PROTECTING SCALEIO USING RECOVERPOINT FOR VIRTUAL MACHINES

ABSTRACT

This white paper provides technical information and best practices that should be considered when planning or designing deployment of EMC RecoverPoint for Virtual Machines with EMC ScaleIO for VMware environment. This guide provide technical deep dive in to the architecture of the RecoverPoint for Virtual Machines, installation best practices and various deployment options.

March 2016
# TABLE OF CONTENTS

## INTRODUCTION ................................................. 5  
Audience ............................................................................. 5

## TERMINOLOGY ...................................................... 5

## OVERVIEW ......................................................... 6  
ScaleIO Architecture for VMware ........................................... 6  
RecoverPoint for Virtual Machines Architecture ................................. 7  
RecoverPoint for Virtual Machines multi-site support ........................... 8  
RecoverPoint for Virtual Machines I/O Path .................................... 9  
Replication Topologies ................................................................ 9

## SCALEIO WORKFLOW WITH RECOVERPOINT ....................... 13  
RecoverPoint for Virtual Machines workflow in a multi-site environment ........ 14  
ScaleIO workflow with RecoverPoint for Virtual Machines .................. 14  
ScaleIO architecture with RecoverPoint for Virtual Machines .............. 15

## RECOVERPOINT FOR VMS ORCHESTRATION AND AUTOMATION ...... 16

## DESIGN RECOMMENDATIONS ..................................... 17  
Recommendations for network design .......................................... 17  
Recommendations for creating vRPAs ........................................ 17  
Recommendations for consistency groups ...................................... 18

## CONFIGURATION AND INSTALLATION ................................ 18  
Prerequisites ........................................................................... 18  
RecoverPoint for Virtual Machines deployment ................................ 19  
Setting up the environment ....................................................... 19  
Installing RecoverPoint for Virtual Machines .................................. 21

## REPLICATION PROCESS ........................................... 23  
Replicating virtual machines to the remote site ................................ 23  
Failover operation ..................................................................... 27  
File consistency after failover process ........................................ 32

## CONCLUSION ....................................................... 33  
Revision history ....................................................................... 34
REFERENCES .................................................................................................................. 34
ACKNOWLEDGEMENT .......................................................................................... 34

LIST OF FIGURES

Figure 1) ScaleIO architecture for VMware ............................................................................. 7
Figure 2) RecoverPoint for virtual machines multi-site support .................................................... 8
Figure 3) RecoverPoint for Virtual Machines write I/O ............................................................... 9
Figure 4) Local protection of a virtual machine within the same vRPA/ESXi cluster .......... 11
Figure 5) Local protection of a virtual machine within the same vRPA/ESXi cluster but between two local ESXi clusters .................................................................................. 12
Figure 6) Remote protection of virtual machine between two vRPA/ESXi clusters ........ 12
Figure 7) Local and remote protection of virtual machines between two vRPA and ESXi clusters ............................................................................................................................... 13
Figure 8) Remote protection of a virtual machine among three vRPA/ESXi clusters .......... 13
Figure 9) RecoverPoint for Virtual Machines workflow in a multi-site environment .... 14
Figure 10) ScaleIO with RecoverPoint for Virtual Machines I/O path ....................................... 16
INTRODUCTION

EMC® ScaleIO® is an industry leading Software-defined Storage solution that enables customers to extend their existing virtual infrastructure into a high performing virtual SAN. All the VMware® ESX® hosts, with Direct Attached Storage (DAS) can be pooled together in a single storage system such that all the servers participate in servicing the I/O requests using massive parallel processing. ScaleIO can scale from as little as three ESX hosts to 1024 ESX hosts in one system. Increasing and decreasing, both the capacity and the IOPs can be done “on the fly” by adding or removing ESX hosts with minimal impact on the user or the application.

EMC RecoverPoint® is an advanced enterprise-class disaster recovery solution supporting heterogeneous storage and server environments. RecoverPoint provides bi-directional local and remote data replication across any distance and utilizes continuous data protection techniques to provide consistent point-in-time recovery.

RecoverPoint helps customers accelerate protection and provides operational and disaster recovery for the ScaleIO deployment within VMware, without affecting production environments.

AUDIENCE

This white paper is intended for EMC customers, partners and employees who want to better understand the ScaleIO replication using RecoverPoint for Virtual Machines.

It is assumed that the reader has familiarity with:

• ScaleIO components and architecture
• VMware components and architecture
• RecoverPoint for Virtual Machines components and architecture

TERMINOLOGY

RecoverPoint

• **RecoverPoint virtual appliance (vRPA):** A virtual data appliance that manages all aspects of data replication.

• **vRPA cluster:** A vRPA cluster is 2-8 vRPAs that work together to replicate and protect data.

• **RecoverPoint for Virtual Machines System:** One or more connected vRPA clusters.

• **Splitter:** A mechanism used to intercept writes so that they can be sent to the designated storage volume and vRPA simultaneously.

• **Consistency groups:** A logical entity used to configure protection policies across one or more volumes.

• **Group Set:** A group set is a collection of consistency group to which the system applies the parallel bookmark at a user-defined frequency. Group sets are useful for consistency groups that are dependent on one another or that must work together as a single unit.

• **Bookmark:** A bookmark is a manual snapshot with a label, which is applied to identify it. Parallel bookmarks are bookmarks with the same name applied at the same time to multiple consistency groups in a group set.

• **Journals:** Each copy of a consistency group must contain a resource pool consisting of one or more datastore that is responsible for maintaining point in time history of the data.

