Copyright © 2013-2019 Dell Inc. All rights reserved.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision history</td>
<td>5</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Understanding the architecture</td>
<td>8</td>
</tr>
<tr>
<td>System overview</td>
<td>8</td>
</tr>
<tr>
<td>System architecture and components</td>
<td>9</td>
</tr>
<tr>
<td>Integrated Data Protection and Vscale Architecture</td>
<td>10</td>
</tr>
<tr>
<td>Planning for backup and recovery</td>
<td>10</td>
</tr>
<tr>
<td>Advantages of Integrated Data Protection converged backup systems</td>
<td>10</td>
</tr>
<tr>
<td>Converged backup systems connectivity overview</td>
<td>12</td>
</tr>
<tr>
<td>Dedicated deployment in a converged backup system with network switches</td>
<td>12</td>
</tr>
<tr>
<td>Converged backup system connectivity to a single Converged System</td>
<td>12</td>
</tr>
<tr>
<td>Converged backup system connectivity to multiple Converged Systems</td>
<td>15</td>
</tr>
<tr>
<td>Dedicated deployment in a converged backup system without network switches</td>
<td>17</td>
</tr>
<tr>
<td>Shared deployment</td>
<td>19</td>
</tr>
<tr>
<td>Backup and recovery</td>
<td>20</td>
</tr>
<tr>
<td>Converged backup systems components</td>
<td>20</td>
</tr>
<tr>
<td>Avamar</td>
<td>21</td>
</tr>
<tr>
<td>NetWorker</td>
<td>23</td>
</tr>
<tr>
<td>Data Domain</td>
<td>24</td>
</tr>
<tr>
<td>Data Domain Standalone</td>
<td>24</td>
</tr>
<tr>
<td>Data Domain Boost for Enterprise Applications</td>
<td>25</td>
</tr>
<tr>
<td>Data Domain and third-party application native backup utilities</td>
<td>25</td>
</tr>
<tr>
<td>Data Domain and third-party backup applications</td>
<td>25</td>
</tr>
<tr>
<td>Data Domain High Availability</td>
<td>26</td>
</tr>
<tr>
<td>Data Domain High Availability features</td>
<td>26</td>
</tr>
<tr>
<td>Data Domain High Availability architecture</td>
<td>26</td>
</tr>
<tr>
<td>Data Domain Virtual Edition in the Public Cloud</td>
<td>27</td>
</tr>
<tr>
<td>Dell EMC Cloud Disaster Recovery</td>
<td>28</td>
</tr>
<tr>
<td>Dell EMC Cloud Disaster Recovery architecture</td>
<td>29</td>
</tr>
<tr>
<td>Converged backup system sizing</td>
<td>31</td>
</tr>
<tr>
<td>Recovery types</td>
<td>31</td>
</tr>
<tr>
<td>Replication of backup data to a second site</td>
<td>32</td>
</tr>
<tr>
<td>Cloud tier support</td>
<td>33</td>
</tr>
<tr>
<td>Cloud tiering with Avamar or NetWorker and Data Domain</td>
<td>33</td>
</tr>
<tr>
<td>IP-based data backup</td>
<td>33</td>
</tr>
<tr>
<td>NDMP backup</td>
<td>33</td>
</tr>
<tr>
<td>Enterprise deployment</td>
<td>34</td>
</tr>
<tr>
<td>Using Oracle RMAN with converged backup systems</td>
<td>35</td>
</tr>
<tr>
<td>ProtectPoint for VMAX3 and VMAX All Flash arrays with Data Domain</td>
<td>36</td>
</tr>
<tr>
<td>Using Enterprise Hybrid Cloud with converged backup systems</td>
<td>40</td>
</tr>
<tr>
<td>Avamar configurations for Enterprise Hybrid Cloud</td>
<td>40</td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td>42</td>
</tr>
<tr>
<td>VPLEX</td>
<td>42</td>
</tr>
</tbody>
</table>
## Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2019</td>
<td>4.0</td>
<td>Added support for Data Domain Virtual Edition and Dell EMC Cloud Disaster Recovery</td>
</tr>
<tr>
<td>March 2019</td>
<td>3.9</td>
<td>Added support for Data Domain High Availability</td>
</tr>
<tr>
<td>January 2019</td>
<td>3.8</td>
<td>Added support for VPLEX 6.1.1 and Dell EMC PowerMax storage</td>
</tr>
<tr>
<td>November 2018</td>
<td>3.7</td>
<td>Added support for Data Protection Suite 18.1</td>
</tr>
<tr>
<td>September 2018</td>
<td>3.6</td>
<td>Added support for IPv6 onVxBlock System 1000</td>
</tr>
<tr>
<td>August 2018</td>
<td>3.5</td>
<td>Added support for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Nexus 9336C-FX2 switch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dell EMC PowerMax 2000 and 8000 arrays</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AMP-3S</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated labels and connections in connectivity diagrams</td>
</tr>
<tr>
<td>May 2018</td>
<td>3.4</td>
<td>Added support for Data Domain 3300</td>
</tr>
<tr>
<td>March 2018</td>
<td>3.3</td>
<td>Added support for XtremIO X2</td>
</tr>
<tr>
<td>February 2018</td>
<td>3.2</td>
<td>Added support for VxBlock System 1000 and AMP-VX</td>
</tr>
<tr>
<td>January 2018</td>
<td>3.1</td>
<td>Added support for RecoverPoint for Virtual Machines 5.1.1.1</td>
</tr>
<tr>
<td>December 2017</td>
<td>3.0</td>
<td>Added support for VMware vSphere 6.5</td>
</tr>
<tr>
<td>November 2017</td>
<td>2.9</td>
<td>• Minor updates to support Avamar 7.5 and NetWorker 9.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Minor updates to ProtectPoint section</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Removed reference to VPLEX GeoSynchrony 6.0 SP1 P5 update.</td>
</tr>
<tr>
<td>August 2017</td>
<td>2.8</td>
<td>Added support for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Domain Standalone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VMAX 950F</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expanded VMware Site Recover Manager for RecoverPoint content</td>
</tr>
<tr>
<td>June 2017</td>
<td>2.7</td>
<td>Added support for Avamar 7.4.1.</td>
</tr>
<tr>
<td>May 2017</td>
<td>2.6</td>
<td>Added support for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NetWorker 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Nexus 93180YC-EX switch</td>
</tr>
<tr>
<td>March 2017</td>
<td>2.5</td>
<td>Added support for Vscale.</td>
</tr>
<tr>
<td>February 2017</td>
<td>2.4</td>
<td>Added support for:</td>
</tr>
</tbody>
</table>

VCE Integrated Data Protection Product Guide 5
<table>
<thead>
<tr>
<th>Date</th>
<th>Document revision</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2016</td>
<td>2.3</td>
<td>Added support for ProtectPoint for VMAX3 and VMAX All Flash arrays with Data Domain.</td>
</tr>
<tr>
<td>November 2016</td>
<td>2.2</td>
<td>• Added support for Avamar Virtual Edition.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Returned physical planning information previously moved to the <em>Converged Systems Physical Planning Guide</em>.</td>
</tr>
<tr>
<td>September 2016</td>
<td>2.1</td>
<td>• Added support for Avamar 7.3 software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for Avamar Gen 4T hardware</td>
</tr>
<tr>
<td>May 2016</td>
<td>2.0</td>
<td>• Added support for NetWorker 9.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Moved physical planning information to the <em>Converged Systems Physical Planning Guide</em>.</td>
</tr>
<tr>
<td>April 2016</td>
<td>1.9</td>
<td>Added support for converged backup systems in a switchless configuration.</td>
</tr>
<tr>
<td>February 2016</td>
<td>1.8</td>
<td>• Added support for RecoverPoint for Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for Data Domain DS60 storage shelf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Expanded VPLEX content</td>
</tr>
<tr>
<td>December 2015</td>
<td>1.7</td>
<td>• Added support for XtremIO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for Enterprise Hybrid Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for VxRack Systems</td>
</tr>
<tr>
<td>September 2015</td>
<td>1.6</td>
<td>• Added support for VxBlock Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for Data Domain DD2200 Controller and Data Domain DD9500 Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for MetroPoint</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added information on the Intelligent Physical Infrastructure appliance added to cabinets.</td>
</tr>
<tr>
<td>March 2015</td>
<td>1.5</td>
<td>Added Avamar 7.1 and Data Domain 5.5 support.</td>
</tr>
<tr>
<td>October 2014</td>
<td>1.4</td>
<td>• Added Oracle RMAN support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Vblock System 240 support</td>
</tr>
<tr>
<td>May 2014</td>
<td>1.3</td>
<td>Added a RecoverPoint section</td>
</tr>
<tr>
<td>December 2013</td>
<td>1.2</td>
<td>Added multi-node support and Data Domain 4500 physical specifications</td>
</tr>
<tr>
<td>November 2013</td>
<td>1.1</td>
<td>Added Data Domain DD4500</td>
</tr>
<tr>
<td>October 2013</td>
<td>1.0</td>
<td>Initial release</td>
</tr>
</tbody>
</table>
Introduction

This document describes the Integrated Data Protection options for Converged Systems.

The target audience for this document includes field personnel, partners, and customers responsible for planning or managing data protection for applications and data that reside on a Converged System. This document is designed for people familiar with Dell EMC Data Protection solutions.

Refer to the Glossary for terms, definitions, and acronyms.
Understanding the architecture

System overview
This section describes the various features of Integrated Data Protection.

Integrated Data Protection provides:

- **Daily backup**
- **Data replication**
- **Business continuity**
- **Workload mobility (flexibility)**
- **Extended retention of backups**

**Daily backup**
Once-daily backups provide minimal required data insurance by protecting against data corruption, accidental data deletion, storage component failure, and site disaster. The daily backup process creates fully recoverable, point-in-time copies of application data.

Successful daily backups ensure that, in a disaster, a business can recover with not more than 24 hours of lost data. The best practice is to replicate the backup data to a second site to protect against a total loss of data in the event of a full site disaster. Most daily backups are saved for 30 to 60 days.

**Data replication**
Most businesses have some data sets that are too valuable to risk losing up to 24 hours of data. Additionally, if disaster strikes, these more valuable data sets must be recovered quickly.

For data sets that are more valuable, data replication achieves a higher level of data insurance. Multiple snapshots of application data can be created throughout the day. Snapshots are used to restore data to a point in time, to retrieve an individual file, or to copy application data to a different server for testing, data mining, and so on.

Retrieving a copy of the data from an offsite location reduces the worst-case data loss from 24 hours to the time since the last snapshot. Data can be copied synchronously, where the data is updated locally and remotely simultaneously. It can also be copied asynchronously, where there may be a time lag in updating the data remotely.

Typically, data replication is done in addition to daily backup. Replication cannot always protect against data corruption, because a corrupted file replicates as a corrupted file. The best level of data protection is achieved by combining daily backup and continuous replication methodologies.

**Business continuity**
Business continuity provides application availability insurance by ensuring zero data loss and near-zero recovery time for business-critical data. Data and applications protected with a business continuity product should still use daily backup to provide multi-day point-in-time copies.

**Workload mobility**
Workload mobility provides data protection by moving the workload to another site in anticipation of a disaster. For example, if a tropical storm is heading for a data center and the decision is made to move critical applications to a data center out of the storm’s path, a good workload mobility design allows that movement to occur easily and with zero downtime.

In addition to data protection purposes, workload mobility is also used for moving applications and data to balance workloads across Converged Systems.
Extended retention of backups

Most businesses have a subset of data with a copy-retention period that spans multiple years. Those data copies are usually retained to meet a specific legal compliance. In the past, long-term retention periods were addressed by placing backup copies on tape and then storing the tapes in an offsite location. Certain Data Domain systems offer a disk-based extended retention feature that delivers a cost-effective alternative to tape.

If there is a business or legal requirement to occasionally export data backups to tape, both Avamar and NetWorker offer solutions. Avamar 7.3 and higher no longer support Avamar Extended Retention with an Avamar Media Access Node. Avamar offers Avamar Data Migration Enabler to export Avamar backups to tape as an alternative solution. For more information on this solution refer to the Avamar Data Migration Enabler User Guide in the reference materials section of this document.

NetWorker can perform backup or clones to tape within a native NetWorker deployment. For more information on this solution, refer to the NetWorker Administration Guide in the reference materials section of this document.

System architecture and components

Integrated Data Protection products are extensions of the Converged System, built by Dell EMC in Dell EMC cabinets.

Integrated Data Protection products are pre-architected, assembled, and supported by Dell EMC. While customers are free to use any data protection system they choose for their Converged System, Integrated Data Protection products provide systems that are faster to deploy, are optimized for Converged Systems, and come with a single-call support model.

The following table describes how Integrated Data Protection products provide backup and recovery, business continuity, and disaster recovery for the Converged System.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Product</th>
<th>Product description</th>
</tr>
</thead>
</table>
| Backup and recovery                            | Avamar (including Avamar Virtual Edition), NetWorker, and Data Domain | • Advanced deduplication backup.  
• Uses high-speed technology to reduce the backup data storage footprint at the target device by 10 to 30 times. Backup times are shortened while full backups are available for rapid, single-step restores. |
| Business continuity (disaster avoidance) and workload mobility providing availability (flexibility) | VPLEX                                | • Shares, protects, or load-balances infrastructure resources across multiple Converged Systems in the same data center or different data centers within a campus or urban area.  
• Moves live VMs between locations, avoiding migration downtime.  
• Handles unplanned events automatically with zero data-loss and zero to near-zero application recovery time. |
| Replication with continuous local and remote protection | RecoverPoint, RecoverPoint for Virtual Machines, and VMware Site Recovery Manager | • Data rollback to any point in time.  
• Quickly restores critical applications and data. |
### Integrated Data Protection and Vsacle Architecture

Integrated Data Protection can protect systems that are part of a Vsacle Architecture.

Vsacle Architecture is a framework that enables organizations to build data center scale IT systems comprised of resources that are logically connected using a Vsacle Fabric to form logical systems.

For more information on Vsacle Architecture, refer to the Dell EMC Vsacle Architecture Overview.

