

Oracle PCA Native DR: Overview and Configuration

Overview and Step-by-Step Guide to Configuring the Native Disaster Recovery on Oracle Private Cloud Appliances

Version [\[1.0\]](#)

June 23, 2025

Copyright © 2025, Oracle and/or its affiliates

Public

Purpose statement

This document provides a high-level overview and example of Native DR configuration steps on Oracle Private Cloud Appliance systems in different physical locations.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of contents

Introduction	4
Cabling and Required IP Addresses	5
Concepts of Native DR	8
Native DR Configuration Steps – Examples	9
1. Create Local Endpoint	9
2. Create Peer Connection	9
3. Create DR Service	10
4. Create DR Configuration	10
5. Add DR Configuration Site Mapping	10
6. Add Compute Instances to DR Configuration	10
7. Create DR Recovery Plans	10

Introduction

This content is provided for informational purposes and self-supported guidance only. Consultancy or other assistance related to the content is not covered under the Oracle Support contract or associated service requests. If you have questions or additional needs, then please do reach out to your Oracle Sales contact directly.

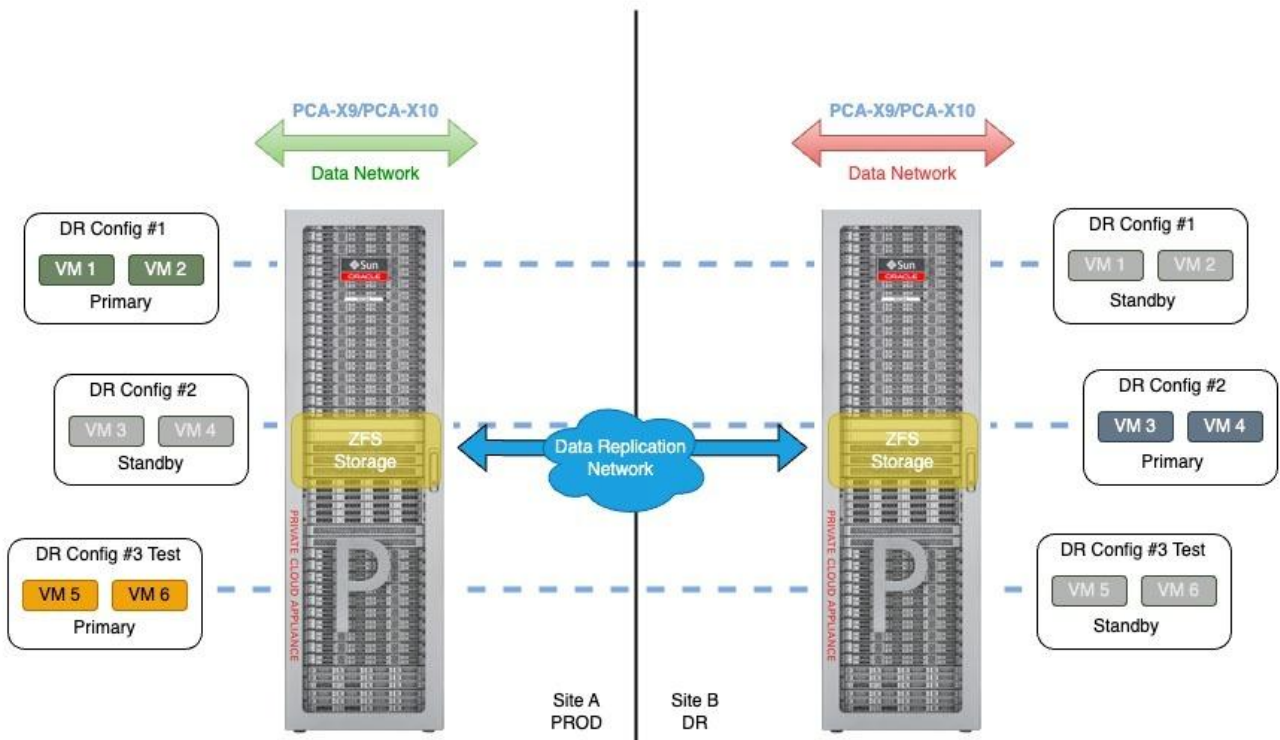
An updated version of Disaster Recovery (DR) Service of Private Cloud Appliance (PCA) was introduced in 3.0.2 M3.10 (3.0.2-b1261765 or later). The new version is referred as Native DR, and it no longer requires the Enterprise Manager to control the DR operations. Also, new network cabling is used in the new version.

