Abstract
This Solution Guide describes the data protection operations and services provided as a modular add-on to the EMC® Enterprise Hybrid Cloud™ 2.5.1, Federation Software-Defined Data Center Edition. The document introduces the main features and functionality of the solution and the solution architecture.

December 2014
**Chapter 1: Executive Summary**

Document purpose ................................................................. 10
Audience ................................................................................. 10
Solution purpose ..................................................................... 10
Business challenge ................................................................. 11
Technology solution ............................................................... 12

**Chapter 2: EMC Enterprise Hybrid Solution Overview**

Introduction ............................................................................... 16
EMC Enterprise Hybrid Cloud features and functionality ............ 17
  Automation and self-service provisioning .................................. 17
  Multitenancy and secure separation .......................................... 18
  Workload-optimized storage ..................................................... 18
  Elasticity and service assurance ............................................... 18
  Operational monitoring and management ................................. 19
  Metering and chargeback ....................................................... 19
  Modular add-on components ................................................... 20

**Chapter 3: Protection Architecture and Design**

Overview .................................................................................. 24
  Key components for data protection ........................................... 24
  Avamar backup and recovery services ....................................... 25
  Component integration ............................................................. 28
Solution architecture ................................................................. 29
  Network design ..................................................................... 32
  Backup service levels ............................................................ 35
Software resources .................................................................... 37
  EMC Enterprise Hybrid Cloud software resources .................. 37
  EMC sizing .......................................................................... 37

**Chapter 4: Data Protection Services**

Hybrid cloud self-service .......................................................... 40
Overview .................................................................................. 40
Federation Software-Defined Data Center self-service portal ....... 40
Contents

Backup and recovery services.................................................................41
Managing backup service levels .........................................................41
User-driven data protection ..................................................................42
Use cases ...............................................................................................44
Use case 1: Create backup service level.................................................44
Use case 2: Deploy virtual machine with automatic data protection ....54
Use case 3: Request on-demand backup ..............................................56
Use case 4: Request list of backups available for a virtual machine ...57
Use case 5: Request an on-demand restore ........................................58
Use case 6: Decommission virtual machine ........................................59
Use case 7: Request cost and usage reports for a virtual machine ......61
Use case 8: Request backup report for a virtual machine ..................62
Use case 9: Delete a backup service level ............................................64
Summary ...............................................................................................65

Chapter 5  Monitoring and Reporting .................................................67
Overview ...............................................................................................68
Monitoring and reporting .................................................................68
Centralized log management .............................................................71

Chapter 6  Resource Sizing Guide .......................................................77
Data protection sizing guide .............................................................78

Chapter 7  Conclusion ........................................................................81
Conclusion .............................................................................................82
Figures