### Planning for backup and recovery

Data backup and recovery planning are critical elements of the comprehensive effort to deploy a Converged System. The use of traditional tape to back up and recover data in a Converged System is effective, but legacy methodology inhibits maximizing the potential of the Converged System.

The early planning stages of Converged System design is the time to consider new backup methodologies and current best practices that are specifically designed for a VMware environment. Implementing new backup and recovery processes at this time offers the following advantages:

- Provides a logical cut-over point. Applications moving into a Converged System can be moved off the old backup infrastructure at the same time.
- Allows for scaling up the amount of protected data, without increasing administration staff.
- Meets data protection service level agreements (SLAs) with plenty of room in the backup window for continued data growth.
- Eliminates tape throughput problems, tape management problems, and security issues associated with tapes.
- Leverages advanced VMware features such as change block tracking, which is a feature specifically designed for data protection.

In some cases, budget constraints, lease expirations on existing backup components, recent license renewals, or staffing constraints may make it impractical to simultaneously roll out a Converged System and a new backup infrastructure. In those situations, it is recommended that you continue to investigate new backup methodologies as part of the Converged System planning efforts. Education during the planning stage allows you to develop a strategy for how to migrate from an older backup system infrastructure.

### Advantages of Integrated Data Protection converged backup systems

This section describes the advantages of using an Integrated Data Protection solution on converged backup systems.

While not mandatory, using an Integrated Data Protection solution provides the following benefits:

- Cost savings
- Manpower savings
- Designed specifically for a Converged System

<table>
<thead>
<tr>
<th>Capability</th>
<th>Product</th>
<th>Product description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Helpful when migrating data from one virtualized Converged System to another.</td>
</tr>
</tbody>
</table>
• Scales painlessly
• Converged System integration accelerates time from delivery to full production use and reduces deployment risk factors
• Offloads the backup network resulting in reduced labor and a path to retiring the backup network
• Provides ability to back up more data in less time: Average nightly backups decrease from hours to minutes
Converged backup systems connectivity overview

A converged backup system is a pre-integrated backup system, built and supported by Dell EMC, and containing a combination of Avamar or NetWorker, Data Domain, and Cisco switches.

Dedicated deployment in a converged backup system with network switches

A dedicated deployment provides one converged backup system dedicated to a single Converged System.

The Converged System network extends into the Integrated Data Protection cabinet. Backup data travels directly between the Converged System and the converged backup system with no impact on the regular flow of data on the customer’s network.

Dell EMC does not support Avamar Virtual Edition with this configuration because it is not a practical option. Refer to Dedicated deployment in a converged backup system without network switches for supported Avamar Virtual Edition configurations.

For Converged Systems, replicate backup data from the Avamar or NetWorker and Data Domain components to a similar converged backup system located in a separate facility. Backup replication traffic traverses through the converged backup system switches to the Converged System switches and uses the Converged System uplinks to the customer network. Replication data crosses the customer network to the secondary location.

To replicate backup data from a site using Avamar and Data Domain, the destination site must also have Avamar and Data Domain. To replicate from a site using NetWorker and Data Domain, the destination site requires only Data Domain. If the main site is unavailable due to an outage, you must restore the NetWorker environment at the secondary site to recover data there.

Converged backup system connectivity to a single Converged System

VxBlock System with 10 GB connections

The following illustration shows the connections of a converged backup system connected to a single VxBlock System with 10 GB connections:
The uplinks from the dedicated data protection network switches are configured for 10 GB, leveraging the 40 GB to 10 GB breakout capability of the VxBlock System network switches.

The following illustration shows the connections of a converged backup system connected to a single VxBlock System 1000 with 10 GB connections:

**VxBlock System 1000 with 10 GB connections**

The uplinks from the dedicated data protection network switches are configured for 10 GB, leveraging the 40 GB to 10 GB breakout capability of the VxBlock System network switches.
VxRack System FLEX with 40GB connections

The following illustration shows the connections of a Converged backup system connected to a single VxRack System FLEX with 40GB connections:
The links between the switches are configured as virtual port Channel (vPC) interfaces, providing bandwidth aggregation and high availability.

**Converged backup system connectivity to multiple Converged Systems**

The following illustration shows the connections of a converged backup system connected to multiple VxBlock Systems with 10 GB connections:
The following illustration shows the connections of a converged backup system connected to multiple VxRack FLEX with 40 GB connections:
Dedicated deployment in a converged backup system without network switches

The dedicated deployment in a converged backup system without network switches is similar to the dedicated deployment with network switches, except there are no dedicated network switches for the converged backup system.

This configuration allows Avamar and Data Domain to connect directly to the Converged System management switches (for IPMI or iDRAC connections) and Converged System production switches (for management, backup, and replication connections). A NetWorker and Data Domain converged backup system requires physical connections to the Converged System production switches for the Data Domain system only.

The following table shows components used in a converged backup system in a switchless configuration for both Avamar and NetWorker systems:
<table>
<thead>
<tr>
<th>Converged backup system</th>
<th>Component</th>
</tr>
</thead>
</table>
| Avamar                  | • Avamar Virtual Edition/M1200/M2400 Single Node (metadata storage only)  
|                         | • Avamar NDMP Accelerator (optional)  
|                         | • A supported Data Domain system |
| NetWorker               | • NetWorker  
|                         | • A supported Data Domain system |
| Data Domain Standalone  | • ProtectPoint for VMAX  
|                         | • Data Domain Boost for Enterprise Applications  
|                         | • Third-party applications and backup applications unsupported by Dell EMC |
| ProtectPoint for VMAX   | • VMAX3 or VMAX All Flash Array  
|                         | • A supported Data Domain system |

The switchless configuration is available for all RCM-supported Converged Systems, provided that the number of available ports is sufficient. Refer to the following table:

<table>
<thead>
<tr>
<th>Converged backup system components</th>
<th>Number of ports for BRS Out-Of-Band Management (1 Gb) on management plane switch</th>
<th>Number of ports for In-Band management (1 Gb) on data plane switch</th>
<th>Number of ports for In-Band management (10 Gb) on data plane switch</th>
<th>Number of ports for backup (10 Gb) on data plane switch</th>
</tr>
</thead>
</table>
| Data Domain 2200/2500/3300/6300 Controller (with Avamar physical systems or standalone) | 0 DD2200/2500  
| | 1 DD3300/6300 | 1 | 0 | 2 |
| Data Domain 2200/2500/3300/6300 Controller (with Avamar Virtual Edition) | 0 DD2200/2500  
| | 1 DD3300/6300 | 0 | 0 | 2 |
| Data Domain 4200/4500/6800/7200/9300/9500 Controller | 0 DD4200/4500/7200  
| | 1 DD6800/9300/9500 | 1 | 0 | 4 |
| Data Domain 6800/9300 Controller in High Availability Configuration | 2 | 2 | 0 | 8 |
| Data Domain 9800 Controller | 1 | 1 | 0 | 8 |
| Data Domain 9800 Controller in High | 2 | 2 | 0 | 16 |
Shared deployment

A shared deployment provides a backup system that can protect more than the directly connected Converged Systems.

You can back up the following systems by connecting their Avamar or NetWorker clients to the converged backup system:

- Vblock System 100
- VxBlock and Vblock Systems 200 series
- Third-party systems

These clients use the connections from the converged backup system to the customer network to communicate with Avamar or NetWorker and send data to the backup repository. NetWorker can also perform image-level backups from virtual environments not on a Converged System by adding VMware Backup Appliances to those environments.
Backup and recovery

An Integrated Data Protection converged backup system solution uses one of the following arrangements of Dell EMC technology and components:

- Avamar
- Avamar with Data Domain
- NetWorker with Data Domain

Converged backup systems components

Dell EMC has a family of products for backup and recovery design for Converged Systems. The correct product to use depends on specific customer requirements.

Dell EMC combines the following components to provide data backup protection for Converged Systems:

<table>
<thead>
<tr>
<th>Product</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar</td>
<td>- Avamar M1200/M2400 Single Node (metadata storage only)</td>
</tr>
<tr>
<td></td>
<td>- Avamar M1200/M2400 Data Store (in a grid configuration)</td>
</tr>
<tr>
<td></td>
<td>- Avamar Virtual Edition (metadata storage only)</td>
</tr>
<tr>
<td></td>
<td>- Avamar NDMP Accelerator Node</td>
</tr>
<tr>
<td></td>
<td>- Avamar VMware Image Backup/FLR Appliance</td>
</tr>
<tr>
<td>NetWorker</td>
<td>- NetWorker server</td>
</tr>
<tr>
<td></td>
<td>- NetWorker storage node</td>
</tr>
<tr>
<td></td>
<td>- NetWorker Management Console server</td>
</tr>
<tr>
<td></td>
<td>- NetWorker vProxy Appliance</td>
</tr>
<tr>
<td>ProtectPoint for VMAX</td>
<td>- VMAX3 or VMAX All Flash Array</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD6300 or higher</td>
</tr>
<tr>
<td>Data Domain</td>
<td>- Data Domain DD2200 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD2500 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD3300 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD4200 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD4500 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD6300 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD6800 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD7200 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD9300 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD9500 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain DD9800 Controller</td>
</tr>
<tr>
<td></td>
<td>- Data Domain Boost</td>
</tr>
</tbody>
</table>
All converged backup systems include the following features:

- Factory integrated by Dell EMC
- Delivered in Dell EMC cabinets
- Dell EMC supported
- Backup data never leaves the Converged System network (does not apply to Vblock System 100 and VxBlock and Vblock Systems 200 series).

For an Avamar Virtual Edition system, install the associated Data Domain system in either a Converged System cabinet or in a customer supplied cabinet.

**Determining which converged backup system to use**

Proper converged backup system sizing requires an understanding of the backup capacity and the backup and restore speeds. Proper sizing includes current backup requirements with a plan to seamlessly scale up to meet the capacity requirements for three to five years. Proper component selection requires the use of appropriate sizing tools.

**Avamar**

Avamar is comprised of software and hardware components and provides a data backup and recovery solution with deduplication technology.

Avamar comes in both physical and virtual editions. In general, references to Avamar through this guide apply to both editions. However, Avamar Virtual Edition is a single node system that integrates with Data Domain Systems DD2200, DD2500, DD3300 and DD6300 only. References to other Avamar configurations and Data Domain systems do not apply to the virtual edition.

**Avamar hardware**

The Avamar Server manages the Avamar backups and, depending on the configuration, targets Avamar data store nodes or a Data Domain or both for backup storage. The metadata maintained by Avamar software is stored on the configured disk drives in the Avamar datastores.

**Avamar software**

Avamar software provides the following features for Converged Systems:

- VMware vSphere Web Client plug-in
- Instant Access VM restore from Data Domain
  
  **Note:** This feature is not supported when integrated with the Data Domain 3300.
- Self-service file restore
- Multiple simultaneous backups per proxy
- 24x7 backups
- Cloud Tier support when integrated with a Cloud Tier-supported and a Cloud Tier-enabled Data Domain System
- Ability to meet high service level agreements (SLAs) expected with applications running on a Converged System
- Avamar Backup and Recovery Manager, which provides real time monitoring of activities and events, backup reports, systems, and configurations. Optionally, use Avamar Backup and Recovery Manager to configure basic Avamar replication.

**Avamar Virtual Edition with Data Domain**

Avamar Virtual Edition combined with Data Domain is a data backup and recovery solution with deduplication technology. It comprises a VMware virtual appliance and Avamar software.

Avamar Virtual Edition provides the following features:

- One Avamar instance deployed as a VM on the management cluster in the AMP-VX to protect management workloads.
May be deployed on the AMP-VX management cluster, as a separate instance, to protect production workloads.

May be deployed on the VMware vCenter production cluster where AMP-2S or AMP-3S is the converged infrastructure management platform to protect production workloads.

May be deployed on the VMware vCenter management cluster on a VxRack System FLEX management controller to protect production workloads.

Supports the backup of VMs through Avamar clients or one or more Avamar proxies.

Integrates with DD2200, DD2500, DD3300 and DD6300 for the Avamar backup target.

Replicates with one of the following:
- Another Avamar Virtual Edition with a Data Domain system
- An Avamar Single Node or Grid with a Data Domain system.

Avamar Virtual Edition integrates with the latest version of Avamar software to provide the same features for Converged Systems as Avamar physical systems provide.

**Avamar Virtual Edition Limitations**

The following limitations apply to Avamar Virtual Edition:

- As with other Avamar with Data Domain systems, a Dell EMC Professional must size the solution.
- Avamar Virtual Edition with Data Domain is supported for backing up a single Converged System. It cannot be used for backing up multiple Converged Systems.
- Avamar Virtual Edition is not supported for backups of non-Converged Systems or physical or VMs outside of the supported Converged System.
- Avamar Virtual Edition is not scalable to a multi-node Avamar server.
- Resizing of the Avamar Virtual Edition VM is not supported.
- Scalability of Avamar Virtual Edition is limited to deploying additional separately managed Avamar Virtual Edition VMs. Each Avamar Virtual Edition instance requires a separate pane of glass for management.
- Avamar Virtual Edition is configured with a single network interface, which means that all management, backup, and replication traffic will traverse a single interface on a single VLAN.

**Use cases for Avamar Virtual Edition with Data Domain**

The following table lists use case details for an Avamar Virtual Edition configuration:

<table>
<thead>
<tr>
<th>Use case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Site</td>
<td>- Small customer sites (non-enterprise) with a single Converged System&lt;br&gt;- Backup and recovery of VMs, through Avamar Client or Avamar Proxy&lt;br&gt;- Backup of Converged System bare metal machines through Avamar Client&lt;br&gt;- Lower capacity and lower change rate environments&lt;br&gt;- No resiliency for Avamar Virtual Edition with Data Domain environments</td>
</tr>
<tr>
<td>Note:</td>
<td>Replicate Avamar Virtual Edition and Data Domain systems to a similar system at a remote location for redundancy.</td>
</tr>
<tr>
<td>Multi-Site</td>
<td>- Remote Office or Branch Office sites&lt;br&gt;- Single Converged System per site&lt;br&gt;- Backup and recovery of VMs, through Avamar Client or Avamar Proxy&lt;br&gt;- Backup of Converged System bare metal machines through Avamar Client&lt;br&gt;- Lower capacity and lower change rate environments</td>
</tr>
</tbody>
</table>
NetWorker

NetWorker is a software-based backup and recovery system that runs on virtual Microsoft Windows servers. NetWorker requires separate storage hardware as a backup target. A converged backup system with NetWorker uses Data Domain for storage.

