsonlinux
Warning: RPMDB altered outside of yum.
 RMM storage pool is currently not configured on this system


Statistics of Storage Pool before configuration is :
====================================================================
|               RMM STORAGE POOL                                   |
====================================================================
no pools available
====================================================================

Specify Disks to be added to RMM Storage Pool
Currently following disks are selected:
None


Existing devices in the system which can be added to RMM Storage Pool are:

====================================================================
|        EXISTING DEVICES                      |
====================================================================
/dev/sda (in-use)
/dev/sda1 (in-use)
/dev/sda2 (in-use for LVM)
/dev/sdb (free)
====================================================================
Please make sure you have all below criteria met before continuing further:
- You have at least one disk/partition/volume free which can be added to RMM storage pool/volume.
- Old images WILL NOT have Sync Backup and Data Retention features. User will have to re-capture images to avail those features.
```

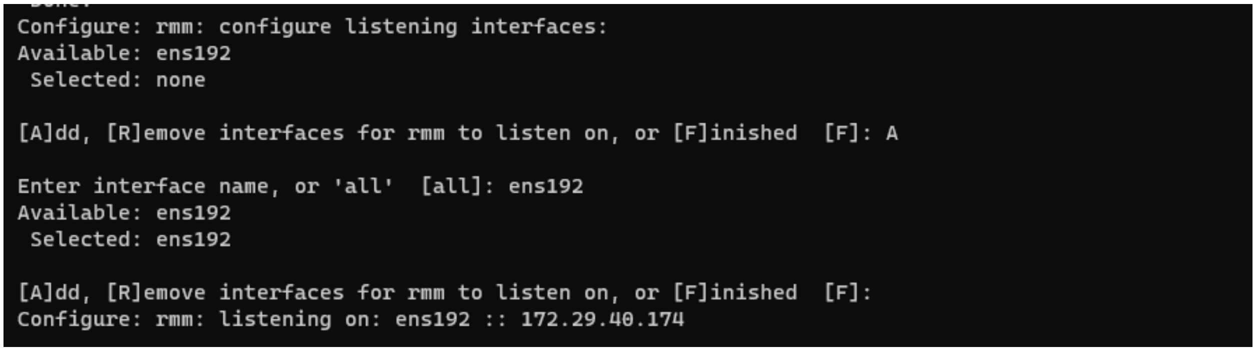


```
[A]dd disks, [R]emove disks or [F]inished  [F]:
Following disks will be added to RMM Storage Pool:
/dev/sdb

Do you confirm adding these devices to RMM Storage Pool, the data in the selected devices will be deleted now? (Y/N)  [Y]:

Updating RMM Storage pool and algorithm values
Creating and configuring RMM Storage pool with 1 device(s): /dev/sdb
Configuring RMM Storage pool Misc properties...
Enabling ZFS Compression...

Final Configuration:
====================================================================
|               RMM STORAGE POOL                                   |
====================================================================
Pool Name       : "rwzpool"
Total Size      : 49.5G
Pool Free       : 49.5G
RMM Storage Pool Compression Algorithm: "lz4"
====================================================================
```

RMM Storage Pool using ZFS can be re-configured any time using the **rwadm zfs configure** command.

Step 10. Configuring Network Interfaces

When prompted for the interfaces on which the RMM will listen, add each of the interfaces the RMM will use to communicate with the source hosts.



```
Configure: rmm: configure listening interfaces:
Available: ens192
 Selected: none

[A]dd, [R]emove interfaces for rmm to listen on, or [F]inished  [F]: A

Enter interface name, or 'all'  [all]: ens192
Available: ens192
 Selected: ens192

[A]dd, [R]emove interfaces for rmm to listen on, or [F]inished  [F]:
Configure: rmm: listening on: ens192 :: 172.29.40.174
```

Step 11. Configuring NTP

The next prompt will ask if the RMM should configure an NTP server. For the RMM to come up properly, the RMM must have access to an NTP server, unless a professional services license is installed.

The default value of N to this prompt means that the RMM will use as the NTP server the default of pool.ntp.org.

If customer chooses to configure NTP server (Enter 'Y' at the prompt), they need to provide the name of the NTP server for the RMM to use.

If the NTP server being used by the RMM is not reachable from the RMM then RMM's license will be temporarily disabled and thus the RMM will not come up.

Step 12. Configuring NAT

The next prompt will ask if a NAT IP needs to be added. Unless otherwise instructed by RackWare,

accept the default value of [F]

Step 13. Rebooting server

Post installation, the server will need to be rebooted once for the installation to complete.

Licensing

The RMM service does not start until a valid license is placed under /etc/rackware.

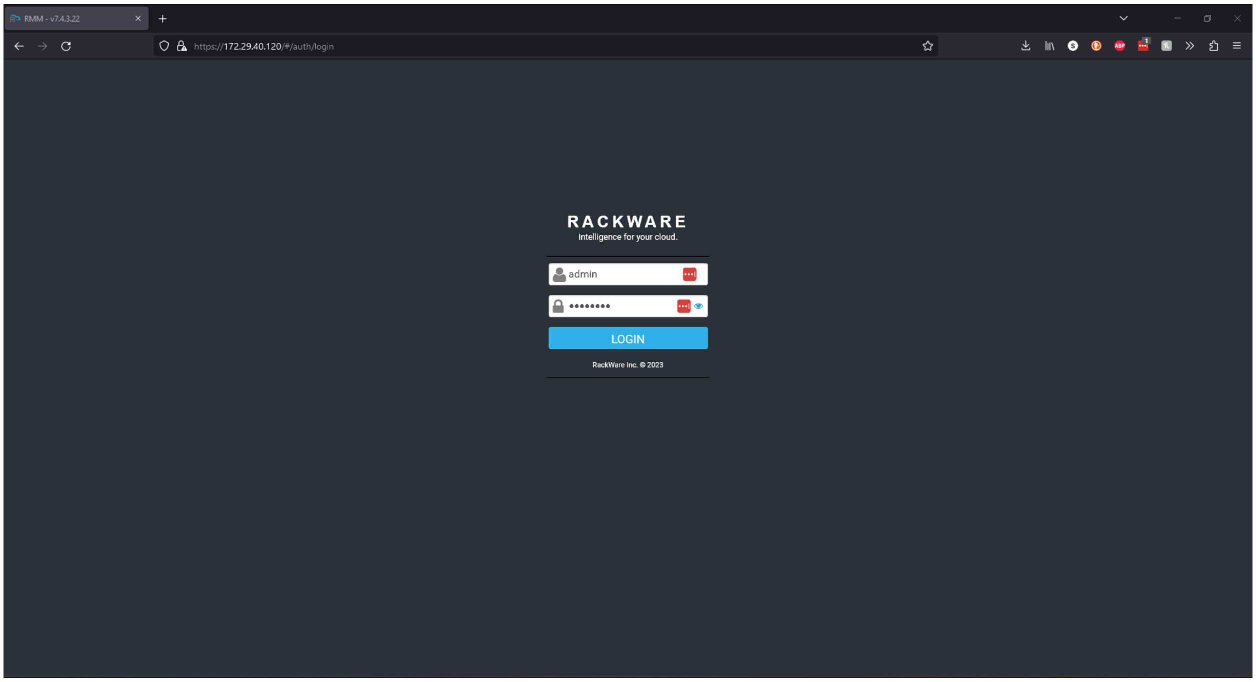
For an initial installation, following messages would be displayed:

License not found in /etc/rackware/.