Native DR allows the appliance administrator to create a protection group of one or more instances that can be replicated and moved to another PCA rack in the case of an emergency or test. Below is a high-level architecture diagram of Native DR. The VMs in each primary DR configuration are replicated to the matching standby DR configuration in the remote PCA. The replication between the two racks can be bi-directional and thus each rack can serve as a primary and standby at the same time.

Note that the DR service does not support the mixed PCA types (X9/X10). An X10 PCA must be paired with a remote X10 PCA for the Native DR. Likewise, an X9 PCA must be paired with a remote X9 PCA.

Detail information and instructions for Native DR configuration are referred to <https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/3.0-latest/admin/adm-native-dr.html#adm-natdr-plans>. The administrator guide also includes the instruction for migrating from the first-generation DR (Site Guard DR) to the Native DR and cabling requirements.

Private Cloud Appliance X9/X10 Native Disaster Recovery (DR) - Reference Setup



DR Control Plan connectivity via PCA Spine Switches

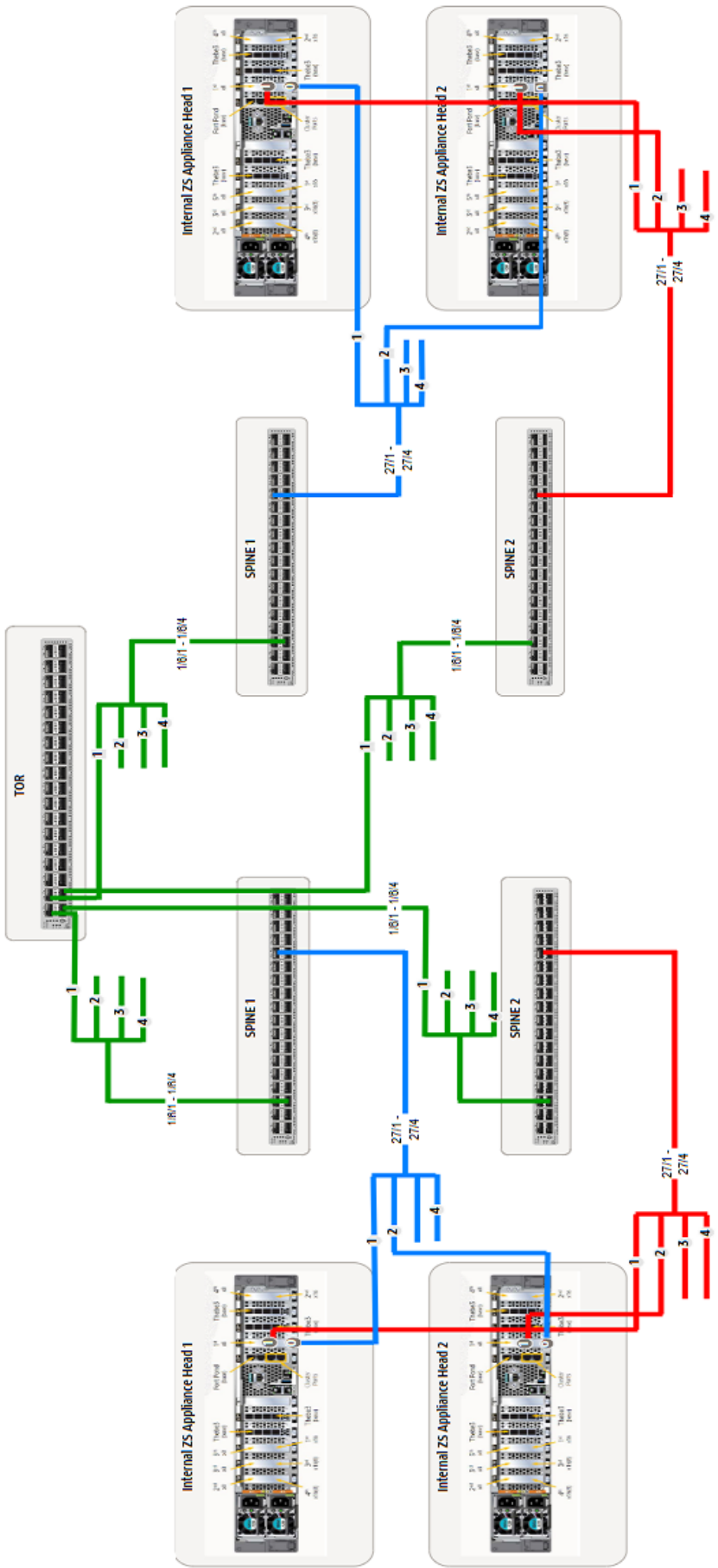
- Physical Port 6 connects to Replication Network. Only 10G/25G option available
- VRF/VLAN based isolation
- Requires 8 additional IPs for the Replication Network