NetWorker software provides the following features for Converged Systems:

- NetWorker is deployed as a minimum of three VMs on the management cluster on the AMP-VX.
- NetWorker is deployed as a minimum of three virtual machines on a production cluster on the AMP-2S and AMP-3S management platforms.
- NetWorker is deployed as a minimum of three VMs on the VXRM cluster on the VxRack Flex Management Controller management platform.
- Ability to back up a wide variety of physical and virtual compute environments, applications, and database, at image and file level.
- VMware vSphere Web-Client plug-in
- Instant Access VM restore from Data Domain
  \[\textbf{Note:} \text{This feature is not supported when integrated with the Data Domain 3300.}\]
- Self-service file restore
- Multiple simultaneous backups per proxy
- 24x7 backups
- Cloud Tier support when integrated with a Cloud Tier-supported and a Cloud Tier-enabled Data Domain System
- Ability to meet high SLAs expected with applications running on a Converged System

The NetWorker server, storage node, and management console server reside on three separate Windows Server-based VMs. The NetWorker vProxy Appliance is a Linux-based virtual appliance that is deployed to VMware vCenter using an OVA.

The following table describes NetWorker components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetWorker server</td>
<td>Provides the services to back up and recover data. Includes an index database of backup history.</td>
</tr>
<tr>
<td>NetWorker storage node</td>
<td>Maintains the physical connection to the backup target device (in Integrated Data Protection, this device is a Data Domain system). The storage node offloads from the NetWorker server much of the data movement involved in a backup or recovery operation.</td>
</tr>
<tr>
<td>NetWorker Management Console server</td>
<td>Manages, monitors, and provides reports on all NetWorker servers and clients in the backup environment.</td>
</tr>
<tr>
<td>NetWorker vProxy Appliance</td>
<td>Acts as a proxy to perform image-level backups for VMware VMs. Integrates with VMware vSphere Web Client.</td>
</tr>
</tbody>
</table>
Data Domain

Data Domain systems provide data storage targets for converged backup systems. Data Domain supports deduplication of backup data before writing it to storage, thus minimizing storage requirements by storing only unique data.

Data Domain Boost

Data Domain Boost (DD Boost) extends the optimization capabilities of Data Domain solutions, simplifies disaster recovery procedures, and significantly increases performance by distributing parts of the deduplication process to the backup server.

Data Domain Extended Retention

The Data Domain Extended Retention software option is a great feature for storing and managing backups that must be kept for long periods of time. Retention periods spanning years are commonly required to meet business requirements such as compliance, e-discovery, or archiving. Data Domain Extended Retention is a two-tiered file system that dedicates storage to active and archive functions. Backups stored on the Data Domain Controller are first placed on the active tier. The data, in the form of complete files, is later moved to the archive tier, based on user-defined data-movement policies.

Data Domain Cloud Tier

Data Domain Cloud Tier sends deduplicated data directly from the Data Domain to a public, private, or hybrid cloud for long term retention. The Cloud Tier feature provides the following benefits:

- Scalable, native, automated, and policy based cloud tiering
- Storage of up to twice the maximum active tier capacity in the cloud for long term retention
- Sends only unique, deduplicated data to cloud storage for reduced storage footprint and network bandwidth
- Allows migration of offsite storage from tape to the cloud

Supported Cloud services include:

- Elastic Cloud Storage
- Virtustream Storage Cloud
- Microsoft Azure
- Amazon Web Services

Data Domain Metadata on Flash

The Data Domain Metadata on Flash feature creates caches for the Data Domain file system metadata. The caches are created on solid-state drives (SSD) and accelerate access to metadata and backup data through low latency and high IOPS. This feature improves performance for both traditional and random workloads.

Data Domain Standalone

In a converged environment where backups utilizing Avamar, NetWorker, or ProtectPoint are not desired, the alternative is Data Domain Standalone.

This offers Data Domain without the requirement of Avamar, NetWorker, or ProtectPoint. When integrated with a Converged System, it is recommended that Data Domain utilizes a Data Domain virtual Ethernet interface and LACP for IP network connectivity with the exception of the DD3300. For Data Domain systems that do not support LACP, such as the DD3300, the use of IFGROUPS is recommended to provide for load balancing across two 10GbE interfaces. It also introduces support for Data Domain Boost over Fibre Channel with the addition of 8 Gb or 16 Gb Fibre Channel IO modules. The use cases for this solution are as follows:

- Data Domain Boost for Enterprise Applications (Dell EMC supported)
Backup and recovery

- Backup using Data Domain Boost over IP
- Backup using Data Domain Boost over FC

  - Backup to Data Domain CIFS or NFS Share
  - Microsoft SQL Management Studio
  - Oracle RMAN
  - Other third party applications that include a native backup utility with the ability to backup to disk (CIFS\NFS)

  - Veeam, NetBackup, HP DataProtector
  - Backup using DD Boost over IP
  - Backup using DD Boost over FC
  - Backup to disk (CIFS\NFS)

Data Domain Boost for Enterprise Applications

This topic describes best practices for performing backups from third-party applications using Data Domain Boost (DDBoost).

In certain environments, backups and restores of supported critical databases and applications can be monitored by a database administrator or application owner with the installation of Data Domain Boost for Enterprise Applications (DDBEA) on the application host. The DDBEA agent integrates with the applications native management utility and allows for efficient backups from the application host to the Data Domain utilizing the DDBoost protocol. Restores may also be performed in the same fashion. For most applications, these backups and restores are supported over both IP and FC. For support of FC backups and restores, the Data Domain must contain two 2-port Fibre Channel IO modules, and the application host contain two FC HBAs connected to the SAN Fabric and zoned correctly. The Data Domain system must also be licensed for the DDBoost feature.

Data Domain and third-party application native backup utilities

This topic describes how third-party applications can perform backups to Data Domain.

Database applications such as Oracle or Microsoft SQL (as well as other third-party applications that are not supported with DDBEA) may also perform backups using their native management utilities by performing them directly to Data Domain. As long as these management utilities support backup to disk over IP, these backups may be directed to either CIFS or NFS shares created on the Data Domain system. These backups will not be as efficient as those using the DDBoost protocol and application side deduplication, but may benefit from target side deduplication on the Data Domain. If all backups are targeted for CIFS or NFS shares only, then a DDBoost feature license is not required. The DDBoost license may be added at a later time, if DDBoost backups are required.

Data Domain and third-party backup applications

Third-party backup applications may also utilize a Data Domain system as a target for its client's backups. These backups may be backed up to disk utilizing CIFS or NFS shares on the Data Domain, or to DDBoost if the backup application supports the DDBoost. Any backup application not utilizing DDBoost will only achieve the benefit of deduplication if it has its own proprietary client side deduplication and/or target side deduplication on the Data Domain. The Data Domain must be licensed for the DDBoost feature if backups are performed using DDBoost.
There are a number of third-party backup applications that contain the DDBoost libraries which support DDBoost backups over both FC and IP. For more information on these see the Dell EMC online Data Domain compatibility guide http://compatibilityguide.emc.com:8080/CompGuideApp/.

**Data Domain High Availability**

Data Domain offers a high availability option which supports nearly all currently supported Data Domain features and functionality, and integrates with all Data Domain supported converged infrastructure systems.

Data Domain High Availability (HA) is also supported in a switchless configuration when integrated with converged infrastructure systems.

Data Domain HA is supported on the following Data Domain systems:
- DD6800
- DD9300
- DD9800

**Data Domain High Availability features**

In a Data Domain HA configuration, two identical Data Domain controllers (nodes) are configured as an Active-Standby pair. This pair allows for redundancy in the event of a system failure, such as loss of power, or system crash of the Active node.

Data Domain HA provides the following features:
- Automatic failover requires no user intervention
- Fully redundant design with no single point of failure within the system
- No loss of performance on failover
- Failover within 10 minutes for most operations (Data Domain Boost applications may take longer than this. CIFS, DD VTL and NDMP must be manually restarted)
- Ease of management and configuration through DD OS CLIs
- Alerting for hardware failures and malfunctions
- Maintains single-node performance and scalability within an HA configuration in both a healthy and degraded state
- Support of the same feature set as single node Data Domain systems (with the exception Data Domain Extended Retention and vDisk)
- Supports systems with all SAS drives
- No impact to the ability to scale the Data Domain system
- Support for non-disruptive software updates and upgrades

**Data Domain High Availability architecture**

Data Domain HA functionality is supported with IP and FC protocols. To ensure high availability, the Active and Standby nodes must have access to the same IP networks and fiber channel SANs.

For IP connectivity, the Data Domain HA system utilizes a floating IP address to ensure data access to the Data Domain HA system, regardless of which physical node is the Active node.

For FC connectivity, NPIV is used by the Data Domain HA system to move the FC WWNs between nodes, providing the FC initiators can re-establish connections after a failover event.
The following illustration shows the IP network and FC connectivity for a Data Domain High Availability system:

The following illustration shows the IP network and FC connectivity for a Data Domain High Availability system:

Data Domain Virtual Edition (DD VE) is a software-based Data Domain system that provides protection storage for any compatible data protection backup application. DD VE runs the same version of the Data Domain Operating System (DDOS) as its physical counterpart, so it supports many of the same features and functionalities such as DD Boost, deduplication, and Data Domain replication.

Data Domain Virtual Edition is not supported for direct deployment to the VxBlock System 1000 system nor the Advanced Management Platform for management of the VxBlock 1000. However, a DD VE instance deployed to the cloud may be leveraged as a replication partner for a VxBlock 1000 Integrated Data Protection system, which includes a Data Domain system.
**Dell EMC Cloud Disaster Recovery**

The Dell EMC Cloud Disaster Recovery (CDR) solution integrates with an on-premise Avamar and Data Domain for copying Avamar VM image backups to the cloud on either the Amazon Web Services (AWS) or Microsoft Azure cloud platform.

The solution allows for "in the cloud" recovery of one or many on-premise VMs that are protected with CDR.

In addition to full recovery and failover of VMs in the cloud, you can use this solution for disaster recovery testing and complete failback of VMs to an on-premise VMware vCenter server after a failover to the cloud. Disaster recovery testing and failover may be performed manually, on a per VM level, through the CDR Server UI or the Avamar UI. Disaster recovery (DR) testing and failover may also be performed through the creation and execution of a DR plan. During a DR test, the VM backup is rehydrated in the cloud and ready for disaster recovery validation or failover. If a failover is performed, the VM is rehydrated and once running in the cloud, is ready for production use.

**Note:** During a failover of a recovered VM in the cloud, it is recommended that you ensure the on-premise production VM is shut down to prevent user access and accidental data loss.

After a failover of a VM, the VM is eligible for failback to an on-premise vCenter. Failback of a VM or VMs that have been failed over to the cloud, is the automated process of copying the recovered VMs back to an on-premise vCenter system.

CDR can operate in one of two modes when configured with Amazon Web Services (AWS); Standard Mode and Advanced Mode. When configured with Microsoft Azure, CDR operates only in Standard Mode.

Standard mode for AWS and Microsoft Azure allows for crash consistent recovery in the cloud. To achieve application consistent recovery of VMs in the cloud, this solution requires CDR to operate in advanced mode, which is only supported with AWS.

CDR requirements for AWS Standard Mode include:

- Integrated Data Protection with Avamar and Data Domain (on-premise)
- VMware vSphere environment
- Network connectivity between on-premise systems and AWS
- AWS IAM user with appropriate permissions along with Access Key ID and Secret Access Key
- S3 bucket on a supported region
- Protected VMs must meet AWS Import/Export requirements

CDR requirements for AWS Advanced Mode include:

- All requirements for AWS Standard Mode
- Avamar Virtual Edition with integrated Data Domain Virtual Edition running as AWS instances
- VPN connectivity between on-premise Avamar with integrated Data Domain and AWS instance of Avamar Virtual Edition with integrated Data Domain Virtual Edition
- Avamar replication configured from on-premise to Avamar Virtual Edition AWS instance

CDR requirements for Azure (Standard Mode only) include:

- Integrated Data Protection with Avamar and Data Domain (on-premise)
- VMware vSphere environment
- Network connectivity between on-premise systems and Azure
- Azure subscription, Directory ID, Application IS, and key value
- Storage account on a supported location
Dell EMC Cloud Disaster Recovery architecture

This topic describes the Dell EMC Cloud Disaster Recovery (CDR) architecture for Amazon Web Services (AWS) and Microsoft Azure using Standard and Advanced modes.

CDR Standard Mode for AWS and Microsoft Azure

This configuration includes:

- An Integrated Data Protection system consists of an Avamar system integrated with a Data Domain deployed and configured to perform VM image backups.
- A CDR Add-on VM on the AMP management platform configures the CDR environment and deploys the CDR Server VM to the cloud.
- The CDR Add-on VM uploads of the image backups to the cloud provider.
- The CDR Server VM converts the VM image backups to the cloud providers VM instance type.

The following figure displays the architecture of a VxBlock System with Avamar and Data Domain Integrated Data Protection configured with CDR support for AWS in standard mode:

The following figure displays the architecture of a VxBlock System with Avamar and Data Domain integrated data protection configured with CDR support for Microsoft Azure in standard mode:
CDR Advanced Mode for AWS

This configuration includes:

- An Integrated Data Protection system consisting of an Avamar system integrated with a Data Domain deployed and configured to perform VM image backups.
- A CDR Add-on VM deployed on the AMP management platform configures the CDR environment and deploy the CDR Service VM to the cloud.
- The CDR Add-on VM uploads the image backups to the cloud provider.
- The Integrated Data Protection Avamar system is configured for replication to the Avamar Virtual Edition cloud instance over the VPN tunnel.
- The CDR Server VM converts the VM image backups to the cloud providers VM instance.
- The CDR Server VM triggers Avamar Virtual Edition to restore an application consistent backup with an Avamar client on the converted/restored instance.