Generating the preinstall file. Preinstall file generated at **/etc/rackware/rwlicense_preinstall_xxxxxxxx**.
Please email this file to licensing@rackwareinc.com to get the license.

After receiving the license from RackWare, the license file needs to be placed under /etc/rackware and customer can now execute **'rwadm start rackware'**

RackWare GUI

To begin working with RackWare GUI, point the web-browser to the IP address of the instance on which RMM was installed. Login using the ‘admin’ user and the password setup during installation process.


RMM - v7.4.3.22
https://172.29.40.120/#/auth/login
RACKWARE
Intelligence for your cloud.
LOGIN
RackWare Inc. © 2023

admin

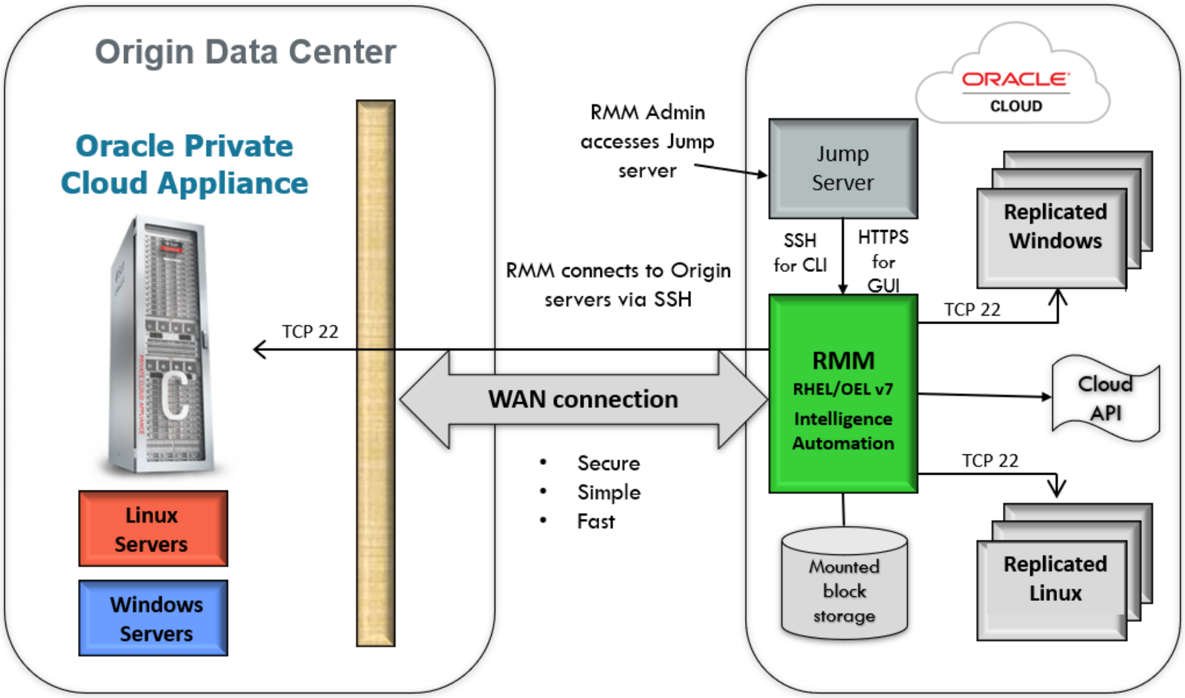
•••••••••

Protecting workloads using RackWare DR

RackWare DR protects workloads grouped as a collection and are referred to as waves. A collection can be a set of applications or user requirement for migration. Before RackWare DR can protect the workloads, the user needs to prepare the Origin and Target hosts.

Architecture / Network Diagram

The most common configuration is to have the RMM establish a TCP connection directly to the Origin server. The diagram below shows the topology and ports that need to be opened when the RMM is performing a Capture/Sync operation to a physical or virtual server in the Target environment.



Prepare Origin and Target

All origin and target hosts need to have password-less SSH access enabled from the RMM over TCP/22 port (Custom ports are also supported with additional configuration).

Linux

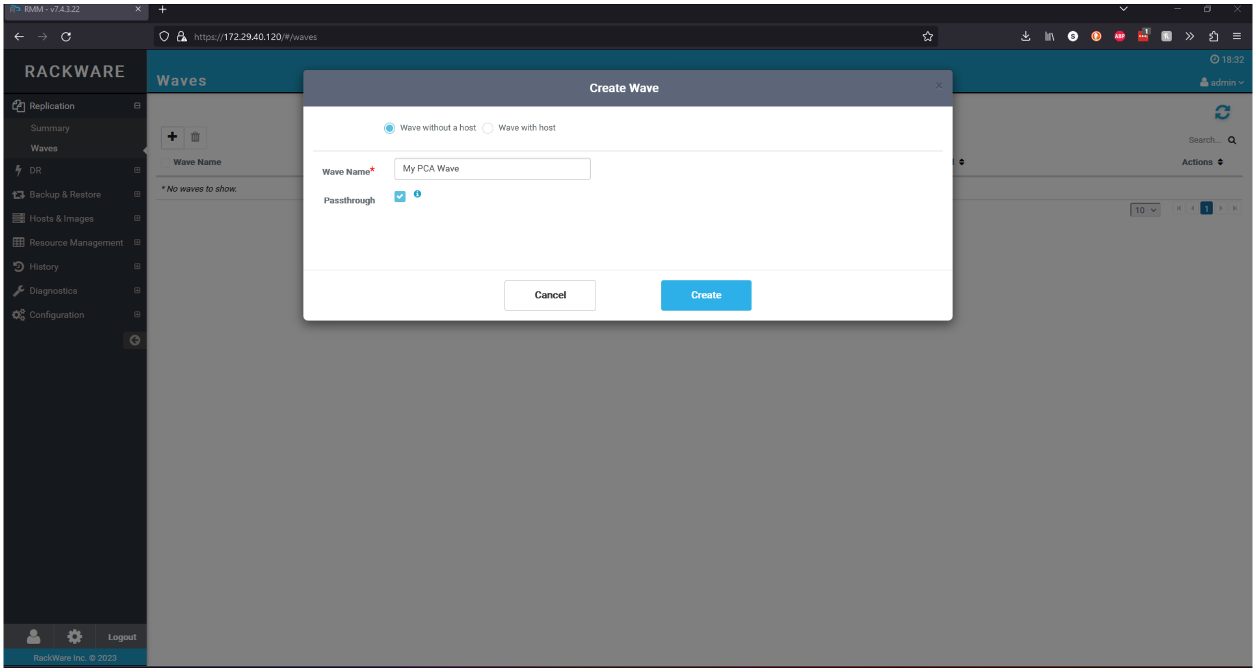
- Access Credentials: root user OR user with sudo privileges
- Storage:
  - Origins' volume groups must have 15% of used space available as free extents.