• **Recovery Point Objective (RPO):** RPO is the maximum period in which data might be lost in case of a disaster. For example, an RPO of 5 minutes means that in case of a disaster, the replication destination should not be behind no more than 5 minutes.
• **Recovery Time Objective (RTO):** RTO is the duration of time within which the business process should be restored after a disaster. For example, an RTO of 1 hour means that the data should be restored within an hour after the disaster.

• **Asynchronous Replication:** A replication mode, that enables you to replicate data across short or long distances while maintaining a dependent write consistent copy of data between the source copy and the replica copies at all times.

• **Synchronous Replication:** A replication mode in which the virtual machine host initiates a write to the production array and the data must be successfully stored by the local vRPA cluster and/or the remote vRPA cluster before an acknowledgement is sent back to the virtual machine host.

For more information on RecoverPoint for Virtual Machine components, please refer to the [RecoverPoint administrator guide](#).

## ScaleIO

• **ScaleIO Data Server (SDS):** The SDS owns local storage that contributes to the ScaleIO Storage Pools. An instance of the SDS runs on every server that contributes some or all of its local storage space (HDDs, SSDs, or PCIe flash cards) to the aggregated pool of storage within the ScaleIO virtual SAN. Local storage may be disks, disk partitions, even files. The role of the SDS is to actually perform the Back-End IO operations as requested by an SDC.

• **ScaleIO Data Client (SDC):** The SDC is a block lightweight device driver that exposes ScaleIO shared block volumes to applications. The SDC runs on the same server as the application. This enables the application to issue an IO request and the SDC fulfills it regardless of where the particular blocks physically reside. The SDC communicates with other nodes (beyond its own local server) over TCP/IP-based protocol, so it is fully routable.

For more information on ScaleIO components, please refer to the [ScaleIO administrator guide](#).

## OVERVIEW

This section provides the architecture overview of ScaleIO and RecoverPoint for Virtual Machines.

### ScaleIO Architecture for VMware

A ScaleIO system consists of three main components: ScaleIO Data Client (SDC), ScaleIO Data Server (SDS) and Metadata Manager (MDM).

**ScaleIO Data Client (SDC):** The SDC is a block lightweight device driver that exposes ScaleIO shared block volumes to applications. The SDC runs on the same server as the application. This enables the application to issue an IO request and the SDC fulfills it regardless of where the particular blocks physically reside. The SDC communicates with other nodes (beyond its own local server) over TCP/IP-based protocol, so it is fully routable.

For VMware, the SDC is installed directly on the ESX server.

**ScaleIO Data Server (SDS):** The SDS owns local storage that contributes to the ScaleIO Storage Pools. An instance of the SDS runs on every server that contributes some or all of its local storage space (HDDs, SSDs, or PCIe flash cards) to the aggregated pool of storage within the ScaleIO virtual SAN. Local storage may be disks, disk partitions, even files. The role of the SDS is to actually perform the Back-End IO operations as requested by an SDC.

For VMware implementations, the SDS is installed in a pre-configured virtual machine also known as ScaleIO Virtual Machine (SVM) which is provided with the ScaleIO software.

**Metadata Manager (MDM):** Metadata Manager manages the ScaleIO system. The MDM contains all the metadata which is required for the system operations. MDM manages the metadata such as device mappings, information regarding the volumes, snapshots, device allocations, capacity, errors and failures. It is also responsible for system rebuilds and rebalances. The MDM is very lightweight and has an asynchronous interaction with the SDC and SDS such that it doesn’t impact performance. It should be noted that the ScaleIO MDM doesn’t sit in the data path between the SDC and SDS. As of ScaleIO 1.33, each ScaleIO system has 3 MDMs i.e. a primary MDM, a secondary MDM and a tie-breaker. The MDM uses an Active/Passive methodology with a tie-breaker component where the primary MDM is always active and the secondary is passive.

Note: With ScaleIO 2.0, there is an option for 5 MDMs which is essentially 3 MDMs and 2 tie-breakers. Always check the [ScaleIO official website](#) for latest information.
For VMware implementations, the MDM is installed in the ScaleIO Virtual Machine (SVM). Figure 1 shows the ScaleIO implementation for VMware.

**Figure 1) ScaleIO architecture for VMware**

![ScaleIO Architecture Diagram](image)

As mentioned before, the SDS and MDM are installed in a ScaleIO Virtual Machine (SVM) and the SDC is installed directly on the ESXi™ host. The LUNs in the figure above can be formatted with the VMFS and then exposed using the ESXi hosts to the virtual machine or they can also be used as a RDM device. When the LUNs are used as a RDM device, the VMFS layer is omitted.

For further details on the ScaleIO architecture with VMware, refer to the white paper [EMC ScaleIO for VMware Environments](#).

**RecoverPoint for Virtual Machines Architecture**

RecoverPoint has established a strong presence and leadership position for block level storage array data protection, while the newest member of the product family, RecoverPoint for Virtual Machines, addresses the need to protect Virtual Machines (VMs) in a VMware virtualized environment. The RecoverPoint family consists of:

- RecoverPoint for Virtual Machines
- RecoverPoint, with its flexible virtual edition option

In this paper, we only focus on RecoverPoint for Virtual Machines.

A RecoverPoint for Virtual Machines system is dependent on the following software components:

- **RecoverPoint virtual appliance (vRPA):** A vRPA is a software component, which simulates the RecoverPoint Appliance. It runs as a separate virtual machine entity and is delivered in an OVA format. Each vRPA cluster can have 2-8 vRPAs.