The following figure displays the architecture of a VxBlock System with Avamar and Data Domain Integrated Data Protection configured with CDR support for AWS in Advanced Mode:
Converged backup system sizing

The specific configuration of a converged backup system is developed using a sizing process. To ensure the right size solution, trained specialists use a sizing tool designed to factor in how well various data types deduplicate. It is recommended that you size the backup system to meet current business needs and to plan up front for non-disruptive scalability to meet business requirements for three to five years.

For example, if you required protection for 50 TB of data, but in 36 months, you might need to protect as much as 150 TB, the backup system would have to scale to meet that need. If the backup system could not scale to meet the requirement, the original backup system would have to be replaced, or a second backup entity added. Proper initial planning will position a single backup entity to add capacity as needed.

Recovery types

Converged backup systems built upon the combination of Avamar or NetWorker and Data Domain deliver several recovery types.

The following recovery types are available:
- Guest-level recovery
- Image-level recovery
- File-level recovery from an image backup

Guest-level recovery

The process of guest-level recovery is the same in this solution for VMs as for traditional recovery from a backup application. You can recover directories, files, and applications in the Avamar Administrator GUI or NetWorker Management Console.
Image-level recovery
To recover data from an image-based backup, you can:

- Recover to the original VM
- Recover to an existing VM
- Recover to a new VM
- Use Instant Access Recovery

**Note:** This feature is not supported on the Data Domain 3300.

File-level recovery from an image backup
You can perform file-level recoveries (FLR) from an image-based backup using Avamar and NetWorker.

Replication of backup data to a second site
Converged backup systems support replication of backup data to a second site.

Replication using Avamar
The Avamar management feature set includes replication between primary and secondary Data Domain systems. The replication policy that is applied to each dataset in the Avamar Administrator controls this. Typical Avamar replication scenarios supported for datasets targeted to Data Domain include:

- Many-to-one, one-to-many, cascading replication
- Extension of data retention times
- Root-to-root replication

Similar to the recovery process, the replication process normally configured in Data Domain is automated in the Avamar framework and is transparent to the backup administrator. This replication functionality requires a remote Avamar server and a remote Data Domain system.

Replication using NetWorker
The NetWorker clone feature replicates save sets from one Data Domain Boost (DD Boost) device to another storage device. The clone is a complete and separate copy of the backup data, used for recovery operations or for creating other clones. The clone feature can act on single save sets or an entire volume of a DD Boost device. The original NetWorker browse and retention policies are maintained in the clone, although the policies can be changed in the clone.

It is recommended for Converged Systems that you replicate NetWorker backups to another Data Domain Data Domain Boost (DD Boost) device to improve replication performance and to maintain deduplication at the recovery site.

Replication of Data Domain Standalone with Data Domain Boost for Enterprise Applications, Application Native Backup Utilities, and third party backup applications
Backups from Data Domain with Data Domain Boost for Enterprise Applications (DDBEA) can be replicated using the Data Domain Replicator. In situations such as backups of Microsoft Applications, the application agent does not initiate or monitor the replication, although the Microsoft application can restore from the replicated copy. This is done by pointing the restore operation to the Data Domain where the replicated copy resides. DDBEA for Oracle allows for replication either through the Data Domain Replicator or through RMAN managed file replication. Managed file replication is the combination of Data Domain replicator and RMAN being configured to manage Data Domain replication. This is done by defining a `backup.cmd` file in RMAN to enable the remote Data Domain system as the target for replication. For these solutions, and any other DDBEA solution, refer to the Dell EMC documentation for specific and complete details.

Backups utilizing applications native backup utilities, when not used in conjunction with DDBEA, may be replicated using the Data Domain replicator. This can be accomplished by configuring replication of the collection, a directory, or Mtree. Replication of the collection, replicates the entire Data Domain system to another Data Domain. Replication of a directory or Mtree only replicates that which is defined in the replication pair.
For replication of backups from a third party backup application, refer to vendor documentation on Data Domain replication (where available).

## Cloud tier support

Converged backup systems support cloud tiering.

### Cloud tiering with Avamar or NetWorker and Data Domain

When integrated with a Cloud tier-supported Data Domain system, Avamar and NetWorker provide a secure and seamless method to tier data to the cloud for long-term storage. The backup administrator can create operations to move backups from the Data Domain to a public, private, or hybrid cloud service. After backups are in the cloud, administrators can perform seamless recoveries, as if the backups were located within the Data Domain system.

## IP-based data backup

Backup data travels between a converged backup system and a Converged System over the IP links that directly connect the two systems. This backup data replicates to an alternate data center using the customer’s IP infrastructure between the two sites. The result is a copy of critical data protected locally on the converged backup system and a duplicate copy of the data safely stored in a secondary location.

The following illustration shows the IP-based, data backup with replication to a second data center:

![IP-based data backup diagram]

## NDMP backup

Converged backup systems use network data management protocol backups to provide a backup and recovery solution for IP storage, such as Isilon, PowerMax/VMAX eNAS, VNX or VNNe products.

The converged backup system reads NDMP data from the IP storage device, deduplicates it, and writes it to a converged backup system storage device. If the storage device is non-NDMP, such as Data Domain, the backup data is first converted to a compatible format. The storage device or other component, depending on the configuration, deduplicates the data prior to it being written to the storage device.

**Note:** Because VxRack FLEX do not support file-based storage, you cannot back them up using NDMP.
Related information

IP-based data backup on page 33

Backup data travels between a converged backup system and a Converged System over the IP links that directly connect the two systems. This backup data replicates to an alternate data center using the customer’s IP infrastructure between the two sites. The result is a copy of critical data protected locally on the converged backup system and a duplicate copy of the data safely stored in a secondary location.

Enterprise deployment

A corporation with multiple branch offices might have multiple isolated backup systems. The best practice is to deploy a centrally-managed backup architecture. Converged backup systems also protect against site disasters by replicating the daily backups offsite. This solution is fast, network efficient, and eliminates the risks and costs associated with tape backups.

Ports are allocated in the Integrated Data Protection cabinet to support up to four directly-connected Converged Systems.

Applications and data in remote offices back up to a local converged backup system. Converged backup systems in remote offices replicate data to the converged backup system in the regional data center. This provides an off-site copy in case of disaster at the remote office.

Applications and data created in the regional data center are backed up to the converged backup system in the regional data center. Only the data that was created in the regional data center is replicated to the primary data center. The converged backup system in the primary data center replicates to the converged backup system in the secondary data center. The converged backup system in the secondary data center replicates to the converged backup system in the primary data center.

The following example shows the global deployment of a converged backup system designed to provide rapid local file recovery:
This illustration shows:

- The remote offices replicate backups to the regional data center for disaster recovery.
- Only data created in the regional data center is replicated at the primary data center.
- If the primary data center and secondary data center are in an active/active configuration, then the most common deployment is to cross-replicate backups between the data centers for disaster recovery.
- If the two data centers are in an active/passive configuration, then the backup replication is one way.
- In some countries, laws prevent backups from crossing regional boundaries. This is important to understand when developing remote backup or replication solutions.

### Using Oracle RMAN with converged backup systems

There are two common methods for using a converged backup system with Oracle databases.

Use one of these systems to back up Oracle databases:
Backup and recovery

- An Avamar agent or a NetWorker Module for Databases and Applications (NMDA) to redirect data to Data Domain.
- Oracle Recovery Manager (RMAN) and Data Domain Boost to back up directly to Data Domain.

Converged backup systems are directly integrated into the Converged System network. As a result, Oracle backup traffic is completely offloaded from the customer's backup network.

A converged backup system implemented for other applications already has the network connections between the Converged System and the Data Domain controller in place.

The following illustration shows the high-level connectivity between a Converged System and converged backup system for Oracle database native backup and recovery directly to Data Domain:

Related information

Converged backup systems connectivity overview on page 12
A converged backup system is a pre-integrated backup system, built and supported by Dell EMC, and containing a combination of Avamar or NetWorker, Data Domain, and Cisco switches.

ProtectPoint for VMAX3 and VMAX All Flash arrays with Data Domain

ProtectPoint for VMAX3 and VMAX All Flash arrays with Data Domain is a data protection solution that integrates primary storage on a VMAX array with protection storage on a Data Domain system.

Note: This ProtectPoint section uses VMAX array as a generic term for VMAX3 and VMAX All Flash arrays.

ProtectPoint offers the following features:
- Uses FC to perform block level copies from application source LUNs to a Data Domain to create incremental backups.
- Provides data protection where small or virtually non-existent backup windows exist.
Meets extremely demanding recovery time objectives (RTO) or recovery point objectives (RPO), where traditional backups might not.

Provides backups with little or no impact on application servers.

Enables direct backup from VMAX array (primary storage) to Data Domain (protection storage).

Sends only unique data from primary storage to protection storage, which eliminates the impact on the local area network and minimizes the impact on the storage area network.

Uses Data Domain as protection storage, which reduces backup storage requirements.

**ProtectPoint components and data flows**

The following illustration shows the components in a ProtectPoint solution:

![ProtectPoint components and data flows](image)

The following points describe the ProtectPoint solution components:

- **AR Host** is the application or recovery host.
  - The application host is where the application being backed up is installed. The data being backed up is on production storage presented to the application host from the VMAX array.
  - The recovery host is where data is restored to. This host can be the application host or a separate host.
- The primary storage software features used for ProtectPoint are *SnapVX* and *FAST.X*
- The primary storage production device is the storage presented to the application host from the VMAX array.
- The primary storage backup device is Data Domain storage encapsulated by the VMAX to appear as VMAX local storage.
- Data Domain block services for ProtectPoint allows the efficient creation of a static image of the primary storage device.
- Data Domain static images are the stored images of the ProtectPoint backups.

The following illustration shows a detailed backup data flow for ProtectPoint:
The following sequence of events occur during backup:

- The primary storage feature *SnapVX* is initiated from the AR Host.
- *SnapVX* creates a snapshot of the primary storage production device.
- Using Change Block Tracking (CBT), the changed data is copied to an encapsulated Data Domain storage device.
- Data Domain creates and stores a static image of the snapshot.

The following illustration shows detailed recovery data flow for ProtectPoint:

There are two types of restore available with ProtectPoint:

- **Object-level** (from VMAX or Data Domain)
- **Full-application rollback**

The following table lists the sequence of events and possible use cases for each restore type:
### ProtectPoint workflows

ProtectPoint workflows are initiated by the application administrator to protect applications and data. Before the workflow is triggered, the application must be quiesced to ensure that the snapshot on the Data Domain system is application consistent. ProtectPoint database application agents work with the application being protected to automatically quiesce the application. The application administrator is also responsible for retaining and replicating copies, restoring data, and recovering applications.

**Note:** When using ProtectPoint in a VMware virtual environment, only VMs running Microsoft or Linux operating systems with RDM storage are supported.

### ProtectPoint File system agent

The ProtectPoint File system agent is compatible with the following operating systems:

- Microsoft Windows
- Red Hat Enterprise Linux
- SuSE Linux Enterprise Server
- Oracle Linux
- HP-UX
- Oracle Solaris
- IBM AIX

<table>
<thead>
<tr>
<th>ProtectPoint restore type</th>
<th>Sequence of restore events</th>
<th>Use case</th>
</tr>
</thead>
</table>
| **Object-level restore from VMAX** | - The Data Domain writes the static image to the encapsulated storage device, making it available on primary storage via FAST.X restore device.  
- The FAST.X restore device is mounted to the AR host by the application administrator.  
- The application administrator uses OS and application-specific tools and commands to restore specific objects to a recovery device on the VMAX array. | - The Data Domain is inaccessible from the AR Host.  
- Prolonged access to recovered data is required.  
- Access to recovered data is required from the production host. |
| **Object-level restore from Data Domain** | - Data Domain restore device is made available to the AR host.  
- The application administrator uses OS and application-specific tools and commands to restore specific objects directly to the AR host. | - The VMAX is inaccessible from the AR Host.  
- Transitory access to recovered data is required.  
- Access to recovered data is required from a host other than the production host.  
- Instant access to recovered data is required.  
- The ability to perform third-party tape out is required.  
- The ability to perform in-place data integrity verification is required. |
| **Full-application rollback** | - The Data Domain writes the static image to the encapsulated storage device, making it available on primary storage.  
- The encapsulated recovery device is copied to the production device (overwriting the production device). | Full recovery of the production LUN to a specific point in time is required. |
ProtectPoint Database application agent

ProtectPoint Database application agent is compatible with the following applications:

- Oracle with RMAN
- SAP on Oracle via BR*Tools
- IBM DB2 using Advanced Copy Services (ACS)

Using Enterprise Hybrid Cloud with converged backup systems

The Enterprise Hybrid Cloud is a solution based on a defined reference architecture, which integrates products and services from Dell EMC and VMware. The solution is based on a number of Dell EMC technologies and the VMware vRealize Suite.

Two major features of the Enterprise Hybrid Cloud solution are automation and self-service provisioning of virtual machines. By combining the Dell EMC-provided customized workflows with a converged backup system (built with Avamar and Data Domain components), Backup as a Service (BaaS) can be implemented to automate and provision backup data protection.

The use of Avamar for backup and recovery of Enterprise Hybrid Cloud provides the following benefits:

- Abstracts and simplifies backup and restore operations for cloud users
- Uses VMware Storage APIs for Data Protection, which provides Changed Block Tracking for faster backup and restore operations
- Provides full image backups for running virtual machines
- Eliminates the need to manage backup agents for each virtual machine
- Minimizes network traffic by deduplicating and compressing data

Avamar configurations for Enterprise Hybrid Cloud

Several Avamar configuration use cases are possible with Enterprise Hybrid Cloud.