  - /var/tmp should have 20 MB of free space available.
- no-exec: /tmp and /var/tmp filesystems should not be configured with no-exec properties in fstab.
- Grub: Origin servers should have /etc/default/grub file
- Antivirus: If any antivirus program is running on Origin, it should whitelist /mnt/rackware/ directory

Windows

- Access Credentials: SYSTEM user or local user with administrative privileges.
- Storage: Each volume should have sufficient free space (approx. 20%) for VSS snapshots.
- Antivirus: Origin should whitelist rsync.exe, rwattr.exe, rwchangesvc.exe and rw_tngsync_util.exe for any antivirus program or Windows Defender
- Language: For any language other than English for SYSTEM locale, contact RackWare Support.

Creating a wave

To create a wave, simply navigate to Replication -> Waves and click on the plus (+) icon to open the wave create wizard. Provide a name and click create.



Create Wave

● Wave without a host ○ Wave with host

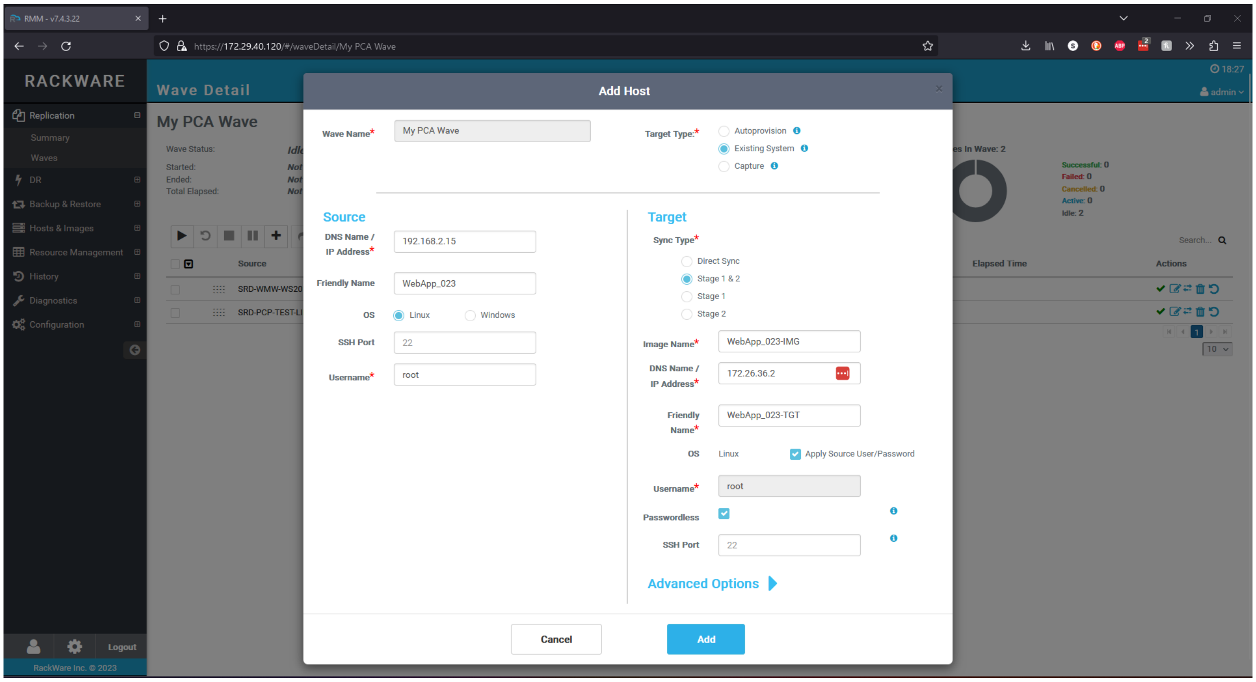
Wave Name*: My PCA Wave

Passthrough: ☑

Cancel | Create

Adding Hosts to Wave

To add host to a wave, click on the wave to inspect. Then click on the add button (✚). The following wizard should pop up allowing users to add the host's details:



Add Host

Wave Name*: My PCA Wave

Target Type:* ○ Autoprovision ● Existing System ○ Capture

Source

DNS Name / IP Address*: 192.168.2.15

Friendly Name: WebApp_023

OS: ● Linux ○ Windows

SSH Port: 22

Username*: root

Target

Sync Type*: ○ Direct Sync ● Stage 1 & 2 ○ Stage 1 ○ Stage 2

Image Name*: WebApp_023-IMG

DNS Name / IP Address*: 172.26.36.2

Friendly Name*: WebApp_023-TGT

OS: Linux ☑ Apply Source User/Password

Username*: root

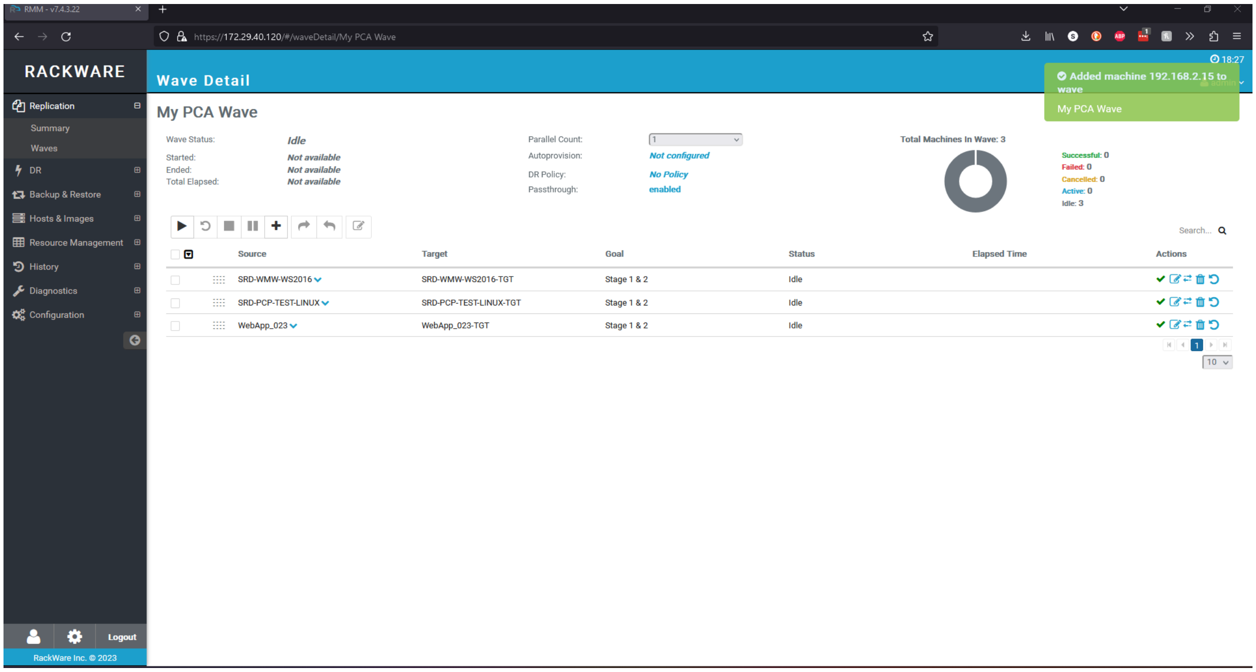
Passwordless: ☑

SSH Port: 22

Advanced Options

Cancel | Add

User can add multiple hosts to a wave:



Wave Detail

Added machine 192.168.2.15 to wave

My PCA Wave

My PCA Wave

Wave Status: Idle

Started: Not available

Ended: Not available

Total Elapsed: Not available

Parallel Count: 1

Autoprovision: Not configured