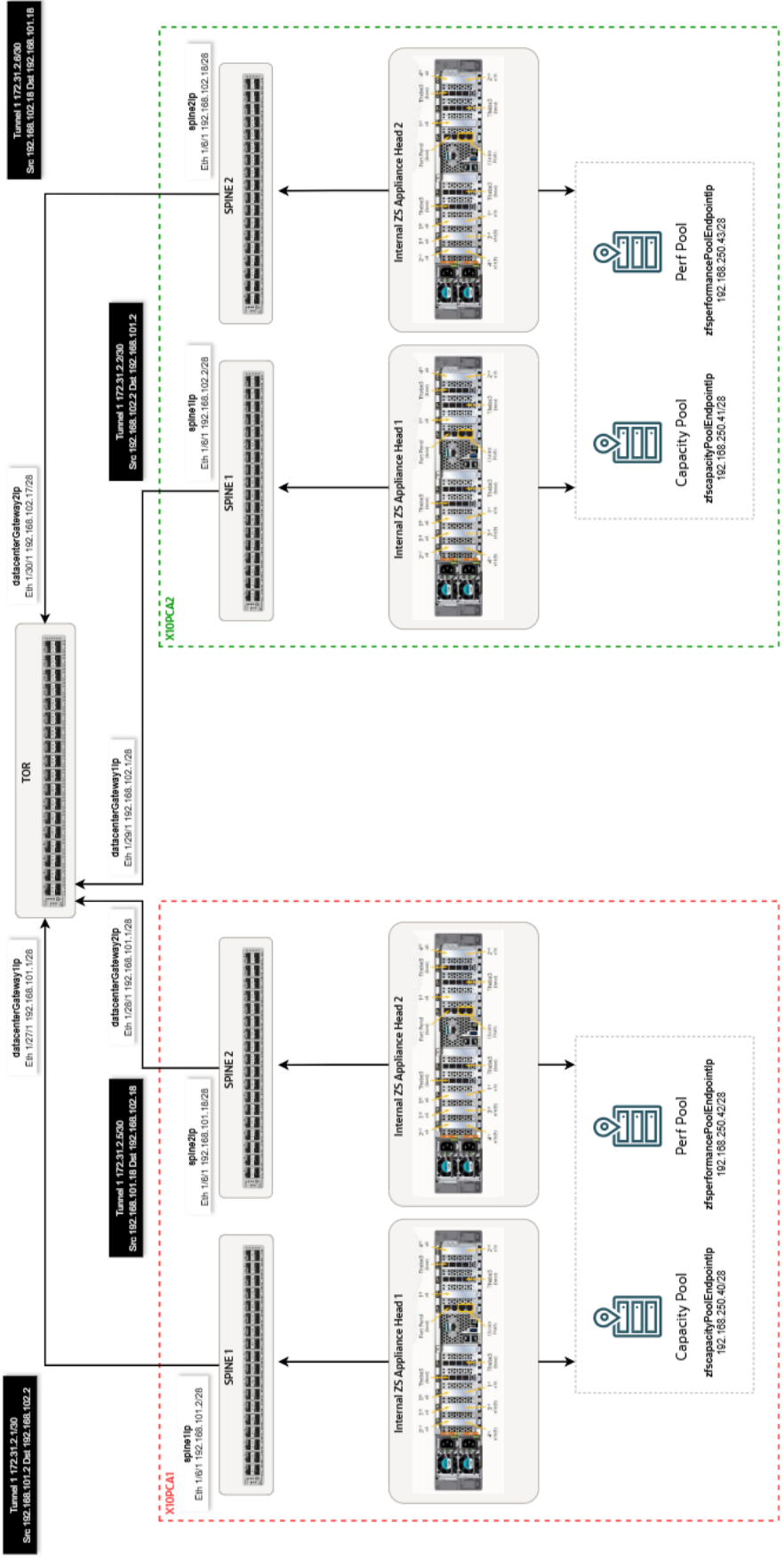
Cabling and Required IP Addresses

New network cabling of PCA is used by Native DR. New cabling is configured at the factory if the PCA was ordered after the PCA 3.0.2 M3.10 release. Though the legacy DR cabling can still be used for Native DR, it is recommended to move to the new configuration unless existing DR configurations are already in use. Native DR requires to multiple IP addresses, and the external IP addresses used for DR need to be routable between the two racks.