Standard Avamar configuration

The following table lists use case details for a standard Avamar configuration:

<table>
<thead>
<tr>
<th>Use case type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Single-site with single VMware vCenter Enterprise Hybrid Cloud deployment</td>
</tr>
<tr>
<td>Alternate</td>
<td>Continuous Availability dual-site/single VMware vCenter Enterprise Hybrid Cloud deployment</td>
</tr>
<tr>
<td></td>
<td>Disaster Recovery dual-site/dual VMware vCenter Enterprise Hybrid Cloud deployment</td>
</tr>
<tr>
<td></td>
<td>Caveats for alternate use cases:</td>
</tr>
<tr>
<td></td>
<td>Provides no resiliency for the second site. If the site that hosts the Avamar instances is lost, there is no ability to restore from backup.</td>
</tr>
<tr>
<td></td>
<td>In a Continuous Availability dual-site/single VMware vCenter environment, virtual machines that reside on the site with no Avamar instances will back up across the WAN.</td>
</tr>
<tr>
<td></td>
<td>In a disaster recovery dual-site/dual VMware vCenter topology, virtual machines that reside on the recovery site (registered with a different VMware vCenter) have no ability to back up.</td>
</tr>
</tbody>
</table>

Redundant Avamar configuration with single VMware vCenter

The following table lists use case details for a redundant Avamar configuration with single VMware vCenter:
Primary

Dual-site/single VMware vCenter Enterprise Hybrid Cloud deployment.

Alternate

Single-site topology. This provides a backup infrastructure that can tolerate the loss of a physical Avamar.

Note:
The redundant Avamar/single VMware vCenter configuration should not be used in a disaster recovery dual-site/dual VMware vCenter topology. The redundant Avamar/dual VMware vCenter configuration better suits the disaster recovery dual-site topology without the need for extra components.

Redundant Avamar configuration with dual VMware vCenter

The following table lists use case details for a redundant Avamar configuration with dual VMware vCenter:

<table>
<thead>
<tr>
<th>Use case type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Dual-site/dual VMware vCenter Enterprise Hybrid Cloud deployment.</td>
</tr>
<tr>
<td>Alternate</td>
<td>No valid alternate use cases for this configuration.</td>
</tr>
</tbody>
</table>

Refer to the Enterprise Hybrid Cloud: Concepts and Architecture Solution Guide for more information.
Business continuity and disaster recovery

Integrated Data Protection provides business continuity services through VPLEX and disaster recovery services through RecoverPoint, and their related products and technologies.

VPLEX

VPLEX delivers enhanced availability (zero data loss, near-zero downtime) of applications and data. VPLEX also delivers enhanced mobility of applications and data (in other words, the migration of applications and data between systems without the burden of work, planning, and downtime associated with traditional migrations).

A VPLEX cluster resides in the data path between the Converged System servers and storage, where it can create data copies. Copies can be created locally or over distance and can be read and written simultaneously.

VPLEX enables dynamic workload mobility and continuous availability within and between Converged Systems over distance. VPLEX also provides simultaneous access to storage devices at two sites through the creation of VPLEX distributed virtual volumes, supported on each side by a VPLEX cluster.

The VPLEX Integrated Data Protection solution for Converged Systems uses the following components and technologies:

- One or more Converged Systems
- VPLEX
- VMware vCenter Server
- VMware vSphere High Availability
- VMware vMotion

Dell EMC supports the following VPLEX systems for Integrated Data Protection solutions:

- VPLEX Local
- VPLEX Metro

VPLEX Local consists of a single VPLEX cluster, which provides the ability to manage and mirror data between multiple Converged Systems from a single interface within a single data center.

VPLEX Metro consists of two VPLEX clusters connected with inter-cluster links over distance. VPLEX Metro enables concurrent read and write access to data by multiple hosts across two locations. By mirroring data between two sites, VPLEX Metro provides non-stop data access in the event of a component failure or even a site failure.

The VPLEX Witness is an optional component for VPLEX Metro implementations. It can be deployed at a third site to improve data availability in the presence of cluster failures and inter-cluster communication loss. The VPLEX Witness deploys as a virtual machine, and its VMware ESXi host must reside in a separate failure domain from both VPLEX clusters to eliminate the possibility of a single fault affecting both a cluster and VPLEX Witness. The VPLEX Witness can be deployed on VMware vCloud Air as a third site domain.

The VPLEX Witness observes the state of the clusters and can distinguish between an outage of the inter-cluster link and a cluster failure. The VPLEX Witness then uses this information, together with the preconfigured detach-rules, to guide the clusters to either resume or suspend I/O.

VPLEX use cases

The following table describes VPLEX use cases:
Use case | Description
--- | ---
Mobility | Enables data mobility and relocation between storage arrays located in Converged Systems in a single data center, or between Converged Systems in two remote data centers, without impacting users.
Collaboration | VPLEX provides efficient real-time data collaboration over distance for big data applications.
VPLEX Metro HA without cross-connect | Significantly reduces the recovery time objective (RTO) by combining VPLEX Metro HA with VMware HA. Virtual machines automatically restart after a failure.
VPLEX Metro HA with cross-connect | Eliminates RTO for most of the failure scenarios. The only single failure scenario that causes a virtual machine restart is a host failure.
MetroPoint | MetroPoint combines VPLEX Metro and RecoverPoint to create a three-site or four-site solution that provides the best of both products for Converged Systems, including continuous availability, operational and disaster recovery, and continuous data protection.

VPLEX hardware models

The VPLEX product is offered in the following models:

- **VPLEX VS2**
  - The VS2 hardware platform is positioned for cost conscious customers that expects limited growth in their environment. The VS2 is the best fit for customers that want the business continuity benefits of VPLEX for small-medium hybrid array environments.
  - The VS2 hardware platform provides front-end and back-end speeds at a maximum of 8 Gbps over FC. It uses 8 Gbps FC for intra cluster communication and offers 10 GbE IP or 8 Gbps FC for WAN replication.

- **VPLEX VS6**
  - The VS6 is the latest hardware platform and is positioned for customers that have a performance intensive environment and are expecting to scale out. These customers probably run all-flash or a hybrid mix of storage arrays and might wish to refresh their VPLEX hardware from the VS2 to the VS6 platform.
  - The VS6 platform provides front-end and back-end speeds at a maximum of 16 Gbps over FC. It uses 40 Gbps InfiniBand for intra-cluster communication and offers 10 GbE IP or 16 Gbps FC for WAN replication.
  - With 2X IOPS at a third of the latency, the new flash optimized VS6 engine is built to handle the most demanding flash applications.

- **VPLEX for All-Flash**
  - VPLEX for All-Flash is a solution for All-Flash storage. This includes Dell EMC Unity AF, XtremIO, and VMAX AF.
  - It provides the customer with an unlimited capacity license for as many All-Flash Arrays (AFA).
  - VPLEX for All-Flash can be ordered with both VS2 and VS6 hardware. However, the VS6 platform is specifically created for All-Flash. Single, dual, and quad engine configurations are supported on both models.

VPLEX performance and scale

The following table compares the specifications for VPLEX VS2 and VS6 hardware:

<table>
<thead>
<tr>
<th>Specification item</th>
<th>VS2</th>
<th>VS6</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Generation</td>
<td>Intel Westmere Single Quad-Core per director</td>
<td>Intel Haswell Dual 6-Core per director</td>
<td>4.2 × VS2</td>
</tr>
<tr>
<td>DRAM Capacity</td>
<td>36 GB per director</td>
<td>128 GB per director</td>
<td>3.5 × VS2</td>
</tr>
</tbody>
</table>
### Specification item

<table>
<thead>
<tr>
<th>VS2</th>
<th>VS6</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front end/Back end</td>
<td>8 Gb FC</td>
<td>16 Gb FC</td>
</tr>
<tr>
<td>Interconnect</td>
<td>8 Gb FC</td>
<td>40 Gb InfiniBand</td>
</tr>
<tr>
<td>WAN</td>
<td>8 Gb FC, 10 GbE</td>
<td>16 Gb FC, 10 GbE</td>
</tr>
<tr>
<td>Management Server</td>
<td>Rack mount 1 RU server</td>
<td>Integrated internal server module, dual MMCS</td>
</tr>
<tr>
<td>Rack Configuration</td>
<td>Single, Dual or Quad Engine</td>
<td>Single, Dual or Quad Engine</td>
</tr>
<tr>
<td>Rack Density</td>
<td>22 RU for Single &amp; Dual, 34 RU for Quad</td>
<td>20 RU for Single &amp; Dual, 25 RU for Quad</td>
</tr>
</tbody>
</table>

### VPLEX components

A VPLEX cluster consists of the following hardware components:

- One, two, or four VPLEX engines
  - Each engine contains two directors
  - Each engine is protected by backup power:
    - VS2: Standby Power Supply (SPS), external to the engine
    - VS6: Battery Backup Unit (BBU), internal to the engine
- One management server
  - VS2: In-rack 1 RU server external to the VPLEX engine.
  - VS6: Embedded two Management Module and Control Stations (MMCS) in VS6 base engine with internal storage. These are named MMCS-A and MMCS-B.
- In the case of a dual or quad engine cluster, the cluster also contains:
  - VS2: Two 1 RU FC switches for communication between the directors in the engines
  - VS6: Two half-width 1 RU InfiniBand switches for communication between the directors in the engines
  - Two uninterruptible power supplies to provide backup power to:
    - VS2: the FC switches and the management server
    - VS6: the InfiniBand switches
- VPLEX Cluster Witness
  - Resides in a 3rd failure domain up to one second away
  - Lightweight VM
    - 1 vCPU and 1 GB RAM
    - 2.54 GB disk
  - IP connectivity
  - Can be deployed in VMware vCloud Air as a third site domain

Refer to the VPLEX Architecture Guide in the reference materials section for more information.

### Enterprise Hybrid Cloud and VPLEX for continuous availability

Enterprise Hybrid Cloud uses VPLEX for continuous availability.

VPLEX is used in a dual-site/single VMware vCenter Enterprise Hybrid Cloud environment when there is a requirement for continuous availability. Requirements for VPLEX remain the same as for non-Enterprise Hybrid Cloud environments,
such as the requirement for stretched Layer 2 VLANs or support of VXLANs, and that there is latency of less than 10 ms between the two sites.

Dual-site/single VMware vCenter Enterprise Hybrid Cloud deployment
The following components are used in a dual-site/single VMware vCenter Enterprise Hybrid Cloud deployment:

- VPLEX in Metro configuration
- VMware vSphere HA
- VMware vSphere vMotion
- VMware vSphere Metro Storage Clusters

Refer to Enterprise Hybrid Cloud: Concepts and Architecture Solution Guide for more information.

RecoverPoint
RecoverPoint is a data replication and recovery product that allows customers to roll back data to potentially any point in time.

RecoverPoint is a key component of the Integrated Data Protection product series, enhancing operational recovery, disaster recovery processes, and reducing potential data loss. RecoverPoint is typically deployed to protect specific business applications and data that need more data protection than a once-per-day backup provides.

RecoverPoint can protect data through the following methods:

<table>
<thead>
<tr>
<th>RecoverPoint protection method</th>
<th>Description</th>
<th>Use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local copy / Local replication</td>
<td>Data is replicated to a local volume.</td>
<td>Operational recovery</td>
</tr>
<tr>
<td>Remote copy / Remote replication</td>
<td>Data is replicated to a remote volume.</td>
<td>Disaster recovery</td>
</tr>
<tr>
<td>Local and remote copy / Local and remote replication</td>
<td>Data is replicated concurrently to local and remote volumes.</td>
<td>Operational and disaster recovery</td>
</tr>
</tbody>
</table>

RecoverPoint components and licensing
Details are provided for RecoverPoint components and licensing.

RecoverPoint systems comprise the following hardware and software components:

- RecoverPoint software provides the interface that customers use to manage replication and recovery.
- RecoverPoint Appliances (RPAs) run the RecoverPoint software. RPAs are physical Linux-based servers. RPAs also manage the replication process.
- RecoverPoint splitter software runs on storage arrays, where it intercepts data writes and splits them into two copies. One copy is passed to an RPA cluster for transfer to a replica copy volume and the other is written to its locally attached production copy.

Note: XtremIO, VMAX3/All Flash, and PowerMax are exceptions to this. XtremIO, VMAX3/All Flash, and PowerMax use a splitterless option called snap-based replication.

- RecoverPoint Storage Replication Adapter is an optional software module that integrates RecoverPoint with VMware Site Recovery Manager.

RecoverPoint use cases
RecoverPoint allows for several use cases.

Typically, RecoverPoint customers implement the following use cases:

- Supplement daily backups
Operational recovery
Disaster recovery and disaster recovery testing
Data repurposing, development, and testing

Supplementing daily backups

RecoverPoint is useful for business applications that cannot tolerate a loss of up to 24 hours of data. For those business applications, the question is whether to use RecoverPoint to replace or to supplement once-per-day backups.

Use RecoverPoint to supplement once-per-day backups, for the following reasons:

- Customers commonly keep once-per-day backups for 30 to 60 days or even archive them indefinitely. A file from any one of those backups can be recovered. RecoverPoint retains data for much shorter periods and does not support long-term data archiving and recovery.
- A corrupted file that is replicated is still a corrupted file. If using RecoverPoint alone, recovery from a corrupted file is only possible if the corruption is detected while a snapshot containing the uncorrupted file is still in the RecoverPoint journal. Using once-per-day backups in conjunction with RecoverPoint delivers a level of insurance above that of either method alone.

The following illustration shows the combination of daily backups and RecoverPoint replication on Converged Systems:

Operational recovery
RecoverPoint allows customers to quickly recover from operational failures through its ability to roll back to any point in time (PiT).

Recovery from an operational disaster using RecoverPoint can occur through the following methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production recovery</td>
<td>Recovers the entire production data set from an uncorrupted point in time on the replica copy volume.</td>
</tr>
<tr>
<td>File recovery</td>
<td>Copies single or multiple files from the replica copy volume to replace corrupted files. Makes the replica copy volume accessible, first, by placing it in one of the available image access modes (physical, virtual, and direct).</td>
</tr>
</tbody>
</table>
By default, RecoverPoint snapshots are crash-consistent. To ensure write-order consistency across specific production copy volumes, add the volumes to the same consistency group. RecoverPoint can provide application consistent snapshots for compatible applications, such as Microsoft Exchange and Oracle.

**Disaster recovery**

The quickest way to resume services after a major infrastructure failure is often to transfer the services to another facility. Remote replication allows customers to maintain up-to-date replica data in remote sites over any distance.