DR Policy: No Policy

Passthrough: enabled

Total Machines In Wave: 3

Successful: 0

Failed: 0

Cancelled: 0

Active: 0

Idle: 3

Source	Target	Goal	Status	Elapsed Time	Actions
SRD-WMW-WS2016	SRD-WMW-WS2016-TGT	Stage 1 & 2	Idle		
SRD-PCP-TEST-LINUX	SRD-PCP-TEST-LINUX-TGT	Stage 1 & 2	Idle		
WebApp_023	WebApp_023-TGT	Stage 1 & 2	Idle		

Wave options

- Parallel Count: Allows user to set the number of parallel transfers within the wave.
- Auto Provision: Users can configure the RMM to provision targets via API calls to the target cloud.
- DR Policy: User can configure a policy to periodically synchronize all the hosts in the wave.
- Passthrough: When enabled, data flows via RMM. (Origin -> RMM -> Destination)

Disaster Recovery with RackWare

Available approaches:

RackWare allows users to protect their workloads in 2 ways depending on customer's requirements of RPO, RTO and Cost.

Dynamically Provisioned Targets:

Users can opt to protect their workloads by maintaining a copy of the origin server's image on the RMM. This image can then be used to deploy an instance on the target infrastructure on demand in case of a DR event.

This approach can significantly reduce costs and lower the RPO at the expense of higher RTO.

Pre-Provisioned Targets:

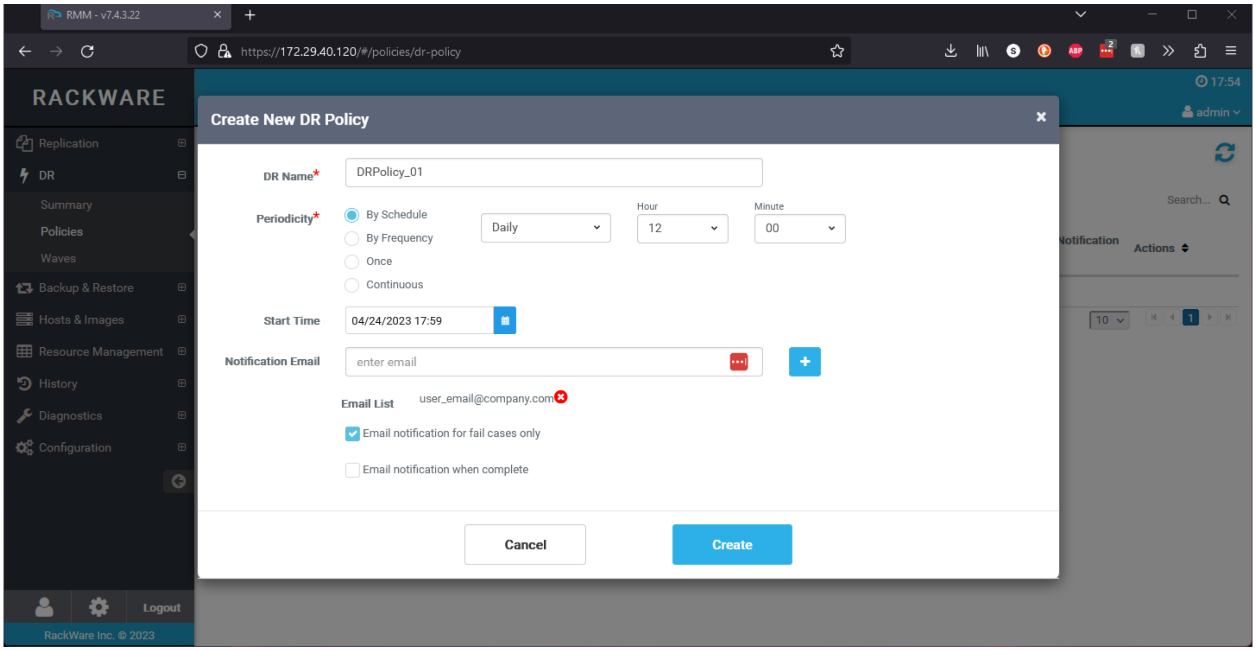
Users can opt to protect their workloads by maintaining an active server instance on the target infrastructure in addition to the origin server's image on the RMM. Synchronization jobs are configured to update the image as well as the target server at user specified intervals.

This approach achieves the lowest RTO but is costly as an active DR site is always maintained.

Creating DR Policy

A DR policy allows users to synchronize deltas from source to its image captured on the RackWare RMM and target instance (in case of pre-provisioned scheme) at user specified intervals.

Users can create as many DR Policies as required with different periodicity. This allows greater flexibility to synchronize different waves at varied intervals based on the user's DR strategy.