Figure 1. Hybrid cloud solution stack .................................................. 11
Figure 2. EMC Enterprise Hybrid Cloud key components .................... 16
Figure 3. EMC Enterprise Hybrid Cloud self-service portal .................. 18
Figure 4. EMC ViPR Analytics with VMware vCenter Operations Manager 19
Figure 5. IT Business Management Suite overview dashboard for hybrid cloud 20
Figure 6. Avamar view of virtual machine inventory and protection status 26
Figure 7. Avamar virtual machine image-level backup using CBT ............ 26
Figure 8. Avamar virtual machine image-level restore using CBT .......... 27
Figure 9. Run a virtual machine from Data Domain backup with Instant Access 27
Figure 10. Connection among backup components ................................ 28
Figure 11. Solution architecture .............................................................. 29
Figure 12. Data protection for Federation Software-Defined Data Center components .......................................................... 31
Figure 13. Backup network architecture for Federation Software-Defined Data Center ........................................................................... 34
Figure 14. vSphere Client views of backup service-level folders in vCenter 36
Figure 15. Data protection services for cloud infrastructure administrators 36
Figure 16. Self-service portal and service catalog overview .................. 40
Figure 17. vCloud Automation Center service catalog ............................ 41
Figure 18. User-defined automatic data protection for virtual machines .. 42
Figure 19. On-demand data protection actions for virtual machines ...... 43
Figure 20. On-demand restore functionality in vCloud Automation Center user portal .................................................................................. 43
Figure 21. Create Backup Service Level from vCloud Automation Center cloud administrator service catalog .................................................. 45
Figure 22. Create Backup Service Level: Service-level description ......... 45
Figure 23. Create Backup Service Level: Name and backup target .......... 46
Figure 24. Create Backup Service Level: Daily backup schedule .......... 46
Figure 25. Create Backup Service Level: Specify retention period .......... 47
Figure 26. Create Backup Service Level: Define a custom retention period 48
Figure 27. Create Backup Service Level workflow: vCenter Orchestrator workflow detail ................................................................................. 49
Figure 28. New backup service level (virtual machine folder) .............. 49
Figure 29. New client in Avamar system ............................................... 50
Figure 30. New Avamar dataset that defines what to back up .................. 50
Figure 31. New Avamar schedule for the new backup service level ...... 51
Figure 32. New Avamar retention policy for the new backup service level 51
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td>Avamar group created and enabled</td>
</tr>
<tr>
<td>34.</td>
<td>Dataset showing the data type to back up: Virtual disks</td>
</tr>
<tr>
<td>35.</td>
<td>Schedule showing the backup interval and time</td>
</tr>
<tr>
<td>36.</td>
<td>Retention policy showing the retention period</td>
</tr>
<tr>
<td>37.</td>
<td>List of proxies for the group</td>
</tr>
<tr>
<td>38.</td>
<td>Create new request in vCloud Automation Center self-service portal</td>
</tr>
<tr>
<td>39.</td>
<td>Select a backup service level for the virtual machine</td>
</tr>
<tr>
<td>40.</td>
<td>Select on-demand backup for the virtual machine</td>
</tr>
<tr>
<td>41.</td>
<td>On-demand backup workflow in vCenter Orchestrator</td>
</tr>
<tr>
<td>42.</td>
<td>Request list of all available backups of a virtual machine</td>
</tr>
<tr>
<td>43.</td>
<td>Workflow in vCenter Orchestrator</td>
</tr>
<tr>
<td>44.</td>
<td>Select on-demand restore of a virtual machine</td>
</tr>
<tr>
<td>45.</td>
<td>On Demand Restore request wizard: Enter request information</td>
</tr>
<tr>
<td>46.</td>
<td>On Demand Restore request wizard: Select backup point-in-time to restore</td>
</tr>
<tr>
<td>47.</td>
<td>Destroy a virtual machine</td>
</tr>
<tr>
<td>48.</td>
<td>vCenter Orchestrator workflow RetireVM used to decommission a virtual machine</td>
</tr>
<tr>
<td>49.</td>
<td>Request virtual machine cost details from the self-service portal</td>
</tr>
<tr>
<td>50.</td>
<td>Email report to cloud user with virtual machine cost summary</td>
</tr>
<tr>
<td>51.</td>
<td>Request virtual machine backup status from the self-service portal</td>
</tr>
<tr>
<td>52.</td>
<td>Backup status report emailed to cloud user on request</td>
</tr>
<tr>
<td>53.</td>
<td>Delete Backup Service Level request in self-service portal</td>
</tr>
<tr>
<td>54.</td>
<td>Select the service level to be deleted</td>
</tr>
<tr>
<td>55.</td>
<td>EMC Avamar Administrator console: Dashboard</td>
</tr>
<tr>
<td>56.</td>
<td>Examination of Avamar appliance through Avamar Administrator console</td>
</tr>
<tr>
<td>57.</td>
<td>Data Protection Advisor: Analysis Policies</td>
</tr>
<tr>
<td>58.</td>
<td>On-demand view of active and failed EMC Avamar clients</td>
</tr>
<tr>
<td>59.</td>
<td>EMC Data Protection Advisor report wizard: Select Report Template</td>
</tr>
<tr>
<td>60.</td>
<td>Centralized logging of hybrid cloud components with Log Insight</td>
</tr>
<tr>
<td>61.</td>
<td>Customized hybrid cloud dashboard using multiple content packs</td>
</tr>
<tr>
<td>62.</td>
<td>Sample of the dashboard view: Avamar content pack</td>
</tr>
<tr>
<td>63.</td>
<td>Create new profile for Log Insight</td>
</tr>
<tr>
<td>64.</td>
<td>Configure syslog server information for the Log Insight profile</td>
</tr>
<tr>
<td>65.</td>
<td>Select event codes to be sent to Log Insight</td>
</tr>
</tbody>
</table>
Tables

Table 1. Cloud management platform resource clusters for Federation Software-Defined Data Center .......................................................... 30
Table 2. Edge network connectivity ........................................................................ 33
Table 3. Suggested backup schedule and retention policies for backup service levels ........................................................................ 35
This chapter presents the following topics:

- **Document purpose** ................................................................. 10
- **Audience** .................................................................................. 10
- **Solution purpose** ...................................................................... 10
- **Business challenge** ................................................................. 11
- **Technology solution** ............................................................... 12
Chapter 1: Executive Summary

Document purpose

The EMC Federation of companies, EMC, VMware, Pivotal, and RSA, work together to research, develop, and validate leading-edge solutions to deliver superior, integrated solution stacks.