- **ESXi Splitter:** The RecoverPoint write-splitter operates in each array where it monitors writes to protected volumes and ensures that RecoverPoint Appliance receives a copy of the write. The ESXi splitter is delivered in a vSphere Installation Bundle (VIB) format. The ESXi splitter utilizes Software iSCSI adapters to communicate with vRPAs. The RecoverPoint for Virtual Machines
splitter is proprietary EMC software, which is installed on every ESXi host in the cluster. Each splitter is exposed to all volumes in the cluster even though only one or two splitters will be accessing the same volume at a specific time. All the splitters in the cluster behave as an aggregate splitter; therefore, an ESXi cluster will be treated as a single entity.

• **RecoverPoint for Virtual Machines Plugin for vSphere Web Client:** RecoverPoint for Virtual Machine is fully integrated with VMware vSphere web client.

By embedding the splitter technology in the ESXi, RecoverPoint for Virtual Machines replicates VMs (with VMDK and/or RDM files) on any type of storage supported by VMware referenced in the VMware hardware compatibility list:


**Note:** RecoverPoint for Virtual Machines does not support ESXi hosts with non-persistent scratch location.

**Note:** RecoverPoint does not support shared VMDK or RDM virtual disks.

**RecoverPoint for Virtual Machines multi-site support**

RecoverPoint for Virtual Machines supports concurrent local and remote replication for production virtual machines. EMC RecoverPoint for Virtual Machine supports the following multi-site designs:

• **Fan-out replication:** With this design technique, RecoverPoint for Virtual Machines can replicate from a local site to up to two remote copies or to one local and one remote copy. Each copy contains data from the same consistency group.

• **Fan-in replication:** With this design technique, RecoverPoint for Virtual Machines can replicate from up to two remote sites to one central site. Each data contains data from different consistency group. With fan-in topology, one remote copy from per consistency group can be synchronous and the other can be asynchronous.

**Figure 2) RecoverPoint for virtual machines multi-site support**

RecoverPoint for Virtual Machines is designed with vAdmins in mind. vAdmins can protect the virtual machines at the hypervisor level with individual granularity and the tool offers better visibility and recoverability in the data protection process. RecoverPoint for Virtual Machines can have up to three vRPA clusters for virtual machine systems.

In this star topology, cluster 1 is connected to cluster 2 and cluster 3, but there is no connection between cluster 2 and cluster 3. RecoverPoint also supports fully connected systems, where all the three sites are connected to each other.
RecoverPoint for Virtual Machines I/O Path

Once RecoverPoint for Virtual Machines protects a VM, write I/O from the virtual machines goes through the virtual iSCSI layer and the I/O will be intercepted by the splitter acting as a vSCSI filter. The write I/O will be sent to the owner vRPA where the I/O is intercepted by the splitter. Once the write I/O is split, it is sent down the stack if the I/O to the vRPA succeeds.

When the write I/O cannot be sent to the vRPA, the splitter will invoke ‘marking mode’ where the I/Os are tracked while they continue to go through their respective VMDK or RDM destination.

Each vRPA exposes LUN0 via iSCSI protocol to each of the ESXi host in the cluster. iSCSI protocol is used to send the I/Os from the splitters to the vRPAs and as a transport pathway for DataComm IOCTL. DataComm perform reads via the splitter and the vSCSI filter can access the production devices without any locking issue. DataComm also facilitates access to the VMDKs or RDM on the remote side for distribution.

The following steps describe the handling of a write I/O with RecoverPoint for Virtual Machines:

1. Virtual machine sends a write to VMDK.
2. ESXi splitter intercepts the write and sends it to vRPA via the iSCSI Software Adapter.
3. vRPA acknowledges the write.
4. ESXi splitter sends the write to VMDK.
5. VMDK (via storage) acknowledges the write.
6. Splitter acknowledges the write to VM. vRPA distributes the write to the journal and replica VM.

Figure 3 shows the above steps in a diagram:

Figure 3) RecoverPoint for Virtual Machines write I/O

Replication Topologies

There can be up to three vRPA clusters in RecoverPoint for Virtual Machines system; one vRPA cluster is used for local replication and up to three vRPAs can be used for remote replication. Local and remote replication can be achieved using two vRPA clusters.
A minimum of two vRPAs required in a vRPA cluster. To scale-up or support higher throughput rate, the cluster can scale up to 8 vRPAs.

**Note:** All the vRPA clusters in a RPA system must have the same number of vRPAs.

The vRPAs in a vRPA cluster can reside on the same ESXi hosts as a protected virtual machines or on a different ESXi host or even on a different ESXi cluster.

**Best Practice:** It is recommended to separate out the ESXi locality of the vRPA virtual machines from the protected virtual machines.

Replication is at a virtual machine level so virtual machines with VMDK or RDM are replicated and not the datastore LUNs. When a virtual machine is selected for a replication, a replica virtual machine with the same configuration can be created automatically or a pre-selected virtual machines can also be selected manually with all of its constituent VMDK files. It is then subsequently added to the consistency group.

**Note:** Virtual machines containing RDM files need to be pre-created and selected as part of the protection process.

A replication environment is consisted of the following logical entities:

- **Consistency Groups:** A consistency group is created for an application whose data needs to be replicated to a consistent point in time. A consistency group is a container for virtual machines and all the copies of the application. The consistency groups is comprised of virtual machines, their copies, and their journals.