Create New DR Policy

DR Name* DRPolicy_01

Periodicity* ● By Schedule ○ By Frequency ○ Once ○ Continuous — Daily — Hour 12 — Minute 00

Start Time 04/24/2023 17:59

Notification Email enter email

Email List user_email@company.com

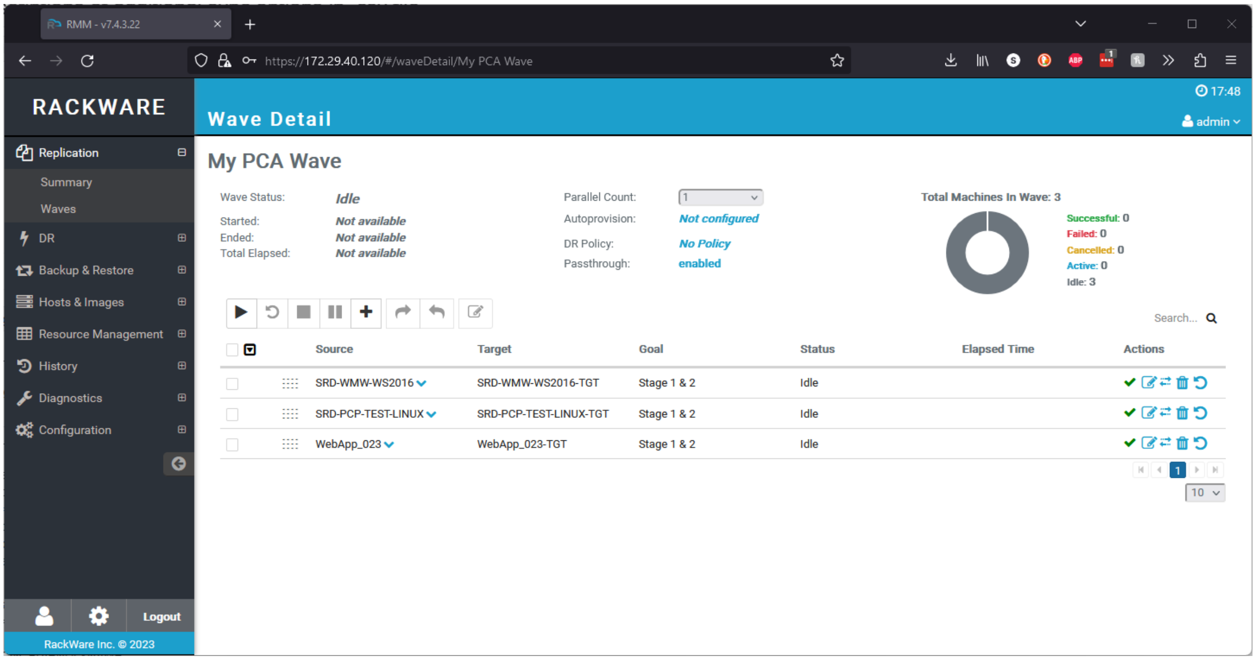
☑ Email notification for fail cases only

□ Email notification when complete

Cancel Create

Applying DR Policy

To apply a DR policy, user can simply click on '***No Policy***' which will open a Configuration dialog box.



Wave Detail

My PCA Wave

Wave Status: *Idle*

Started: *Not available*

Ended: *Not available*

Total Elapsed: *Not available*

Parallel Count: 1

Autoprovision: *Not configured*

DR Policy: *No Policy*

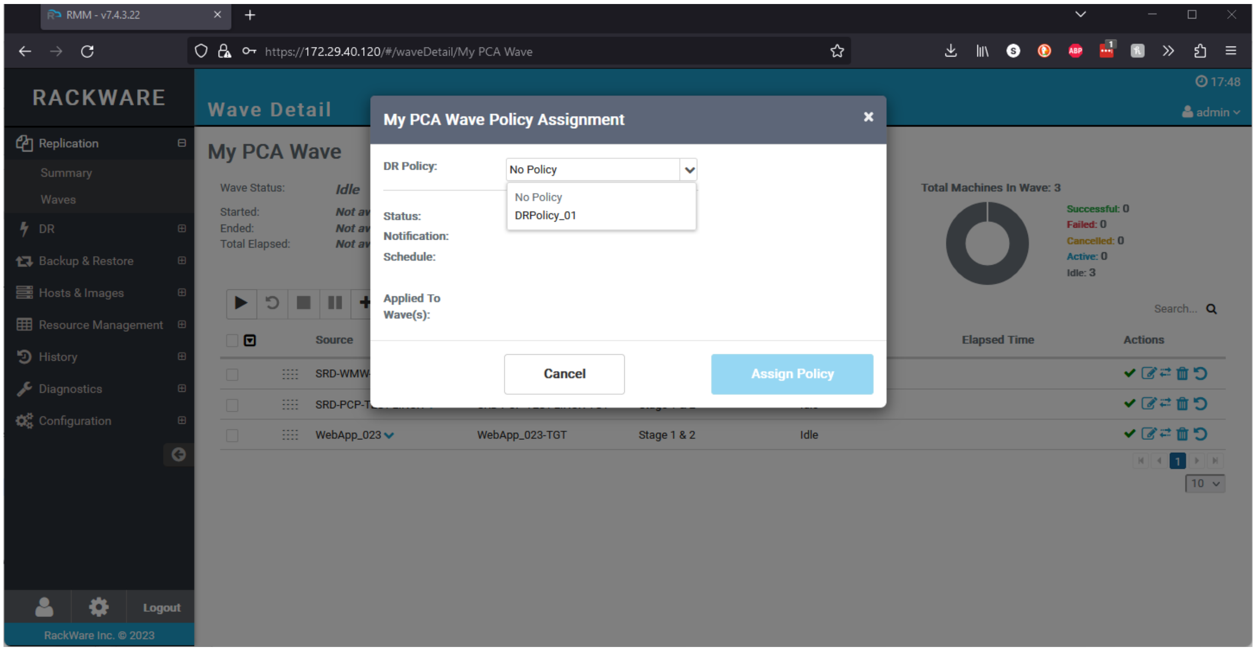
Passthrough: enabled

Total Machines In Wave: 3

Successful: 0
Failed: 0
Cancelled: 0
Active: 0
Idle: 3

Source	Target	Goal	Status	Elapsed Time	Actions
SRD-WMW-WS2016	SRD-WMW-WS2016-TGT	Stage 1 & 2	Idle		
SRD-PCP-TEST-LINUX	SRD-PCP-TEST-LINUX-TGT	Stage 1 & 2	Idle		
WebApp_023	WebApp_023-TGT	Stage 1 & 2	Idle		

Select which policy needs to be applied to the current wave and click on the '***Assign Policy'*** button.