The diagrams in the next two page shows an example of network cabling and IP addresses. Note that the subnet masks are to be /29 for the PCA 3.0.2 M3.10. TOR in the diagrams is not necessarily one switch, and it may map to multiple switches and external network. Also, the IP addresses are presented only as examples. The exact IP addresses are not required.

Direct peering between racks requires dedicated cabling for each participating system. Dedicated cabling must be installed between the spine switches and the data center network. The additional connections between the spine switches and the data center network are the physical basis on which the network tunnels of the peer connection are configured. For each rack, four IP addresses are required for the local and remote endpoint for each tunnel. For peering, port 6 on each spine switch must be connected to the data center network.





Concepts of Native DR

These objects need to be created in the order below,

1. Local endpoint

Local endpoint is a listener that can be used by peering to connect the two racks together, but not external to the rack.

2. Peering

When peering is configured, a tunnel is created between the two racks to allow the two local endpoints to connect to each other. Peering allows the DR service to work between the racks. Other future services may also use this peering connection.

3. Disaster recovery service

The two peered racks can enable the disaster recovery service, which exchanges metadata between the racks on a 5-minute schedule.

4. Disaster recovery configuration

One or more instances are placed into a DR configuration, then, the data and metadata are replicated to the peer rack.

After the DR configuration objects are created successfully, three types of DR plans need to be created.

1. Switchover Plan

Switchover is useful for testing or planned outages. When a switchover is performed, there is no outage, so both peered systems are online. The DR configuration may move from the primary rack to the standby rack. When this is done, instances are stopped and removed from the source rack and started on the peer rack. The operation takes a few minutes to complete and requires some downtime.

Note that this operation is not useful for situations when the source system cannot be contacted.

2. Failover Plan

When necessary, maybe due to an unplanned outage like a disaster situation, the DR configuration in the primary rack can be failed over to the standby rack in the remote site. This operation is to be used only when the source rack is unavailable, and the source rack cannot contact the target rack. After the failover is completed, the instances are started on the target rack.

Note that the instances are not stopped on the source rack as it is assumed the source side cannot be contacted. Once the unplanned outage (i.e., disaster) is over and the source side is back online, extra steps are required for the DR configurations to return to a normal state, where the instances are running only on one side.

3. Post failover

A postfailover plan is performed after a failover, when the system that experienced an outage comes back online, and the peer connection is restored. The goal is to clean up the DR configuration on the primary system that went down and set it up as the standby for the new primary system.

Native DR Configuration Steps – Examples

This section provides the examples of Native DR configuration steps via PCA-ADMIN CLI. The same steps can be done using the PCA Service Web UI, where the DR configuration menus are available under the “Disaster Recovery Service”.

1. Create Local Endpoint

Traffic between peered Private Cloud Appliance systems flows through tunnels between endpoints. A rack must have a local endpoint configured before it can participate in a peer connection.

At the source PCA,

```
PCA-ADMIN> create LocalEndpoint spine1Ip=<10.212.128.3/29>
datacenterGateway1Ip=<10.212.128.1> spine2Ip=<10.212.128.4/29>
datacenterGateway2Ip=<10.212.128.2> zfsCapacityPoolEndpointIp=<10.212.128.129/29> \
zfsPerformancePoolEndpointIp=<10.212.128.130/29> localAsn=<136025>
```

At the target PCA,

```
PCA-ADMIN> create LocalEndpoint spine1Ip=<10.212.129.3/29>
datacenterGateway1Ip=<10.212.129.1> spine2Ip=<10.212.129.4/29>
datacenterGateway2Ip=<10.212.129.2> zfsCapacityPoolEndpointIp=<10.212.128.131/29>
zfsPerformancePoolEndpointIp=<10.212.128.132/29> localAsn=<136026>
```

After creating the LocalEndpoint, run `getLocalEndpoint` command to verify the local endpoint configuration.