- **Copies:** A copy of the virtual machine and its application data is created which is accessible by the vRPA cluster. The following types of copies are created:
  - **Production copy:** Production copy is the source for the replication, which consists of all the virtual machines with their application data.
  - **Local copy:** A local copy is a copy of the production virtual machine and its replication data that is accessible by the vRPA cluster running in production. The local copy is used for continuous data protection. A virtual machine is identified by the ".copy.recoverpoint" extension at the end of the virtual machine name.
  - **Remote copy:** A remote copy is copy of the production virtual machine and its data, which is accessible by the remote vRPA cluster. A remote copy is also identified by ".copy.recoverpoint" extension.

- **Shadow VM:** A shadow virtual machine is in a shutdown state, which represents the replica VM. Shadow virtual machines are identified by a period symbol in from of the virtual machines name and ".copy.recoverpoint" extension. No user actions are possible on the Shadow VM.

- **Journals:** Journals are used to keep the point in time information of the data that has been protected. There are 2 different journals:
  - **Production Journal:** Production journals store information about the replication process. After failing over, a production journal becomes a copy journal.
  - **Copy Journal:** A copy journal receives the successive writes written to production. Copy journals are used to apply or undo writes so that the copy image can go in any point in time.

- **Snapshot:** A snapshot consists of information between two copies of consistent written data.

- **Snapshot consolidation:** Snapshot consolidation is used to consolidate multiple snapshots into a single snapshot, which allow longer history to be retained.

- **Bookmark:** A bookmark is a manual snapshot which is created with a label to identify it later.

- **Group set:** A group set is a collection of consistency groups to which parallel bookmarks are applied. Group sets are useful for consistency groups that are dependent on one another or that must work together as a single unit.

**Topologies**
The following RecoverPoint for Virtual Machines topologies are supported for the deployment. With RecoverPoint for Virtual Machines 4.3, up to two concurrent replica copies are supported.

**Figure 4) Local protection of a virtual machines within the same vRPA cluster**
Figure 5) Local protection of a virtual machine within the same vRPA cluster but between two local ESXi clusters

Site A

VMware vCenter

EMC RecoverPoint for VMs Plug-in

VMware ESXi Kernel

VMware ESXi Cluster 1

Figure 6) Remote protection of a virtual machine between two vRPA clusters

Site A

VMware vCenter

EMC RecoverPoint for VMs Plug-in

VMware ESXi Kernel

VMware ESXi Cluster 1

Site B

VMware vCenter

EMC RecoverPoint for VMs Plug-in

VMware ESXi Kernel

VMware ESXi Cluster 2

WAN
**SCALEIO WORKFLOW WITH RECOVERPOINT**

This section describes the IO path for ScaleIO in conjunction with RecoverPoint for Virtual Machines. It is required that the reader is familiar with the ScaleIO architecture. Please refer to EMC [ScaleIO Deployment and Performance Best Practices for VMware](#) guide for more details.
Before describing ScaleIO workflow with RecoverPoint for Virtual Machines, it is important to understand the RecoverPoint for Virtual Machines workflow in a multi-site environment.

**RecoverPoint for Virtual Machines workflow in a multi-site environment**
The steps below explain the IO workflow for a virtual machine protected as a part of an asynchronous remote replication scenario.

1. The host virtual machines initiate a write IO.
2. The ESXi splitter intercepts the write and sends it to the vRPA via the software iSCSI adapter.
3. Once the vRPA acknowledges the write, ESXi splitter sends the write to the VMDKs.
4. The vRPA in the source vRPA cluster sends the write as a part of the snapshot to its partner vRPA in the target vRPA cluster. The snapshot is sent over the WAN link.
5. The target vRPA sends the write to the owner ESXi host.
6. The write is distributed by the ESXi hosts to the consistency group, copy journal and replica VM.

**Figure 9) RecoverPoint for Virtual Machines workflow in a multi-site environment**

![Diagram of RecoverPoint for Virtual Machines workflow](image)

**ScaleIO workflow with RecoverPoint for Virtual Machines**

This section describes the ScaleIO architecture and IO workflow with RecoverPoint for Virtual Machines in a VMware environment.

One of the prerequisite of the RecoverPoint for virtual machines is that the datastores for the virtual repository must be mapped to every ESXi capable of running vRPAs. Therefore prior to installation of RecoverPoint for VM, it is required to install ScaleIO on the VMware environment to replicate the virtual machines running on datastores which are created using ScaleIO storage.

- Install ScaleIO on all ESXi hosts that will participate in ScaleIO storage. Please follow [ScaleIO Installation Guide](#) and [ScaleIO Deployment and Performance Best Practices for VMware](#) guide, for details on ScaleIO installation.
- Create a ScaleIO volume and map the volume to every ESXi that is capable of running vRPAs.
• Create datastores on the ESXi hosts from the mapped ScaleIO volume.
• Deploy a virtual machine on the datastore created from the mapped ScaleIO volume.
• Install RecoverPoint for Virtual Machines. Refer to the RecoverPoint for Virtual Machines configuration and installation section.

**ScaleIO architecture with RecoverPoint for Virtual Machines**

The steps below explain the ScaleIO IO workflow for virtual machines that is deployed on a datastore created from a ScaleIO storage.

• Guest virtual machines that is deployed on a datastore created from a ScaleIO volume, initiates an IO.
• The ESXi splitter intercepts the write and sends it to the vRPA via the software iSCSI adapter.
• Once the vRPA acknowledges the write, ESXi splitter sends the write to the VMDKs.
• IO will go the ScaleIO Data Client (SDC).
• SDC talks to the hypervisor. Hypervisor uses VMkernel port to communicate with the ScaleIO Virtual Machine (SVM). SVM have ScaleIO Data Server (SDS) installed in them.
• SDS looks up the destination on ScaleIO volume and initiates a write to the datastore.
RECOVERPOINT FOR VMS ORCHESTRATION AND AUTOMATION

RecoverPoint for Virtual Machines simplifies operational recovery and disaster recovery with built-in orchestration and automation capabilities accessible via the VMware vSphere Web Client.