This document describes the data protection operations and services provided as a modular add-on to the EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition solution. The document introduces the main features and functionality of the EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition solution and the solution architecture. This document is a companion to the *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition: Foundation Infrastructure Solution Guide*, which is an enablement reference to begin planning and design for data protection in your hybrid cloud.

The following documents provide information about how to implement other specific capabilities or enable specific use cases with the EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition solution:

- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition: Foundation Infrastructure Reference Architecture*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition: Foundation Infrastructure Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition: Data Protection Disaster Recovery Solution Guide*
- *EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition: Data Protection Continuous Availability Solution Guide*

Audience

This document is intended for executives, managers, architects, cloud administrators, and technical administrators of IT environments who want to implement data protection for their hybrid cloud infrastructure-as-a-service (IaaS) platform. Readers should be familiar with the VMware vCloud Suite®, storage technologies, and general IT functions and requirements, and how a hybrid cloud architecture accommodates these technologies and requirements.

Solution purpose

This EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition solution enables EMC Enterprise Hybrid Cloud customers to build an enterprise-class, scalable, multitenant infrastructure that enables:

- Complete management of the infrastructure service lifecycle
On-demand access to and control of network bandwidth, servers, storage, and security

Provisioning, monitoring, protection, and management of the infrastructure services by line-of-business end users, without IT administrator involvement

Maximum asset utilization

Access to application services from a single platform for both business-critical and next-generation cloud applications

This solution provides reference architecture and best practices necessary to integrate data protection functionality with a hybrid cloud, as shown in Figure 1.

---

**Business challenge**

Business leaders typically demand that their organization address the following fundamental challenges:

- Providing shareholder value by increasing revenues
- Improving competitiveness by driving business agility
- Increasing investment by lowering operational costs

While many organizations have successfully introduced virtualization as a core technology within their data center, the benefits of virtualization have largely been restricted to the IT infrastructure owners. End users and business units within customer organizations have not experienced many of the benefits of virtualization, such as increased agility, mobility, and control.
Transforming from the traditional IT model to an IaaS model involves overcoming the challenges of legacy infrastructure and processes, such as:

- Inefficiency and inflexibility
- Slow, reactive responses to customer requests
- Inadequate visibility of the requested infrastructure cost
- Limited choice of availability and protection services

The difficulty in overcoming these challenges has given rise to public cloud providers who have built technology and business models specifically catering to the requirements of end-user agility and control. Many organizations are under pressure to provide the same service levels within the secure and compliant confines of the on-premises data center. As a result, IT departments need to create alternatives to public cloud services that are cost effective and that do not compromise enterprise features such as data protection, disaster recovery (DR), and guaranteed service levels.

As IT organizations implement a hybrid cloud, they must consider the following factors:

- The infrastructure must be quick to deploy so that business value can be recognized quickly.
- The infrastructure and operations must be designed to reduce costs through higher utilization and higher staff productivity.
- Risk of downtime must be controlled through disciplined change control and careful management of component compatibility.
- Support agreements must be established for all elements of the solution.

**Technology solution**

This solution integrates the best of EMC and VMware products and services, and empowers IT organizations to accelerate implementation and adoption of the hybrid cloud while still enabling customer choice for the compute and networking infrastructure within the data center. The solution caters both to customers who want to further use their existing infrastructure and to those who want to build new infrastructures dedicated to the hybrid cloud.

This solution takes advantage of the strong integration between EMC technologies and the VMware vCloud Suite. The solution, developed by EMC and VMware product and services teams, includes using EMC scalable storage arrays and integrated EMC and VMware monitoring and data protection suites to provide the foundation for enabling IaaS.

The key solution components include:

- EMC ViPR® software-defined storage platform
- EMC XtremIO and/or VNX® and/or EMC Symmetrix® VMAX® storage platforms
- EMC Avamar® and/or EMC Data Domain® backup and recovery solutions
- EMC and VMware integrated workflows
- VMware vCloud Suite
- VMware NSX™ software-defined networking
- VMware vSphere® virtualization platform
This chapter presents the following topics:

Introduction .............................................................................................................. 16

EMC Enterprise Hybrid Cloud features and functionality ..................................... 17
**Introduction**

The EMC Enterprise Hybrid Cloud solution is an engineered solution that offers a simplified approach to IT functionality to IT organizations, developers, end users, and line-of-business owners. In addition to delivering baseline infrastructure as a service (IaaS), built on software-defined data center architecture, the EMC Enterprise Hybrid Cloud delivers feature-rich capabilities to expand from IaaS to business-enabling IT as a service (ITaaS). Backup as a service (BaaS) and disaster recovery as a service (DRaaS) are now policies that can be enabled with just a few clicks. End users and developers can quickly access a marketplace of resources for Microsoft, Oracle, SAP, and EMC Pivotal applications, and can add third-party packages as required. Resources can be deployed on private cloud or EMC-powered public cloud services, including VMware vCloud® Air™.