Use synchronous replication when the distance between two Converged Systems is short enough to allow it. Data in the disaster recovery site will be fully synchronized with the production site and the disaster recovery site can resume operations should a disaster occur at the production site. XtremIO requires the use of VPLEX in front of RecoverPoint to provide synchronous replication.

Use asynchronous replication when the distance between Converged Systems is too far to support synchronous replication. Data in the disaster recovery site will be synchronized as closely as possible with the production site. Any data lag that occurs depends on network bandwidth, data change rate, and the distance between the production and disaster recovery sites.

The following illustration shows disaster recovery using traditional methods:

The following illustration shows disaster recovery using RecoverPoint:
When a disaster occurs, corrupted data might be replicated to the replica copy volume. With RecoverPoint, customers can easily choose any point in time and check it to ensure data integrity before doing a full failover of the production site. This avoids the delay of having to redo failovers that used corrupted data.

RecoverPoint supports multi-site topologies. Consider multi-site designs to consolidate or diversify disaster recovery sites.

Disaster recovery plans are typically tested before a real disaster recovery situation to ensure the plans function correctly. With RecoverPoint, customers can take replica data at a disaster recover site offline and use it in disaster recovery testing, as required, without impacting production data and without the delay of restoring data at the disaster recovery site from a tape backup.

Disaster recovery failover and testing is a manual process when using RecoverPoint alone. RecoverPoint integrates with VMware Site Recovery Manager to provide automated disaster recovery operations. Customers benefit from simplified failover and testing to any point in time.

**Data repurposing, development, and testing**

Customers can use replicas of their production data for repurposing, developing, and testing. As well as creating the replicas, RecoverPoint facilitates this use case by supporting the following features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to four copies of a single production volume</td>
<td>Having multiple copies means that customers can allocate some copies to recovery and others to alternative activities. This minimizes the risk of copy data being unavailable for recovery due to other activities being performed on it, while still allowing customers to work with up-to-date copies of production data.</td>
</tr>
<tr>
<td>Host application access to replica copy volumes</td>
<td>Various image access methods allow customers to access copy data while RecoverPoint continues to buffer production writes on the replica copy journal. Customers can also roll back changes made during image access when image access is suspended (if using logged access). This means that customers can perform testing and other activities on copy data with minimal risk to production data, even where only single copies of production data exist.</td>
</tr>
<tr>
<td>Recovery of replica copy volumes to an alternative location</td>
<td>Customers can restore data from a replica copy volume to any appropriate volume. This allows customers to repurpose data for alternative production requirements, such as analysis and reporting, or to recreate production environments in a testing or</td>
</tr>
</tbody>
</table>
RecoverPoint replication

RecoverPoint supports data replication over any distance.

Replication modes

RecoverPoint replicates data in one of the following replication modes:

- Asynchronous mode
- Synchronous mode (not supported with XtremIO)

Asynchronous mode

Asynchronous mode is the default replication mode for RecoverPoint. The application initiates a write and does not wait for the acknowledgment from the remote RecoverPoint Appliance (RPA) before initiating the next write. The data of each write is stored on the production RecoverPoint cluster, which acknowledges the write. The remote RPA cluster decides when to transfer the writes, based on the lag policy and system loads/available resources.

The main advantage of asynchronous replication is its ability to provide synchronous-like replication without degrading the performance of host applications.

Asynchronous mode might not be the best option for all situations. For example, a high data change rate can increase data stored between transfers and can cause data loss if a disaster occurs.

RecoverPoint replicates asynchronous only in situations in which doing so enables superior host performance without resulting in an unacceptable level of potential data loss.

Asynchronous snap-based replication mode (XtremIO is not supported)

RecoverPoint provides VNX users with an alternative asynchronous replication option called snap-based replication mode. This mode is particular useful during periods where a high load occurs or at user-configured intervals.

During a high load situation, the replication process cannot keep up with the incoming writes, which means that replication cannot continue and initialization is required. If high load continues during the initialization, RecoverPoint might be unable to create snapshots, which jeopardizes recovery point objective (RPO) requirements.

Snap-based replication improves performance under high load periods and uses write-folding to reduce WAN traffic. The longer the gaps between the snapshots, the higher the bandwidth reduction, and the greater the protection window due to less journal space being consumed.

In VNX snap-based asynchronous replication mode, the splitter still captures and provides the writes to the RPA journal.

The Dell EMC Unity array does not support snap-based replication.

Asynchronous XtremIO-supported snap-based replication mode

For both non-XtremIO and XtremIO, snap-based replication uses array-based snapshots and replicates the delta between two snapshots to the remote RecoverPoint cluster. However, snap-based replication for XtremIO is implemented differently to that of non-XtremIO, which is why both are discussed separately. Snap-based replication for XtremIO is implemented in different ways, depending on the types of array where the production volume and replica copy reside.

The following table describes how XtremIO snap-based replication is implemented:
The journal contains only pointers to snapshots and metadata. The journal does not contain any replicated data. Therefore, the journal size can be small—10 GB for regular consistency groups and 40 GB for distributed consistency groups.

A splitter is used at the replica and XtremIO snapshots are stored in the journal of the target array for distribution and point-in-time (PIT) access. After the entire snapshot has been replicated, it is bookmarked. This bookmarked snapshot is available for image access.

Writes coming from the production array splitter are stored as XtremIO snapshots. If the production array has snap-based replication enabled, a snap is created at the remote XtremIO array when the replication of a snapshot from production completes. When continuous replication is configured, snapshots are created at the remote XtremIO array once every minute.

When XtremIO is at the target, image access and recovery time objective (RTO) to any point in time is instantaneous.

**Asynchronous VMAX3/AF and PowerMax snap-based replication mode**

VMAX3/AF snap-based replication uses the native VMAX3/AF snap capabilities to create point-in-time consistent snaps of a consistency group's production volumes, and uses the snaps to synchronize the production volumes with the copy volumes.

This solution supports manual, continuous, and periodic snapshots, with a minimum period of 1 minute.

The following table describes the different replication options available:

<table>
<thead>
<tr>
<th>Production copy array type</th>
<th>Replica copy array type</th>
<th>Snap-based replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>XtremIO</td>
<td>XtremIO</td>
<td>The journal contains only pointers to snapshots and metadata. The journal does not contain any replicated data. Therefore, the journal size can be small—10 GB for regular consistency groups and 40 GB for distributed consistency groups.</td>
</tr>
<tr>
<td>XtremIO</td>
<td>Non-XtremIO</td>
<td>A splitter is used at the replica and XtremIO snapshots are stored in the journal of the target array for distribution and point-in-time (PIT) access. After the entire snapshot has been replicated, it is bookmarked. This bookmarked snapshot is available for image access.</td>
</tr>
<tr>
<td>Non-XtremIO</td>
<td>XtremIO</td>
<td>Writes coming from the production array splitter are stored as XtremIO snapshots. If the production array has snap-based replication enabled, a snap is created at the remote XtremIO array when the replication of a snapshot from production completes. When continuous replication is configured, snapshots are created at the remote XtremIO array once every minute.</td>
</tr>
</tbody>
</table>

In protecting VMAX3/AF and PowerMax arrays, the entire VMAX3/AF or PowerMax storage group is protected rather than the individual devices.

RecoverPoint supports using TimeFinder SnapVX to clone a copy, enabling you to access the clone rather than using RecoverPoint image access to access the copy directly.

Cloning a copy with TimeFinder SnapVX is recommended in the following situations:

- Image access is needed for an extended time.
- The accessed needs to support a heavy write workload.

For RecoverPoint for VMAX3/AF and PowerMax limitations, see to the *RecoverPoint 5.1 with VMAX3/AF/PowerMax Technical notes* document on Dell EMC support.

**Synchronous mode**

In synchronous mode, the application initiates a write, which is replicated to the remote RPA cluster. The write is acknowledged when it reaches the remote RPA memory. Therefore, the remote copy is always up-to-date with its
production copy. Application performance may be impacted when the solution is not properly sized. Poor WAN performance, SAN performance, and array performance, and high RPA load can all cause the application performance to degrade.

By default, new consistency groups are created with asynchronous mode enabled, and can be set to replicate synchronously through the Link policies.

**Dynamic synchronous mode**

You can enable dynamic synchronous mode for environments that replicate over longer distances or that experience high latencies at times on their WAN link. When dynamic sync is enabled, you can configure the replication policy to switch from synchronous to asynchronous replication when latency or throughput thresholds are exceeded. When the value drops below the threshold again, RecoverPoint returns to synchronous replication.

**RecoverPoint consistency groups**

RecoverPoint protects data volumes using consistency groups. By replicating changes to production volumes in the correct write order, consistency groups ensure that copies are always consistent and available for failover or restore.

Each consistency group can have an individual recovery point objective (RPO) and recovery time objective (RTO).

![Note:](image)

An RPO is the maximum tolerable data loss, measured in time, resulting from a data failure. An RTO is the maximum tolerable time that data can remain offline following a data failure. For example, if data must be restored to within one hour of when a failure occurs, and it takes two hours to restore the data, then the RPO is one hour and the RTO is two hours.

**RecoverPoint storage awareness**

RecoverPoint storage awareness provides a unified interface for storage integration and management from the RecoverPoint cluster.

It enhances RecoverPoint so customers can provision journal volumes on the storage array directly from the RecoverPoint console.

To enable RecoverPoint snap-based replication, register the VNX array in the RecoverPoint console. Dell EMC Unity arrays auto-register with RecoverPoint.

Registering the storage or VMware vCenter Server makes it possible to monitor connectivity and removes the requirement to repeatedly enter credentials to collect system information.

**RecoverPoint auto-provisioning and auto-matching for XtremIO arrays**

RecoverPoint 5.1.x and XtremIO version 6.0 and above can automatically provision volumes on XtremIO arrays.

When XtremIO arrays are used at both the production and copy site, RecoverPoint can automatically provision the production and copy journal volumes, and the copy data volume. The end user must only create the production data volume that is being replicated by RecoverPoint.

**Copy volume auto-matching (from the GUI only)**

If the production volumes reside on an XtremIO array at the replica site, and contain exposed volumes with the same names and sizes as the production volumes, RecoverPoint will automatically match these volumes to the production volumes according to name and size.

**RecoverPoint multi-site support**

RecoverPoint allows a single RecoverPoint cluster to replicate to multiple clusters, or multiple clusters to replicate to a single cluster.

RecoverPoint supports the following multi-site designs:
- Fan-out replication from a local site to up to four remote copies, or to one local and three remote copies. Each copy contains data from the same consistency group.
- Fan-in replication from up to four remote sites to one central site. Each copy contains data from a different consistency group.

**Note:** For fan-in topologies, one remote copy per consistency group can be synchronous and the remaining three (or all four) can be asynchronous. Because each link is independent, customers can access different points in time (PIT) in different locations.

Fan-out replication for XtremIO supports a maximum of three copies, consisting of one production and two copies. These copies can be local, remote, or a mix of both.

The following illustration shows RecoverPoint in a fan-out topology:

![Fan-Out 1:4](image-url)

The following illustration shows RecoverPoint in a fan-in topology:
Uses for multi-site topologies

The following table shows uses for multi-site topologies:

<table>
<thead>
<tr>
<th>Use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-level protection</td>
<td>Fan-out topologies allow you to implement multi-level protection for core data. You can choose how many copies of data to make and at how many locations to store those copies. Because each copy in a fan-out topology is independent of other copies, you can allocate copies to different roles. For example, you can allocate one copy to disaster recovery and another to testing and development.</td>
</tr>
<tr>
<td>Disaster recovery site consolidation</td>
<td>Fan-in topologies allow you to reduce the complexity and costs of managing multiple remote sites, by allowing you to replicate multiple remote sites through one RecoverPoint cluster in one central location. You can manage and maintain all replica data in one place and avoid the need for multiple clusters or multiple sites. You can also maintain a single disaster recovery site to protect multiple production sites.</td>
</tr>
</tbody>
</table>

Enterprise Hybrid Cloud and RecoverPoint for disaster recovery

Enterprise Hybrid Cloud uses RecoverPoint for disaster recovery.

RecoverPoint is used in a dual-site/dual vCenter Enterprise Hybrid Cloud environment when there is a requirement for disaster recovery. Typically, VMware vCenter Site Recovery Manager is part of the disaster recovery solution. RecoverPoint, as with typical environments, provides continuous data protection for any point in time (PiT) recovery. When paired with VMware vCenter Site Recovery Manager, it can also provide centralized recovery plans, automated failover and failback, non-disruptive testing of disaster recovery, and planned migration.

Dual-site/dual VMware vCenter Enterprise Hybrid Cloud deployment

The following components are used in a dual-site/dual VMware vCenter Enterprise Hybrid Cloud deployment:

- RecoverPoint
- VMware vCenter Site Recovery Manager

Refer to Enterprise Hybrid Cloud: Concepts and Architecture Solution Guide for more information.
RecoverPoint and VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) tightly integrates with VMware vCenter Server and vSphere Web Client to simplify disaster recovery (DR) management by automating the testing and orchestration of centralized recovery plans.

VMware SRM automates the orchestration of the failover process to the recovery site and also the failback to the production site. Failover and failback automation eliminates both complexity and errors inherent to manual processes. This level of automation also enables users to test their recovery plans non-disruptively, as often as required, increasing the predictability of recovery time objectives (RTOs) and ultimately increasing the level of confidence in the recovery plan.

RecoverPoint is responsible for all data replication between the production and recovery site. VMware SRM works in conjunction with RecoverPoint to automate and orchestrate the process of migration, recovering, testing, re-protecting, and fail-back of virtual machines. VMware SRM communicates with RecoverPoint through a Storage Replication Adapter (SRA) that is installed on the VMware SRM server.

The Virtual Storage Integrator (VSI) plug-in provides the additional ability to select recovery from any point in time from RecoverPoint. The VSI runs on a virtual machine that is deployed through an OVA into the virtual environment.

Use cases

VMware Site Recovery Manager supports several use cases and provides significant capability and flexibility to Dell EMC customers.