RecoverPoint for Virtual Machines has the following orchestration features to complement its recovery capabilities:

- **Start-up priority/sequence**: With this feature, virtual machines can now be pre-configured to facilitate prioritization when performing recovery activities. It supports application inter-dependency by sequencing the start-up of virtual machines within a consistency group and/or with multiple consistency groups within a group set. With this feature, a virtual machine can be set to be critical, and when it fails to power-up, the start-up sequence will be paused by the system, and no other virtual machines will be power-up.

- **User scripts and User Prompts**: These options allows configuration of the User Scripts and User Prompts before powering on and after powering on. The prompter message feature provides the option of administrator configurable messages during the recovery flow.

  **Note**: VMware tools should be installed in the operating system of a virtual machine to facilitate the use of user scripts.

- **Re-IPing**: This feature for replica virtual machines facilitates network configuration automation to avoid IP duplication and can be applied through scripts and network information in CSV format.
RecoverPoint for Virtual Machines has the following automation features:

- **VMDK manageability:** This feature provides the vAdmin the ability to select the type of VMDK to use for the copy VM. The available options are:
  - Same as source
  - Thick
  - Thin

  This feature is useful to exclude certain VMDKs from replication. It is also useful to add or expand a VMDK without losing the journal or sweeping the consistency group.

- **Application consistent bookmark:** This feature is available for Microsoft Windows 2008 and Microsoft Windows 2012R2 by using RecoverPoint for Virtual Machines KVSS utility.

- **Replication of virtual machine hardware changes:** This feature enables the vAdmin to keep Replica virtual machines in-line with Production virtual machines’ hardware settings. VMDKs added to a protected virtual machine can automatically be provisioned on all copies of virtual machines. Replication of hardware changes occurs periodically.

  **Note:** Please follow the RecoverPoint administrator guide for further details about orchestration and automation features.

**DESIGN RECOMMENDATIONS**

This section provides the best practices and recommendations to design and deploy RecoverPoint for Virtual Machines in a ScaleIO environment. There are various configuration settings to optimize the replication, among which the most important ones are discussed in this section.

**Recommendations for network design**

- In low-traffic deployments, all four-network cards can be placed on the same virtual network (on a single vSwitch).

- For high availability and performance, separate LAN and WAN traffic from iSCSI traffic. For even better performance, place each network i.e. LAN, WAN, iSCSI1 and iSCSI2 on a separate virtual switch.

- Scenarios, where clients need to have redundant physical switches, the best practice is to route each iSCSI card to a different physical switch. This involves creating one VMkernel port on every vSwitch and dvSwitch (vNetwork Distributed Switch) dedicated for iSCSI.

- The performance of RecoverPoint for Virtual Machines is dependent on the bandwidth that you expose to the vRPA iSCSI vSwitches. It is recommended to configure vSphere hosts with quad port NICs and present them to the vRPAs as single or dual iSCSI networks. You can also implement VLAN tagging to logically divide the network traffic among multiple vNICs.

- Configure the iSCSI network with an MTU of 9000.

- For synchronous replication, the round trip time (RTT) should not exceed 200ms and packet loss should be less than 1 percent.

**Recommendations for creating vRPAs**

- When using 4CPU/4GB or 8CPU/8GB configurations to run a vRPA, the best practice is to reserve all RAM for RecoverPoint for Virtual Machines.

- To allow redundancy in case an ESXi server fails, it is recommended that the vRPAs should not share the same ESXi server.

- In the case when the vRPAs are deployed on the same host, make sure sufficient resources are made available:
  - CPU and memory: Total resources available on a shared host must be the sum of resources required by each of the individual vRPAs on the server.
  - Network bandwidth must be sufficient to handle I/Os of all vRPAs.
• It is recommended to deploy all vRPAs in a single cluster with the same configuration file. If this is not possible, it is recommended to deploy the first and second vRPAs in the vRPA cluster to use a more powerful configuration profile as they are candidates to run cluster control. The cluster control vRPAs run additional processes and therefore require additional CPU and memory resources.

• In scenarios when vRPAs are deployed with different configuration profiles, it is recommended to deploy vRPAs in pairs of the same configuration profile to provide enough failover capacity and performance in case of a vRPA failure.

• The performance of the vRPAs does not scale linearly, hence it is recommended to use two smaller-sized vRPAs instead of a single large size vRPA.

• To avoid single points of failure, it is recommended to deploy the first two vRPAs on different ESX hosts. Placing the first two vRPAs on the same ESX host will create a single point of failure.

  Note: vRPAs can be added to the vRPA cluster but they cannot be removed from the vRPA cluster.

Recommendations for consistency groups
A consistency group is a group of virtual machines and their disks that are replicated together in a way to ensure write-order consistency. Consistency groups are used to ensure write-order consistency on a single virtual machine and also across multiple virtual machines that reside in different consistency groups.

• Newly created consistency groups are load balanced across the vRPAs in the cluster. It is recommended that after the consistency group has been replicated for at least a week, the I/O load on all the vRPAs is researched and consistency groups are manually rebalanced across the vRPAs in the cluster.