My PCA Wave Policy Assignment

DR Policy: No Policy

- No Policy
- DRPolicy_01

Status:

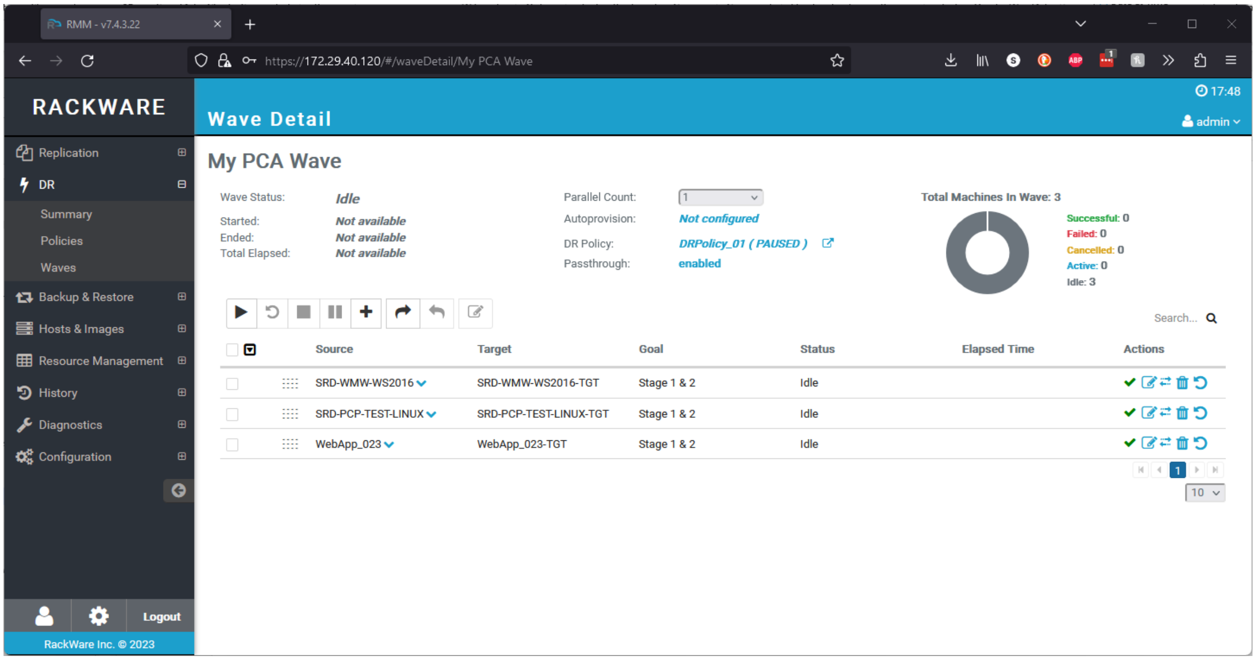
Notification:

Schedule:

Applied To Wave(s):

Cancel | Assign Policy

Assigning a policy to a wave will move the said wave from *Replication->Waves* to *DR->Waves* as it's now configured for DR.



My PCA Wave

Wave Status: Idle
Started: Not available
Ended: Not available
Total Elapsed: Not available

Parallel Count: 1
Autoprovision: Not configured
DR Policy: DRPolicy_01 (PAUSED)
Passthrough: enabled

Total Machines In Wave: 3
Successful: 0
Failed: 0
Cancelled: 0
Active: 0
Idle: 3

Source	Target	Goal	Status	Elapsed Time	Actions
SRD-WMW-WS2016	SRD-WMW-WS2016-TGT	Stage 1 & 2	Idle		
SRD-PCP-TEST-LINUX	SRD-PCP-TEST-LINUX-TGT	Stage 1 & 2	Idle		
WebApp_023	WebApp_023-TGT	Stage 1 & 2	Idle		

Auto-Provisioning

Auto-provisioning is a feature that allows RMM to self-provision target instances identical to the origin using API calls. RMM requires a user with sufficient privileges in the destination management node. Auto-provisioning also requires that TCP/443 port is open to the destination's API service.

Creating a user on PCA

This is the list of required permissions a user must have for basic autoprovision to work. Permissions required for additional autoprovision features are listed by feature below:

- read permission on the instance-images resource.
- manage permission on the instances resource.
- inspect permission on the VCNs resource.
- use permission on the subnet resource.
- inspect permission on the private-ips resource.
- read permission on the public-ips resource.
- use permission on the vNIC resource.
- inspect permission on the vNIC-attachments resource.
- inspect permission on the compartments resource.

To use reserved public IP addresses, these additional permissions are required:

- manage permission on the public-ips resource.
- use permission on the private-ips resource.

To attach additional volumes to instances, these additional permissions are required.

- manage permission on the volumes resource.
- manage permission on the volume-attachments resource.

If a simpler set of permissions is desired at the cost of being slightly more permissive, these permissions can be used in place of the above:

- manage permission on the instance-family, volume-family and virtual-network-family resources.
- inspect permission on the compartments resource.

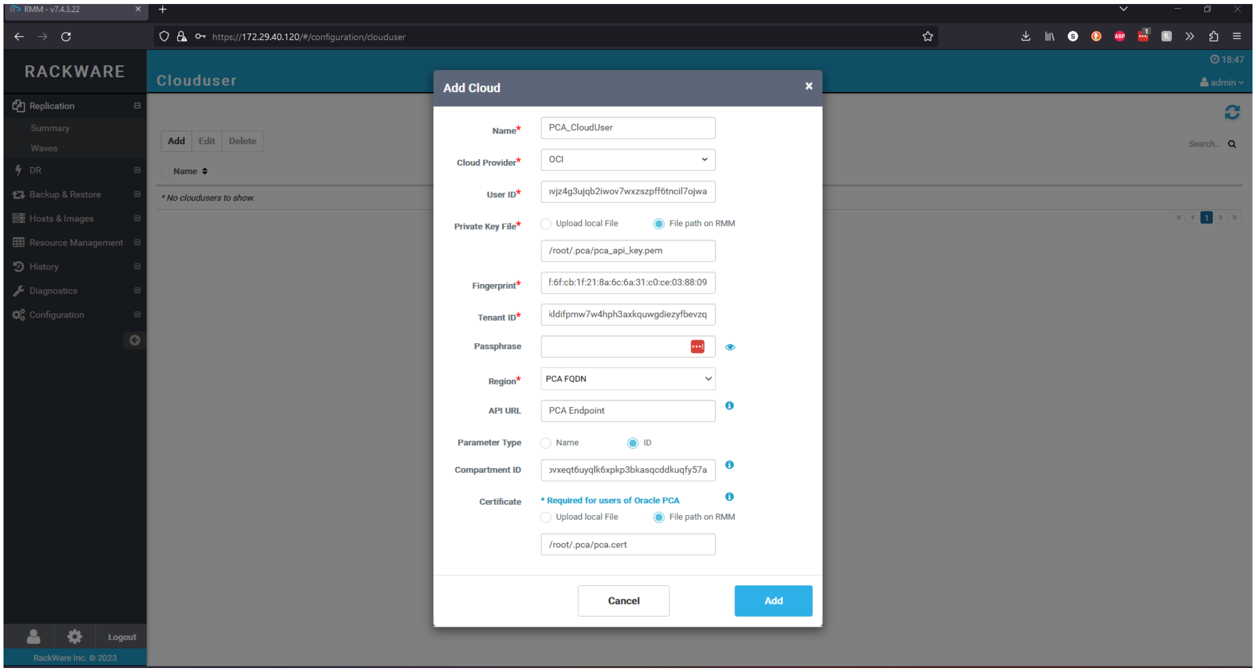
If simplicity in the policy is highest priority, a single permission can be used:

- manage permission on the all-resources resource.