The following use cases for VMware Site Recovery Manager with Converged Systems are supported:

<table>
<thead>
<tr>
<th>Use case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster recovery</td>
<td>VMware SRM was specifically designed for disaster recovery. This is the least frequently used use case, but the most critical one. Site failures do not happen often, but when they do, fast recovery is critical to the business.</td>
</tr>
<tr>
<td>Planned migration / Disaster avoidance</td>
<td>Moving VMs and applications between sites during planned migration and disaster avoidance exercises are two common use cases for VMware SRM. VMware SRM gracefully shuts down the VMs at the protected site and restarts them at the recovery site in a predefined order. It supports full testing of the migration in a manner completely non-disruptive to production systems. It will also pause if any issues are discovered during the migration, thus providing an opportunity to correct them.</td>
</tr>
<tr>
<td>Upgrade and patch testing</td>
<td>The VMware SRM test environment provides an ideal location for operating system and application upgrade and patch testing. These test environments are complete copies of the production environments, but exist in an isolated network, which ensures that testing does not impact production workloads or replication.</td>
</tr>
</tbody>
</table>

The following illustration shows how Converged Systems use VMware SRM and RecoverPoint to provide automated failover with any point in time (PIT) recovery:
VMware SRM creates recovery plans that automate the failover of resources if a disaster occurs. VMware SRM recovery plans use protection groups to define specific items to move from a protected site to a recovery site. Customers must align the VMware SRM protection groups with RecoverPoint consistency groups, so that the failover of a VMware SRM protection group automatically includes the RecoverPoint data sets needed by the resources.

The following advantages apply when using RecoverPoint with VMware SRM:

- VMware SRM can use the point-in-time (PiT) recovery abilities of RecoverPoint.
- VMware SRM removes the need to interact with the RecoverPoint console during a DR situation and can automate the DR workflow to the point of pressing a single button.
- RecoverPoint removes distance limitations between production and DR sites through its ability to replicate data asynchronously while maintaining write-order consistency.

### AMP Protection

VMware Site Recovery Manager uses RecoverPoint to replicate the datastores on which the virtual machines reside. RecoverPoint connects to the Converged System storage array over Fibre Channel. The physical servers used in the AMP are not configured with HBAs and therefore cannot connect to the storage array over FC. Because of this and other reasons, VMware Site Recovery Manager cannot protect the AMP. If there is a need to protect one or more of the AMP element managers, the best practice is to move those VMs to the VMware ESXi hosts that run on the Cisco blade servers.

### Orchestration and automation

VMware Site Recovery Manager provides the vAdmin with built-in automation and orchestration capabilities to simplify the recovery of virtual machines. vAdmins can access these capabilities via the VMware vSphere Web Client snap-in.

The following table shows the automation capabilities and orchestration capabilities available with VMware Site Recovery Manager:

<table>
<thead>
<tr>
<th>Group</th>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation</td>
<td>Inventory mapping</td>
<td>Allows resource mapping, folder mapping, and network mapping. These mappings provide default settings for recovered VMs. For example, a VM can be connected to Network-A on the protected site,</td>
</tr>
<tr>
<td>Group</td>
<td>Capability</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Automation</td>
<td>Protection Groups with Datastore Groups or Storage Policy Protection Groups</td>
<td>Datastore Groups: Uses a manual process to protect/unprotect VMs, but with more flexibility. Storage Policy Protection Groups: Enables the automatic protection of VMs that are associated with a storage policy. More limitations than Datastore groups.</td>
</tr>
<tr>
<td>Automation</td>
<td>Deep integration with other VMware solutions</td>
<td>VMware vSphere PowerCLI provides Microsoft Windows PowerShell functions to administer VMware SRM or to create scripts that automate SRM tasks. The VMware vRealize Orchestrator plug-in for Site Recovery Manager allows you to automate the creation of a VMware SRM infrastructure to add virtual machines to protection groups and configure recovery settings of virtual machines.</td>
</tr>
<tr>
<td>Orchestration</td>
<td>Recovery Plans</td>
<td>Recovery plans are like an automated run book, controlling all the steps in the recovery process. A VM can be part of multiple recovery plans.</td>
</tr>
<tr>
<td>Orchestration</td>
<td>Priority Groups (Start-up Sequence)</td>
<td>There are five priority groups in VMware SRM. VMs in group one are recovered first and VMs in group five are recovered last. All VMs in a priority group are started at the same time and the next priority group is started only after all the previous VMs are booted up and responding. VMware tools must be installed.</td>
</tr>
<tr>
<td>Orchestration</td>
<td>Dependencies</td>
<td>When more granularity is needed for startup order, you can use dependencies on a per-VM level.</td>
</tr>
<tr>
<td>Orchestration</td>
<td>Shutdown and Startup actions</td>
<td>Shutdown actions apply to the protected VM at the protected site during a recovery plan run. Shutdown actions are not used during recovery plan testing. Startup actions apply to a VM that is recovered by VMware SRM. Powering on a VM after it is recovered is the default setting. In some cases, it might be desirable to recover a VM, but to leave it powered off.</td>
</tr>
<tr>
<td>Orchestration</td>
<td>Pre and Post power on steps</td>
<td>VMware SRM can run commands or scripts from the VMware SRM server at the recovery site before and after powering on a VM. Running a script inside a VM is also supported as a post-power-on step. VMware SRM can also display a visual prompt as a pre- or post-power-on step.</td>
</tr>
<tr>
<td>Orchestration</td>
<td>IP customization</td>
<td>The most commonly modified VM recovery property are the IP settings. Most companies have different IP networks at the protected and recovery sites. IP customization can be used in testing, failover, and fail-back operations. There are three methods to customize network settings:</td>
</tr>
</tbody>
</table>
RecoverPoint for Virtual Machines

RecoverPoint for VMs is a software-only product used to protect virtual machines that reside in a VMware vSphere environment. It provides local and remote replication capabilities with virtual machine-level granularity.

RecoverPoint for VMs targets the VMware administrator, whereas the standard RecoverPoint product targets the storage administrator. The RecoverPoint for VMs virtual RecoverPoint Appliances (vRPA) are installed in the VMware vSphere environment. The appliances then provide the RecoverPoint for VMs plugin into the VMware vSphere Web Client.

The vRPAs use the IP protocol to communicate with the VMware vSphere datastore. Each VMware ESXi host that participates in protecting virtual machines requires the RecoverPoint for VMs splitter to be installed.

VMware administrators can use the VMware vSphere Web Client to take a more active role in protecting and recovering virtual machines to any point in time with built-in orchestration and automation capabilities. RecoverPoint for VMs fully supports all standard RecoverPoint operations:

- Test Copy
- Recover Production
- Fail Over

With the automation and orchestration capabilities provided by RecoverPoint for VMs, VMware Site Recovery Manager (SRM) is not required. VMware SRM should be used only with RecoverPoint Classic.

RecoverPoint for VMs architecture

Describes and illustrates the RecoverPoint for VMs system architecture.

The RecoverPoint for VMs system consists of the following components:

- One or more RecoverPoint for VMs clusters. Refer to the latest documentation for the maximum number of clusters that a RecoverPoint for VMs system can contain.
A minimum of one virtual RecoverPoint Appliance (vRPA) and a maximum of eight vRPAs for each RecoverPoint for VMs cluster. These vRPAs manage all aspects of the data replication process. 

**Note:** Even though a single vRPA can be used to create a RP4VM cluster, the best practice for Converged Systems is to deploy a minimum of two vRPAs.

- RecoverPoint for VMs splitter installed in the VMware ESXi hypervisor. The RecoverPoint for VMs splitter is installed on every VMware ESXi host in the VMware vSphere cluster that will host VMs protected by RecoverPoint for VMs. The RecoverPoint for VMs splitter splits the write coming from the host and sends it to the vRPA and the virtual machine’s VMDK. The vRPAs handle all traffic to the journals and replicas as they do in a physical RecoverPoint system. All storage traffic between the vRPAs and the VMware vSphere datastores use the IP protocol.

- VMware vSphere Web client plug-in. The plug-in is the user interface for managing the RecoverPoint for VMs system. The vAdmin can manage all RecoverPoint for VMs operations from this interface.

The following illustration shows the RecoverPoint for VMs system architecture:

**RecoverPoint for VMs multi-site support**

RecoverPoint for VMs allows a single RecoverPoint for VMs cluster to replicate to multiple clusters, or multiple clusters to replicate to a single cluster.

RecoverPoint for VMs supports the following multi-site designs:

- **Fan-out replication** 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** from up to two remote sites to one central site. Each copy contains data from a different consistency group.
**Note:** For fan-in topologies, one remote copy per consistency group can be synchronous and the other can be asynchronous. As each link is independent, you can access different points in time (PiT) in different locations.

Besides the multi-site options listed above, RecoverPoint for VMs also supports a fully connected system, where all sites are connected with each other.

**Orchestration and automation**

RecoverPoint for VMs provides the vAdmin with built-in automation and orchestration capabilities to simplify the recovery of VMs. The vAdmin can access these capabilities using the VMware vSphere Web Client snap-in.

The following table shows the automation capabilities and orchestration capabilities available with RecoverPoint for VMs:

<table>
<thead>
<tr>
<th>Group</th>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automation             | VMDK manageability                   | • The ability to select the type of VMDK to use for the copy VM. The available options are:  
  - same as the source  
  - thick  
  - thin  
  • The ability to exclude certain VMDKs. For example, shared or non-persistent VMDKs.  
  • The ability to expand or add a VMDK without losing the journal or causing a full sweep of the consistency group. |
| Replication of VM hardware changes |                                    | • Memory and CPU changes to protected VMs are allowed and can be automatically replicated to all copy VMs.  
  • VMDKs added to a protected VM can automatically be provisioned on all copy VMs. |
| CAUTION                |                                      | When a VMDK is removed from a protected VM, the corresponding copy VMDK is not removed. This protects against accidental changes.  
  When a protected VM is deleted, the corresponding copy VMs are not removed. This protects against accidental changes. |
<p>| MAC address replication |                                      | MAC addresses of remote copy VMs located on a different vCenter are automatically replicated. |
| Orchestration          | Start-up Sequence                    | Both consistency groups and group sets have the ability to use the <em>Start-up Sequence</em> feature to define the startup order for the VMs in the consistency groups and the consistency groups in the group sets. |
|                        | User prompts                         | You can add user prompts in the <em>Start-up Sequence</em> for a consistency group for each VM to provide the vAdmin with configurable messages at certain points in the workflow. |</p>
<table>
<thead>
<tr>
<th>Group</th>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User scripts</td>
<td></td>
<td>You can add pre and post power up external scripts in the Start-up Sequence for a consistency group for each VM. You must define an external host for each vRPA cluster in the RecoverPoint for VMs system.</td>
</tr>
<tr>
<td>Networking enhancements</td>
<td></td>
<td>• The network settings for a VM can be changed for the copy VM in three different ways. Which method is used depends on the number of VMs that require their network settings to be changed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use the RecoverPoint for VMs GUI to change the network configuration of a small number of VMs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use a CSV file to change the network configuration of multiple VMs at a copy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use a CSV file to change the network configuration of multiple VMs in a system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If re-IP glue scripts have already been implemented during a previous version of RecoverPoint of VMs, these glue scripts can continue to be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To ensure that you don not lose your protection VM network configuration when you fail back to the production, ensure that you also edit the copy network configuration of your production VMs.</td>
</tr>
</tbody>
</table>

Note: For details regarding specific operating systems refer to the RecoverPoint for Virtual Machines Administrator’s Guide.

The following illustration lists the steps required to configure the network settings for the different use cases previously listed:
RecoverPoint and VPLEX

VPLEX extends services, such as automated disaster recovery (DR), distributed resource scheduling (DRS), high-availability (HA), and fault tolerance (FT), across data centers, where these were previously confined to single data centers. RecoverPoint enhances VPLEX by extending disaster recovery to additional sites and over long distances without additional investment in VPLEX infrastructure. RecoverPoint further enhances VPLEX by allowing data rollback to any point in time (PiT), meaning that all possible disaster recovery and business continuity requirements are met.

RecoverPoint uses the built-in VPLEX write splitter software, which splits data writes across VPLEX and RecoverPoint volumes. The VPLEX splitter also allows multiple RecoverPoint clusters to share a single splitter, so that up to four RecoverPoint clusters can protect a single VPLEX cluster.

**Note:** Dell EMC supports RecoverPoint access to third-party arrays through VPLEX only while customers are migrating data to an array.

VPLEX with RecoverPoint Data Protection

By integrating with RecoverPoint, VPLEX can take advantage of RecoverPoint’s DVR-like rollback of data. VPLEX volumes can replicate to local RecoverPoint volumes to provide Continuous Local Protection, or to remote volume to provide Continuous Remote Replication. Either scenario allows VPLEX to recover data to any point in time.

The following illustration shows how Converged Systems integrate VPLEX and RecoverPoint to provide two active failover sites with any-point-in-time recovery:
VPLEX with RecoverPoint data protection provides:

- Recovery to any point in time at the local or remote site.
- Support for heterogeneous storage arrays.
- Protection from data loss and corruption.

**VPLEX with RecoverPoint Disaster Recovery**

VPLEX can extend its disaster recovery capabilities to very long distances by using the RecoverPoint asynchronous replication capability and VMware SRM integration.

The following illustration shows how Converged Systems can integrate VPLEX and RecoverPoint to extend disaster recovery services to asynchronous distances:
VPLEX with RecoverPoint disaster recovery provides:

- The ability to combine short- and long-distance disaster recovery site locations.
- The ability to use VMware Site Recovery Manager for disaster recovery site operations.
- The extension of VPLEX disaster recovery functionality without the need for additional VPLEX hardware.

**MetroPoint**

MetroPoint combines VPLEX Metro and RecoverPoint to provide enhanced data protection for Converged Systems. MetroPoint protects writes from both sides of a VPLEX Distributed Device. MetroPoint replicates data from one VPLEX Metro site in a cluster to a remote Converged System over IP or Fiber Channel networks, using asynchronous, near-synchronous, or synchronous replication. Additionally, MetroPoint replication allows local copies at all VPLEX Metro sites. Dell EMC customers benefit from continuous availability of active-active applications across data centers while maintaining operational and disaster recovery.

MetroPoint can operate in a two-site, three-site, or four-site topology. It can load balance replication data across WAN links and can use VMware Site Recovery Manager to manage disaster recovery operations.