• RecoverPoint for Virtual Machines does not support distributed consistency groups (unlike a traditional RecoverPoint appliance). Since the consistency groups are not distributed, they run on a single vRPA and are limited by the resources of the vRPA.

• Fewer consistency groups are better for performance.

• If the load of two or more virtual machines is greater than what a single vRPA can replicate, it is recommended that two consistency groups must replicate the virtual machines. In this way, both the consistency groups run on a separate vRPA.

• If write-order consistency is required between two consistency groups, they can be placed together in a group set on which parallel bookmarking has been enabled. It should be noted that there is a 20 seconds time gap between the frequencies for parallel bookmarking. Therefore, consistency groups that use parallel bookmarking do not support recovery to any point in time.

  Note: For more details, please follow the RecoverPoint for Virtual Machines Scale and Performance Guide.

CONFIGURATION AND INSTALLATION
This section describes the configuration and installation activities required for RecoverPoint for Virtual Machines deployment. Please refer to the RecoverPoint for Virtual Machines Installation and Deployment Guide to obtain the latest information.

Prerequisites
Before starting with the deployment, please make sure your environment meets the following requirements:

• All the ESXi hosts in the cluster must have SSH enabled. SSH is required for the installation or removal of the RecoverPoint for Virtual Machines splitter. It may be disabled at all the other times.

• VMware vCenter™ and ESXi Servers release 5.1 U1, 5.5, 6.0 and later updates are required for the installation.

• The RecoverPoint for Virtual Machines splitter requires at least 800 MB of RAM per ESXi node.

• The scratch location specified during installation process must point to persistent storage.

• Ensure that the network infrastructure is configured in VMware vSphere® to meet the vRPA requirements. Four virtual networks (LAN, WAN, 2 iSCSI); 1 software iSCSI adapter per ESXi node with 2 VMkernel ports are required. For higher performance, it is recommended to place each network on a separate virtual switch.
Depending on the size of your infrastructure, the following virtual appliance configuration options are available:

- 2 vCPUs / 4 GHz, 4 GB RAM, 44 GB storage
- 4 vCPUs / 9 GHz, 4 GB RAM, 44 GB storage
- 8 vCPUs / 17 GHz, 8 GB RAM, 44 GB storage

The vRPA OVA package can be deployed only from the vCenter management console, not via vSphere management console. This is a VMware limitation for vAPP functionality, which is used by the OVA script.

**RECOVERPOINT FOR VIRTUAL MACHINES DEPLOYMENT**

This section includes the following topics:

- Setting up the environment
  - Installing RecoverPoint for Virtual Machines splitter
  - Configuring network
  - Creating vRPAs
- Installing RecoverPoint for Virtual Machines
  - Creating a vRPA cluster
  - Connecting vRPA clusters
  - Registering vCenter Servers

**Setting up the environment**

To setup the RecoverPoint for Virtual Machines environment, install the RecoverPoint for Virtual Machines splitters on all ESXi hosts which are part of RecoverPoint for Virtual Machines cluster, configure iSCSI software adapter on those ESXi hosts which needs to be protected and deploy vRPAs using the OVA file which is extracted from the RecoverPoint for Virtual Machines download.

**Installation of splitter on an ESXi server**

There are two methods of installing the splitter on an ESXi server: using the RecoverPoint for Virtual Machines VIB installer or using the splitter with 'boxmgmt'.

- **Installation using RecoverPoint for Virtual Machines VIB installer**
  - SSH the RecoverPoint VIB file to the ESXi host using secure copy protocol.
  - To install the RecoverPoint VIB file, run the following command on the ESXi host:
    
    ```bash
    esxcli software vib install -v /<full_path>/<vib_name> --no-sig-check
    ```
  - To test the VIB installation, run the following command:
    
    ```bash
    esxcli software vib list
    ```

- **Installation of splitter using boxmgmt**
  - To install new splitter using boxmgmt, SSH to a vRPA and login as a boxmgmt user (username: `boxmgmt`, password: `boxmgmt`). Once you log in, vRPA will provide a list of menu options.
    - From the **Main Menu**, select **Installation > Upgrade > Splitter Upgrade**
    - Provide the vCenter Server credentials.
    - Approve the certificate. There will be a prompt message to deploy the splitter on all ESX cluster in the vCenter. There are 2 options for the prompt:
      1. Respond Y to deploy splitter on all ESXi cluster in the vCenter.
2. Respond **N** to deploy splitter on each ESXi cluster individually. To install splitter individually, you need the ESXi Cluster Managed Object Reference (MOref) ID. To find MOref ID:

- On a web browser, enter your ESXi or vCenter fully qualified domain name or the IP address followed up with '/mob'. For example:
  
  https://<ESXi/vCenter details>/mob

- Login using vCenter credentials.

- Under the Return Type of Service content, click **RetrieveServiceContent > invoke method**

- Select the value displayed in the **rootFolder** row.

- In the **childEntity** row, select the datacenter where the ESXi cluster is located.

- Select the ESXi cluster listed in the **hostFolder** row. The value listed in the **childEntity** row is the ESXi MOref ID. For example, **domain-s17 (10.108.161.47)**

Please follow the [VMware knowledge transfer link](#) for more details on finding the ESXi MOref ID.

### Configuring network

To allow the ESXi server to communicate with the vRPAs, create a Software iSCSI Adapter and two VMkernel ports per ESXi node on each ESXi server that will be a part of the vRPA.

**Note**: The VMkernel ports must be able to communicate with the vRPA iSCSI ports.

**Best Practice**: Configure both iSCSI (vRPA and VMkernel) networks on the same subnet.

- Set up two VMkernel ports. Assign IP addresses that are on a routable subnet or on the same subnet as the vRPA iSCSI interfaces that will be assigned when deploying the vRPA cluster.