Registering Clouduser on RMM

Since PCA uses OCI APIs, from the RackWare GUI, navigate to Configuration -> Clouduser and select OCI as the cloud provider.

Input all the required details and add cloud user.



* No cloudusers to show.

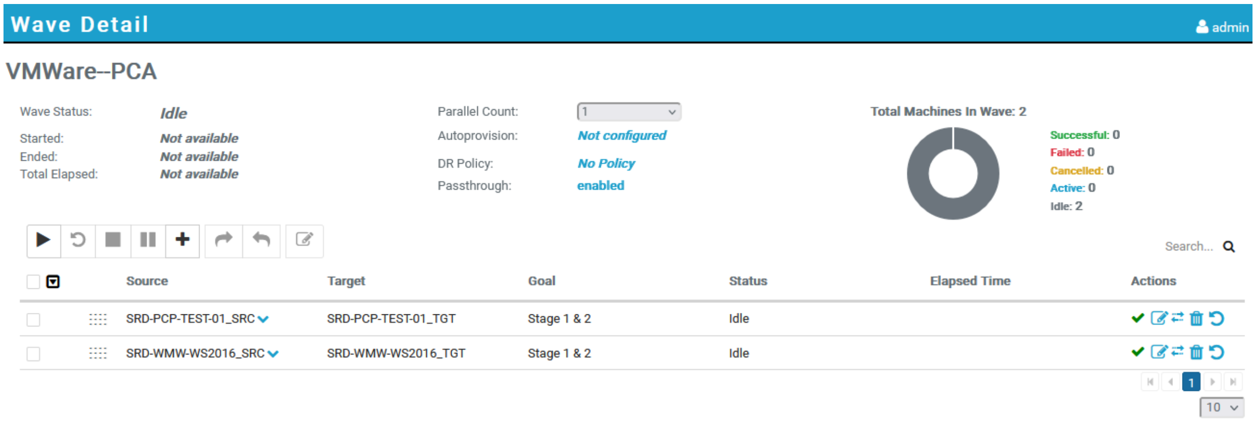
Add Cloud

Name*	PCA_CloudUser
Cloud Provider*	OCI
User ID*	›vjz4g3ujqb2iwov7wxzszpff6tncil7ojwa
Private Key File*	○ Upload local File ● File path on RMM
	/root/.pca/pca_api_key.pem
Fingerprint*	f:6f:cb:1f:21:8a:6c:6a:31:c0:ce:03:88:09
Tenant ID*	kldifpmw7w4hph3axkquwgdiezyfbevzq
Passphrase	
Region*	PCA FQDN
API URL	PCA Endpoint
Parameter Type	○ Name ● ID
Compartment ID	›vxeqt6uyqlk6xpkp3bkasqcddkuqfy57a
Certificate	* Required for users of Oracle PCA ○ Upload local File ● File path on RMM
	/root/.pca/pca.cert

Once Clouduser is successfully added, it can be used to configure the wave with auto-provisioning. This allows users with a large set of granular options to finetune the migration. Users can configure network settings, compute shapes, compartments, etc.

Applying Cloud Configuration to Waves

Cloud configurations can be applied to waves by clicking on *'Not Configured'* hyperlink for autoprovisioning.



VMWare--PCA

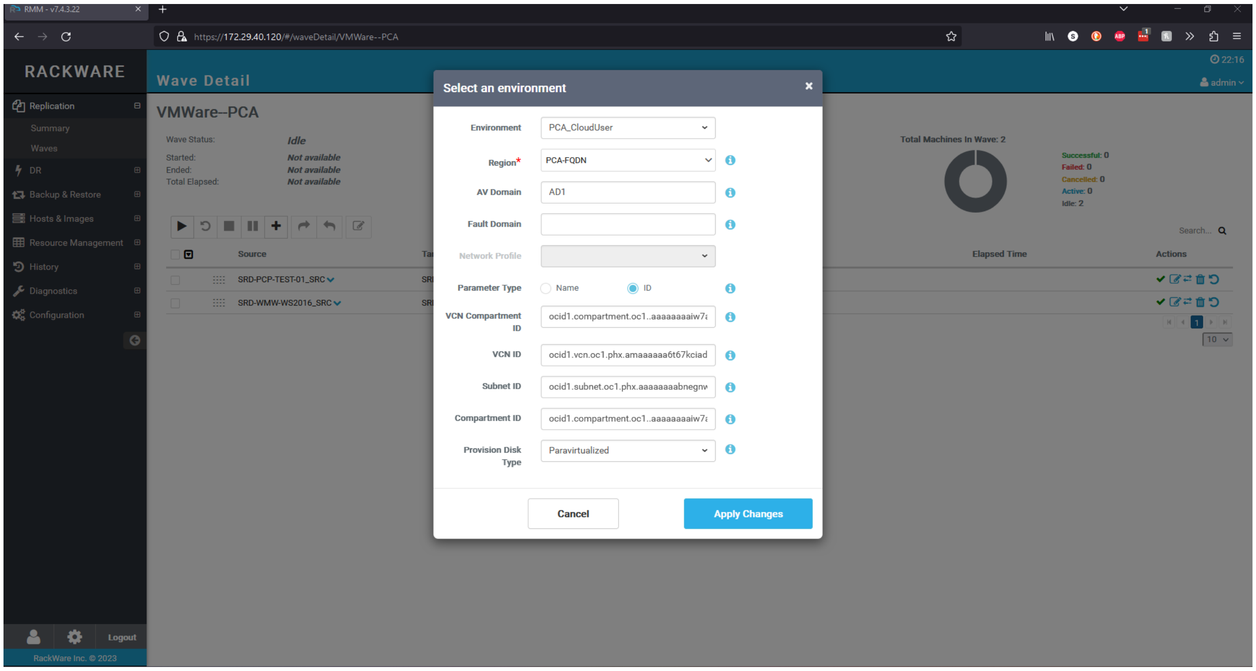
Wave Status:	*Idle*	Parallel Count:	1
Started:	*Not available*	Autoprovision:	*Not configured*
Ended:	*Not available*	DR Policy:	*No Policy*
Total Elapsed:	*Not available*	Passthrough:	enabled

Total Machines In Wave: 2

Successful: 0
Failed: 0
Cancelled: 0
Active: 0
Idle: 2

Source	Target	Goal	Status	Elapsed Time	Actions
SRD-PCP-TEST-01_SRC	SRD-PCP-TEST-01_TGT	Stage 1 & 2	Idle		
SRD-WMW-WS2016_SRC	SRD-WMW-WS2016_TGT	Stage 1 & 2	Idle		

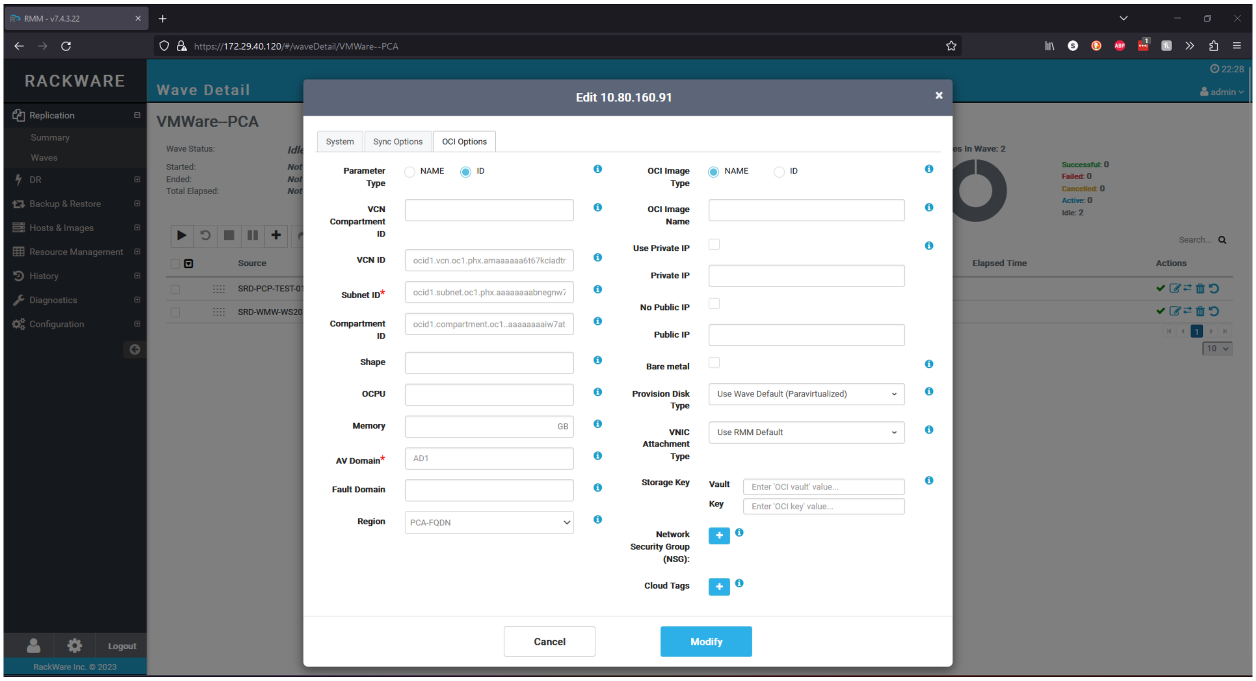
On selecting the PCA_CloudUser, fill in the values for the environment variables as shown below.



Select an environment

Environment	PCA_CloudUser
Region*	PCA-FQDN
AV Domain	AD1
Fault Domain	
Network Profile	
Parameter Type	○ Name ● ID
VCN Compartment ID	ocid1.compartment.oc1..aaaaaaaaiw7a
VCN ID	ocid1.vcn.oc1.phx.amaaaaaa6t67kciad
Subnet ID	ocid1.subnet.oc1.phx.aaaaaaaabnegnw