2. Create Peer Connection

In the examples below, `peerAdminCaChain` is a string like “-----BEGIN CERTIFICATE----- ...”. To obtain the CA chain string, run the curl command first,

```
curl -k https://<iaas.mypca2.mydomain.com>/cachain -o x10pca1.pem
```

Then, convert the output of the curl command to a single line with this command,

```
awk 'NF {sub(/\r/, ""); printf "%s\\n", $0;}' mypca2.pem
```

At the source PCA,

```
PCA-ADMIN> create PeerConnection name=<peerconnection1> description=<"my peer
connection 1"> peerSerialNumber=<1654BF2465> peerSystemName=<mypca2>
peerDomainName=<mydomain.com> localEndpoint1Ip=<172.16.21.1/30>
remoteEndpoint1Ip=<172.16.21.2> localEndpoint2Ip=<172.16.21.5/30>
remoteEndpoint2Ip=<172.16.21.6> remoteSpine1Ip=<10.212.129.3>
remoteSpine2Ip=<10.212.129.4> peerAdminHostname=<mypca2.mydomain.com>
peerAdminUserName=<admin> peerAdminPassword=<password> peerAdminCaChain=<ca_string>
remoteAsn=<136026>
```

At the target PCA,

```
PCA-ADMIN> create PeerConnection name=<peerconnection2> description=<"my peer
connection 2"> peerSerialNumber=<1654BF2464> peerSystemName=<mypca1>
peerDomainName=<mydomain.com> localEndpoint1Ip=<172.16.21.2/30>
remoteEndpoint1Ip=<172.16.21.1> localEndpoint2Ip=<172.16.21.6/30>
remoteEndpoint2Ip=<172.16.21.5> remoteSpine1Ip=<10.212.128.3>
remoteSpine2Ip=<10.212.128.4> peerAdminHostname=<mypca1.mydomain.com>
```

```
peerAdminUserName=<admin> peerAdminPassword=<password> peerAdminCaChain=<ca_string>
remoteAsn=<136025>
```

3. Create DR Service

At the source PCA,

```
PCA-ADMIN> drNativeSetupService peerSerialNumber=<1654BF2465>
```

At the target PCA,

```
PCA-ADMIN> drNativeSetupService peerSerialNumber=<1654BF2464>
```

4. Create DR Configuration

At the source PCA,

```
PCA-ADMIN> create DrConfig configName=NativeDrTest2 zfsProjectName=NativeDrTest2
```

5. Add DR Configuration Site Mapping

At the source PCA,

```
PCA-ADMIN> drAddSiteMapping drConfigId=ec9addf6-da14-4e76-906c-bafd5f406ebf
objType=compartment sourceId=ocid1.compartment.AK03057621.ca-
x10pca1.9h3ic8to41ei3oenvqkb2e0yd08k48z05wf3awwowb0hcor2z66tjhiwyu6l
targetId=ocid1.compartment.AK03099400.ca-
x10pca2.7rvtr80rhgc5mdq0xwxszl0mz8zxyu2h21lwbwudlaf5810tj0es1991znt7
```

```
PCA-ADMIN> drAddSiteMapping drConfigId=ec9addf6-da14-4e76-906c-bafd5f406ebf
objType=subnet sourceId=ocid1.subnet.AK03057621.ca-
x10pca1.onh221bbznueobm3wbj6hce2jigelugiqdm1gwo0nlzxma6rk9uhd4seoqf9
targetId=ocid1.subnet.AK03099400.ca-
x10pca2.j7jka77duo5j5c9pymvso8y4481ctl72n8t6o7q7nltqhi9iz339sfgwktl8
```

6. Add Compute Instances to DR Configuration

At the source PCA,

```
PCA-ADMIN> drAddComputeInstance drConfigId=<drConfig ID>
instanceId="ocid1.instance1....uniqueID","ocid1.instance2....uniqueID"
```

When performing this step, the instances must be quiesced. The instances may be shut down before this step and restart after this step is completed.

7. Create DR Recovery Plans

At the source PCA,

```
PCA-ADMIN> create DrPlan drConfigId=ec9addf6-da14-4e76-906c-bafd5f406ebf
operation=SWITCHOVER planName=pca1-switchover
```

```
PCA-ADMIN> create DrPlan drConfigId=ec9addf6-da14-4e76-906c-bafd5f406ebf
operation=FAILOVER planName=pca1-failover
```

```
PCA-ADMIN> create DrPlan drConfigId=ec9addf6-da14-4e76-906c-bafd5f406ebf
operation=POSTFAILOVER planName=pca1-postfailover
```

Connect with us

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com). Outside North America, find your local office at: [oracle.com/contact](https://www.oracle.com/contact).

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2025, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Author: Tae Y. Chang, David Graham

11 Oracle PCA Native DR: Overview and Configuration / Version [1.0]

Copyright © 2025, Oracle and/or its affiliates / Public