- Login to the vSphere Web Client, in **Inventory**, select **Hosts and Clusters**. Select an ESXi server (host), click the **Manage tab > Storage > Storage Adapters** and create a software iSCSI adapter. Add the VMkernel ports to the network configuration under the **iSCSI Software Adapter**.

- Click **Add** and confirm that you want to add the iSCSI software adapter.

- Verify that the Port Group Policy for every VMkernel you created is compliant and at least one of them is active.

**Troubleshooting iSCSI software adapter**: If your hosts throw up the 'Call "IscsiManager.QueryBoundVnics" for object "iscsiManager-57" on vCenter Server "VMWARE-VCENTER.SierraFrontTech.local" failed', fix it by doing the following:

1. Disable the iSCSI software adapter. Copy the iqn and settings. Do not reboot yet.

2. Winscp to the host using SFTP -> navigate to /etc/vmware/vmkiscsid/ and copy the contents to your workstation.

3. Once copied, delete the contents in /etc/vmware/vmkiscsid/

4. Reboot the host.

5. Create a new software iSCSI adapter -> write over the IQN with the old one you copied earlier.

6. Add iSCSI port bindings and targets.

### Creating vRPAs

vRPAs must be created with an OVA package file. It can only be deployed from the VMware vCenter management console and not from the vSphere management console.

- At the vCenter management console, from the **File menu**, select **Deploy OVF Template**.
• In the source screen, specify the vRPA OVA package location.

• In the OVF template details screen, review the general properties of this OVA template. To accept, click Next.

• In the EMC End-User License Agreement screen, if you accept the terms of the EMC End-User License Agreement, click Accept and Next.

• In the Name and Location screen, enter the name you wish to assign to this vRPA. If you enter the name of an existing vRPA, you will not be permitted to continue.

• In the Deployment Configuration screen, select the desired configuration profile.

• In the Storage screen, select the vRPA storage (datastore) that will be used to host the vRPA virtual machine files. The best practice is to select a high-performance datastore. In the Disk Format screen, select Thin Provision or Thick Provision disk format.

• In the Network mapping screen, map the four required vRPA Ethernet ports. Do not select the internal VMware iSCSI network.

• In the IP address allocation screen, select the IP allocation policy for the vRPA temporary IP, which will later be used to connect to the Deployment Manager. Select IP Allocations - Static.

• Enter the required IP properties.

• Summarize all your selection and click Finish.

It is required to create a vRPA cluster. There should be two or more vRPAs in a cluster. To deploy more vRPAs, follow the steps described above.

**Installing RecoverPoint for Virtual Machines**

To install the RecoverPoint for Virtual Machines, use the RecoverPoint for Virtual Machines installer in the Deployment Manager to create a cluster and to connect them if you are using more than one cluster.

**Prerequisites**

• RecoverPoint Deployment Manager (DM) 2.2 or later.

• The datastore for the virtual repository must be mapped to every ESXi capable of running vRPAs. An additional minimum of 6 GB of storage is required for the repository.

• The vRPA has ongoing validation algorithms. A failure of any validation causes the vRPA to disconnect from the vRPA cluster (meaning that this vRPA will not function as an active RPA). Validation verifies that the vRPA has enough system resources.

• Sharing vRPA iSCSI interfaces (iSCSI1 and iSCSI2) with the vRPA regular networks (LAN and WAN) may result in performance degradation and unexpected behavior of the vRPA.

• Java™ version 7 or newer, 32-bit, installed on the computer running Deployment Manager is required.

**Creating the cluster**

To create a vRPA cluster, follow the following steps:

• Launch the Deployment Manager and select Install RecoverPoint for Virtual Machines. Click Login.

• In the RecoverPoint Deployment Manager Wizard screen, select the RecoverPoint Installer Wizard.

• In the Prerequisites screen, read the prerequisites. Once you have ensured that the conditions are met, select the I have fulfilled the conditions for installing the RPA cluster checkbox.
• In the Configuration file screen, select whether to create a new installation configuration file or to continue installation from a saved file. Type the appropriate file location.

• In the Environment settings screen, define the Cluster name. Define the environment settings.

• In the RPA discovery screen, define how you want to set the IP addresses of the vRPAs.

• In the IP and connectivity settings screen, define the vRPA cluster IP configurations and vRPA IP settings.

• In the Login credentials screen, enter the default login credentials. (password: boxmgmt)

• In the Connectivity results screen, review the results of the connectivity test.

• In the Cluster iSCSI settings screen, define the vRPA cluster iSCSI settings. If you want to use CHAP, configure the credentials for the iSCSI ports.

• In the RPA iSCSI ports screen, define the vRPA cluster iSCSI IP configuration.

• Select appropriate option from the Update RecoverPoint release team.

• In the Apply configuration results screen, the results of applying the configuration settings to all vRPAs are displayed.

• In the vCenter Server registration screen, enter the vCenter server credentials, RecoverPoint administrator credentials (login: admin, password: admin), and the location of the vCenter certificate. The vCenter certificate can be found on the vCenter server at the following location:
If using vCSA, the vCenter certificate can be found at the following location:
/etc/vmware-vpx/ssl/rui.crt

- In the Datastores screen, select a datastore from the Available datastores table to be the vRPA repository.
- In the Storage configuration - cluster summary screen, review the vRPA information.