Compartment ID	ocid1.compartment.oc1..aaaaaaaaiw7a
Provision Disk Type	Paravirtualized

Once autoprovisioning is configured on the wave, users are allowed additional VM deployment options for individual wave items.



Edit 10.80.160.91

Parameter Type	○ NAME ● ID	OCI Image Type	● NAME ○ ID
VCN Compartment ID		OCI Image Name	
VCN ID	ocid1.vcn.oc1.phx.amaaaaaa6t67kciadtr	Use Private IP	□
Subnet ID*	ocid1.subnet.oc1.phx.aaaaaaaabnegnw7	Private IP	
Compartment ID	ocid1.compartment.oc1..aaaaaaaaiw7at	No Public IP	□
Shape		Public IP	
OCPU		Bare metal	□
Memory	GB	Provision Disk Type	Use Wave Default (Paravirtualized)
AV Domain*	AD1	VNIC Attachment Type	Use RMM Default
Fault Domain		Storage Key	Vault: Enter 'OCI vault' value... Key: Enter 'OCI key' value...
Region	PCA-FQDN	Network Security Group (NSG):	+
		Cloud Tags	+

Additional features offered by RackWare RMM

Right Sizing with Auto Provisioning: User can decide on reducing / increasing the compute and storage specification for target instances. Allowing users the granularity of re-sizing the filesystems.

Dynamic Provisioning during DR: Users can leverage RackWare's ability to locally maintain a replica image of the source instance and use this image to deploy a failover instance in a DR event.

Backup, Single File Restore and Protected Snapshots: RackWare's Backup offering comes with rich feature-sets like snapshot retention up to 3 years, selective file restores and unlimited protected snapshots for point-in-time recovery.

BIOS to UEFI: Users can seamlessly migrate to UEFI enabled instances without any additional configuration changes to the original instance.

Throttled-Migrations: Users have a greater control over every single migration by being able to throttle the bandwidth individually.

Completely Automated Failover and Fallback: Failover is completely automated as is falling back to the Origin environment.

RMM provides many more features like selective filesystem syncs, file and folder exclusions, enabling cloud-init, and custom post-scripts.

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com   facebook.com/oracle   twitter.com/oracle