The following illustration shows an overview of MetroPoint operation:
MetroPoint operation

MetroPoint replication topologies

MetroPoint uses consistency groups to configure replication. An MetroPoint consistency group consists of the following copies:

- Two source copies (active production and standby production)
- Up to two local copies
- Up to one remote copy

A fully configured MetroPoint consistency group contains five copies. These copies are distributed as shown in the following illustration:
For a more detailed look at MetroPoint replication topologies, refer to the white paper *MetroPoint Continuous Availability with Comprehensive Data Protection* in the reference materials section of this document.

**Two-site MetroPoint topology**

In a two-site MetroPoint deployment, each site hosts a Converged System and an Integrated Data Protection cabinet running one VPLEX Metro site and containing one connected RecoverPoint cluster.

The following illustration shows an Integrated Data Protection two-site MetroPoint implementation:

In this two-site MetroPoint, the VPLEX Metro cluster is hosting a Distributed Volume (DR1) that spans Site A and Site B. At each site, a RecoverPoint splitter intercepts data writes destined for the Distributed Volume and passes a copy to
the RecoverPoint cluster. The RecoverPoint cluster replicates the data to a local copy and also maintains a journal volume for the copy.

You can add a third Converged System to the MetroPoint system at a later point and add a remote copy non-disruptively.

**Three-site MetroPoint topology**

A three-site MetroPoint deployment is similar to a two-site deployment but adds a remote Converged System. The remote Converged System contains a RecoverPoint cluster and a remote copy. The local copies are optional in a three-site MetroPoint topology.

The following illustration shows an Integrated Data Protection three-site MetroPoint implementation:

This illustration shows a full-meshed RecoverPoint system, which is recommended in a three-site MetroPoint. Replication to the remote site happens from either site of the VPLEX Metro. In this illustration, Site A is the active source and is replicating to the remote site. Site B is the standby source and is marking only. The active and standby sources are both replicating the same VPLEX Distributed Volume (DR1). During a source switchover, replication undergoes a short initialization phase.

**Four-site MetroPoint topology**

In a four-site MetroPoint topology, the remote site is also a VPLEX Metro site.
Note: The replica copy in a four-site topology should be a local device in a MetroPoint consistency group. Using a distributed device results in a fractured state. The replica device exists only after you enable image access, or after you fail the remote copy over to, and set it to, production. In those cases, VPLEX Metro synchronizes the fractured leg of the distributed device automatically.

The following illustration shows an Integrated Data Protection four-site MetroPoint implementation:

In the previous illustration, the distributed devices running Site A and Site B replicate to Site D, while distributed devices running at Site C and Site D replicate to Site A.
Data Protection Management

The ability to protect critical data, manage and view system health, performance and efficiency is imperative in an enterprise environment.

Dell EMC offers a variety of solutions to make managing the data protection systems easier. The following data protection management solutions may be integrated with a VxBlock 1000 managed by an AMP-VX.

- Data Protection Central
- Data Protection Search
- Data Protection Advisor

Data Protection Central

Data Protection Central is a management console for Avamar, NetWorker, Data Domain, Data Protection Search, and Data Protection Advisor.

Data Protection Central provides the following features:

- Ability to launch the following administrator consoles from a central location:
  - Avamar Management Console
  - NetWorker Management Console
  - Data Domain System Manager
  - Data Protection Search Console
  - Data Protection Advisor Console
- Supports single sign-on authentication for the following:
  - Data Protection Search 18.1 and above
  - Avamar 7.5.0-183 Hotfix HF284113_2 and above
  - NetWorker 18.1 and above
- Dashboard for information for the following Avamar and Data Domain details, including:
  - Backup Activities
  - Replication Activities
  - Capacity information for Avamar and Data Domain
  - Health
  - Alerts
- Monitoring multiple systems at the job, systems, and alert levels
- Management capabilities for Avamar systems:
  - View, add, edit, and delete policies, retentions, schedules, and datasets
  - Add clients and proxies to policies
  - Perform a backup of a policy
  - Rerun a backup or replication activity
  - View existing clients that are associated with an Avamar system
Complex search and recover operations through integration with Data Protection Search
Reporting capabilities through integration with Data Protection Advisor

Data Protection Search

Data Protection Search is a scalable index and search appliance that integrates with Avamar and NetWorker. Through scheduled collection activities, backup content of one or more Avamar or NetWorker servers is gathered, indexed, and stored within the Data Protection Search node. This allows users to perform searches across the backup environment from which the user can then preview, download, or restore the backup content.

The Data Protection Search index capability allows the following:
- Process content from multiple input sources
- Index only metadata or full content
- Leverage scalable, fault tolerant open source indexing technology

Data Protection Search allows the following:
- Search using an easy to use interface
- Perform advanced and powerful searches
- Perform cross-server, cross-platform searches
- Preview backup file content without downloading
- Download backup files locally
- Restore backups to original or alternate locations
- Apply visual filters to search results

VMware disk space size requirements

Each deployment of a search appliance is pre-configured with three virtual disks with a combined total of 180GB of disk space.
- Disk 1: 40 GB System Disk
- Disk 2: 100 GB Index Data Disk
- Disk 3: 40 GB Temporary Space Disk

To support a larger number of metadata files, it may be necessary to expand the disk space for Disk 2 and Disk 3. You must size the Search node VMs appropriately before powering on the VM for the first time.

Index Data Disk

The following table details size requirements for the Index Data Disk:

<table>
<thead>
<tr>
<th>Number of files supported</th>
<th>Index Disk Space Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 Million</td>
<td>120 GB</td>
</tr>
<tr>
<td>500 Million</td>
<td>300 GB</td>
</tr>
<tr>
<td>1 Billion</td>
<td>600 GB</td>
</tr>
<tr>
<td>2 Billion</td>
<td>1.2 TB</td>
</tr>
<tr>
<td>4 Billion</td>
<td>2.4 TB</td>
</tr>
</tbody>
</table>

When sizing the Index Disk, consider the following:
- More disk space is required when implementing full content indexing
Add additional search nodes to increase the total amount of Index Disk space

- The total disk space required can be divided by the number of Search Nodes
- If data index replication is enabled, twice as much disk space is required
- File counts are for unique files. A file that is unchanged through several backups remains a single file in the index

**Temporary Space Disk**

The following table details size requirements for the Temporary Space Disk:

<table>
<thead>
<tr>
<th>Largest backup</th>
<th>Required size for disk 3</th>
<th>Indexing both Avamar and NetWorker</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 million files</td>
<td>40 GB</td>
<td>80 GB</td>
</tr>
<tr>
<td>10 million files</td>
<td>58 GB</td>
<td>116 GB</td>
</tr>
<tr>
<td>20 million files</td>
<td>94 GB</td>
<td>188 GB</td>
</tr>
<tr>
<td>50 million files</td>
<td>202 GB</td>
<td>404 GB</td>
</tr>
<tr>
<td>100 Million files</td>
<td>382 GB</td>
<td>764 GB</td>
</tr>
<tr>
<td>200 Million files</td>
<td>742 GB</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>500 Million files</td>
<td>1.8 TB</td>
<td>3.6 TB</td>
</tr>
</tbody>
</table>

**Sizing and performance guidance for Search nodes**

When determining node sizing:

- Total number of clients to index across all backup servers
- Determine whether or not index replication is required

<table>
<thead>
<tr>
<th>Total clients</th>
<th>Estimated files</th>
<th>Estimated unique files over 30 days of backups</th>
<th>No replication</th>
<th>With replication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Estimated total space (GB)</td>
<td>Recommend ed nodes</td>
</tr>
<tr>
<td>250</td>
<td>125 Million</td>
<td>200 Million</td>
<td>112</td>
<td>1</td>
</tr>
<tr>
<td>500</td>
<td>250 Million</td>
<td>400 Million</td>
<td>224</td>
<td>2</td>
</tr>
<tr>
<td>1000</td>
<td>500 Million</td>
<td>800 Million</td>
<td>447</td>
<td>4</td>
</tr>
<tr>
<td>2500</td>
<td>1.25 Billion</td>
<td>2 Billion</td>
<td>1118</td>
<td>8</td>
</tr>
<tr>
<td>10000</td>
<td>5 Billion</td>
<td>8 Billion</td>
<td>4470</td>
<td>24</td>
</tr>
</tbody>
</table>

**Replication**

This section contains information on single and multiple search node cluster replication.

**System Index Replication**

If the Search cluster contains more than one search node, system indexes are automatically replicated.

**Data Index Replication**

If the Search cluster contains more than one search node, data index replication can be enabled manually. When data index replication is enabled, the total amount of disk space required is doubled.

In a multi-node search cluster, it is recommended that the Index Replica is set to On, otherwise failover cannot occur.
Data Protection Advisor

Data Protection Advisor is a platform for performing reporting and analytics on a data protection environment. It can provide full visibility into the health and effectiveness of the data protection strategy. This solution has the ability to monitor technologies including backup software, storage array replication, servers, databases, and virtual infrastructures.

The Data Protection Advisor reporting engine provides highly customizable reports for the following:
- Highlighting issues within the environment
- Capacity management
- Service level
- Chargeback
- Change management
- Troubleshooting

The Data Protection Advisor Predictive Analysis Engine provides the following:
- Early warnings about potential issues
- Alerts to allow for early resolution of potential issues
- A reduction in negative business impacts

The following systems will be discovered and monitored in the initial release of Data Protection Advisor:
- Avamar
- NetWorker
- Data Domain
- VPLEX
- RecoverPoint
- RecoverPoint for Virtual Machines

Other hardware or software that is listed in the Data Protection Advisor Software Compatibility Guide may be added for monitoring after the initial deployment.

Determining Data Protection Advisor datastore and application server sizing

To determine the sizing for the Data Protection Advisor datastore server and application server, the Data Protection Advisor Sizing Estimator available in Solution Builder should be utilized.

The sizing estimator utilizes the following input to size the Data Protection Advisor environment accordingly:
- Total number of backup servers to be monitored
- Total number of backup jobs per day
- Storage replication capacity
- Reports and analysis rules run per day
- Expected annual growth

The sizing estimator utilizing the above input, provides the following output for both the datastore server and application server:
- Minimum storage requirement
- Minimum CPU requirement
Minimum memory requirement

The sizing estimator is not an exact science, and may only provide a general recommendation based on assumptions and expectations. Therefore, best practice is to virtualize each of these components to allow for the flexibility to expand the systems resources as necessary.

The Data Protection datastore and application servers are installed on Microsoft Windows Server virtual machines, which are hosted on the AMP-VX.

The memory, CPU, virtual disk, and NIC of each of the virtual machines will have the following resource settings applied:

<table>
<thead>
<tr>
<th>VM</th>
<th>CPU Shares</th>
<th>Memory Shares</th>
<th>Memory Reservation</th>
<th>Reserve all guest memory (All locked)</th>
<th>Virtual Disk Format</th>
<th>vNIC Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Advisor</td>
<td>High</td>
<td>High</td>
<td>Maximum</td>
<td>Yes</td>
<td>Thick Provision Eager Zeroed</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Datastore VM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection Advisor</td>
<td>High</td>
<td>High</td>
<td>Maximum</td>
<td>Yes</td>
<td>Thick Provision Eager Zeroed</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Application VM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Backup of the Data Protection Advisor datastore

This section describes important information for safely backing up the Data Protection datastore.

It is highly recommended that the datastore is exported to a flat file on a regular schedule. This flat file should be backed up in the traditional method with a backup product such as Avamar or NetWorker. This is the only supported method for backing up the Data Protection Advisor datastore.

⚠️ CAUTION VMware snapshots, and replication solutions such as RecoverPoint for Virtual Machines or RecoverPoint Classic, should not be relied upon for the datastore backup. The only supported method of backup and recovery is the export and backup of the datastore flat file.

Data Protection Advisor Agents

This topic provides information about Data Protection Advisor Agents.

The Data Protection Advisor (DPA) agents perform data collection from objects monitored by Data Protection Advisor. When possible, it is highly recommended to install the DPA agent directly on the object being monitored such as NetWorker. For objects such as Avamar and Data Domain, a DPA proxy agent should be deployed on a designated host, other than the datastore and application servers, for data collection services.

When monitoring objects at remote sites, DPA proxy agents should be deployed at each site for collection duties. The agents communicate with monitored objects typically using CLI, SNMP, SSH, or direct database connection, and may be sensitive to latency which may cause collection of data to fail.

There is no limit to the number of objects that can be monitored from a single DPA agent, and no limit on the number of DPA agents that may be deployed. There are also no additional licensing costs for the DPA agents themselves, but there may be additional licensing costs for the operating systems on which the agents operate.
# Data Protection reference materials

Use these links to access additional references used through the document.

<table>
<thead>
<tr>
<th>Document</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Domain Boost for Oracle Recovery Manager (RMAN)</td>
<td><a href="http://www.emc.com/collateral/hardware/white-papers/h10683-dd-boost-oracle-rman-tech-review-wp.pdf">www.emc.com/collateral/hardware/white-papers/h10683-dd-boost-oracle-rman-tech-review-wp.pdf</a></td>
</tr>
<tr>
<td>RecoverPoint Release Notes</td>
<td>support.emc.com/docu85467_RecoverPoint_5.1_Release_Notes.pdf</td>
</tr>
<tr>
<td>RecoverPoint with VMAX3/AF Technical Notes</td>
<td>support.emc.com/docu85444_RecoverPoint_with_VMAX3/AF_Technical_Notes.pdf</td>
</tr>
<tr>
<td>MetroPoint Continuous Availability with Comprehensive Data Protection</td>
<td><a href="https://support.emc.com/docu55669_White-Paper:-EMC-MetroPoint-Continuous-Availability-with-Comprehensive-Data-Protection.pdf">https://support.emc.com/docu55669_White-Paper:-EMC-MetroPoint-Continuous-Availability-with-Comprehensive-Data-Protection.pdf</a></td>
</tr>
</tbody>
</table>

For more information on Dell EMC products, refer to [Dell EMC support](https://support.dell.com/).

To calculate power consumption and heat dissipation for a specific storage configuration, refer to the power calculator at [powercalculator.emc.com/PC3/](https://powercalculator.emc.com/PC3/).