**Connecting vRPA clusters**

To connect two vRPA clusters, perform the following steps:

- Launch the Deployment Manager and select **Install RecoverPoint for Virtual Machines**. Then click Login.
- Select the **Connect Cluster Wizard** to pair a new cluster to an existing RecoverPoint system.
- In the Select connection step screen, select **Prepare new cluster for connection**.
- In the Preparation prerequisites please ensure that the conditions are met and then select the **I have fulfilled the conditions for preparing the new cluster checkbox**.
- In the **New cluster login credentials** screen, enter the first vRPA cluster management IP address and the RecoverPoint login credentials to this cluster.
- In the **Connect now or later** screen, select **Connect the new cluster to an existing RecoverPoint system**.
- In the **Existing cluster login credentials** screen, enter the management IP of the second vRPA cluster (already prepared) and the RecoverPoint login credentials to this cluster.
- If necessary, please add additional gateways in the Cluster connection settings screen.
- The connecting vRPA clusters should complete successfully.

**Registering vCenter Servers**

You can add up to four vCenter Servers to each vRPA cluster. To register additional vCenter Servers in your RecoverPoint for Virtual Machines system, do the following:

- Check whether each additional vCenter Server is already registered by creating an SSH connection to one of the vRPAs and entering your RecoverPoint username and password to log in to the CLI, and running the **get_storage** command.
- If the vCenter is not registered, run the **register_storage** command.
- Log out of vSphere and log back in. The RecoverPoint for Virtual Machines plug-in should be installed in the additional vCenter web client. If not, wait for 10 minutes and log back in or restart the vSphere web client.

**REPLICATION PROCESS**

This section describes the basic protection process for protecting virtual machines using RecoverPoint for Virtual Machines.

**Replicating virtual machines to the remote site**

- Right click on the virtual machines and select **Protect** in order to bring up the Protect virtual machines wizard.
• **Select** to add the virtual machines to a new Consistency group or to an existing one.

Enter the name of the Consistency group and select the production RecoverPoint for Virtual Machines cluster. Click **Next**.

Enter the name of the production copy and configure the capacity of the production journal. Select the replication datastore automatically or manually.
• Name the target copy and select the location of the target copy. Click **Next**.

• Configure the target Journal. Configure the Replication policy from a template or manually. Select mode of replication. Synchronous or Asynchronous. Click **Next**.

• Select to automatically create the target virtual machines or use an existing one. Pick the target virtual machines location. Select the datastore to house the target VM. Click **Next**.
• Review the settings and click **Finish** to complete the Replication of the VM.
Navigate to RecoverPoint for Virtual Machines tab to check the status of the virtual machines replication. For more details on the operations of the RecoverPoint, please refer to RecoverPoint for Virtual Machines administrator guide.

Failover operation

Navigate to RecoverPoint for Virtual Machines plugin and select Protection. Click on the Consistency Groups.
• Click on **Apply Bookmark** tab. Provide meaningful Bookmark name. Select consistency type (Crash-Consistent/Application-Consistent)
Click on **Edit Start-Up** sequence. Enter Start-up priority.
• Click on **Fail Over**. Select Consistency Group. If you have created Group Set, select Group set. Click **Next**. Select an image from the drop down menu. In this test scenario, the image name is “failover_testing”. Select the image.

![Image of Fail Over wizard](image.png)

• Define testing network and click next. Verify image to access. Click **Next**.

• In the last step, wait until Storage shows “Logged Access”. Click **Finish**.
• Click on **Finish** to complete the Failover process. Login to the remote site vCenter to check the copy of the Source VM. As shown in the figure below, remote vCenter shows the Source virtual machine is up and running. The virtual machine has an extension ".copy".
File consistency after failover process

- In this use case, we are testing the consistency of the files among the virtual machines which have been failed over from one vRPA cluster to another.

- The figure below shows the source virtual machine with a file named “file1”

- The source virtual machine is failed over to a remote vRPA cluster. The failed over virtual machine has an extension of “.copy”. Figure below shows the failed over virtual machine with a file named “file1” with the same content as of the source virtual machine.
CONCLUSION

This document provides information on how to protect ScaleIO environment using RecoverPoint for Virtual Machines. RecoverPoint for Virtual Machines is a flavor of the EMC RecoverPoint family, which is targeted at enterprises, mid-range customers and service providers. It is designed for VMadmins who supports VMware implementations and deployments.

RecoverPoint for Virtual Machines version 4.3 supports both synchronous and asynchronous replication of the virtual machines. It also offers multi-copy capabilities with enhanced automation and orchestration tools.

This guide provides all the information that is required to deploy RecoverPoint for Virtual Machines with ScaleIO for a VMware environment. The best practices and recommendations provided in this white paper, have been proved through the internal testing and the recommendations provided by the RecoverPoint for Virtual Machines engineering. After reading this paper, you should be able to deploy and configure RecoverPoint for Virtual Machines with ScaleIO for VMware environment.

Although this guide attempts to generalize many best practices as recommended by RecoverPoint for Virtual Machines, different conditions with different considerations may apply in different environments. For a specific use case, please consult with your representative from EMC.
REFERENCES
ScaleIO User Guide
ScaleIO Installation Guide
EMC ScaleIO for VMware Environment: Deployment and Performance Best Practices
RecoverPoint for virtual machines Administrator Guide
RecoverPoint for virtual machines Installation Guide
RecoverPoint for virtual machines Sizing Guide
ScaleIO - Network Best Practices Guide
EMC RecoverPoint for Virtual Machines Version 4.3

ACKNOWLEDGEMENT
Idan Kentor, EMC RecoverPoint