The EMC Enterprise Hybrid Cloud solution uses the best of EMC and VMware products and services, and takes advantage of the strong integration between EMC and VMware technologies to provide the foundation for enabling IaaS on new and existing infrastructure for the hybrid cloud.

Figure 2 shows the key components of the EMC Enterprise Hybrid Cloud solution.

![Figure 2. EMC Enterprise Hybrid Cloud key components](image)

For detailed information, refer to *EMC Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition: Foundation Infrastructure Solution Guide*. For an overview of EMC Enterprise Hybrid Cloud modular add-on solutions, which provide functionality such as data protection, continuous availability, and application services, refer to Modular add-on components. For detailed information on the add-on solutions, refer to the individual Solution Guides for those solutions.
EMC Enterprise Hybrid Cloud features and functionality

The EMC Enterprise Hybrid Cloud solution incorporates the following features and functionality:

- Automation and self-service provisioning
- Multitenancy and secure separation
- Data protection
- Workload-optimized storage
- Elasticity and service assurance
- Monitoring
- Metering and chargeback

The solution provides self-service provisioning of automated cloud services to both users and infrastructure administrators. It uses VMware vCloud® Automation Center™, integrated with EMC ViPR software-defined storage and VMware vCloud® Networking and Security™ or VMware NSX, to provide the compute, storage, network, and security virtualization platforms for the software-defined data center.

Cloud users can request and manage applications and compute resources within established operational policies. This can reduce IT service delivery times from days or weeks to minutes. Automation and self-service provisioning features include:

- **Self-service catalog**—Provides a cross-cloud storefront that delivers a catalog of custom-defined services for provisioning applications based on business and IT policies, as shown in Figure 3
- **Role-based entitlements**—Ensures that the self-service portal presents only the virtual machine, application, or service blueprints appropriate to a user’s role within the business
- **Resource reservations**—Allocates resources for use by a specific group and ensures that access is limited to that group
- **Service levels**—Defines the amount and types of resources that a particular service can receive during initial provisioning or as part of configuration changes
- **Blueprints**—Contains the build specifications and automation policies that specify the process for building or reconfiguring compute resources
Chapter 2: EMC Enterprise Hybrid Solution Overview

Figure 3. EMC Enterprise Hybrid Cloud self-service portal

Multitenancy and secure separation

The solution provides the ability to enforce physical and virtual separation for multitenancy, as strong as the administrator requires. This separation can encompass network, compute, and storage resources to ensure appropriate security and performance for each tenant.

The solution supports secure multitenancy through role-based access control (RBAC) in vCloud Automation Center, which enables the roles to be mapped to Microsoft Active Directory groups. The self-service portal shows only the appropriate views, functions, and operations to cloud users, based on their role within the business.

Workload-optimized storage

The solution enables customers to take advantage of the proven benefits of EMC storage in a hybrid cloud environment. Using ViPR storage services with EMC VNX, VMAX, and XtremIO, the solution provides software-defined, policy-based management of block- and file-based virtual storage. ViPR abstracts the storage configuration and presents it as a single storage control point, enabling cloud administrators to access all heterogeneous storage resources within a data center as if the resources were a single large array.

Elasticity and service assurance

The solution uses the capabilities of vCloud Automation Center and various EMC tools to provide the visibility and alerting required to proactively ensure service levels in virtual and cloud environments. Infrastructure administrators manage storage, compute, and network resources within resource pools, while cloud users manage those resources at the virtual machine level. Cloud users can select from a range of service levels for compute, storage, and data protection for their applications and can expand the resources of their virtual machines on demand to achieve the service levels required by their application workloads.
Chapter 2: EMC Enterprise Hybrid Solution Overview

Operational monitoring and management

The solution features automated monitoring and management capabilities that provide IT administrators with a comprehensive view of the cloud environment to enable intelligent decision making for resource provisioning and allocation. These automated capabilities are based on a combination of EMC ViPR Storage Resource Management (SRM), VMware vCenter® Log Insight™, and VMware vCenter Operations Manager™, and use EMC plug-ins for ViPR, VNX, VMAX, XtremIO and Avamar, part of EMC Storage Analytics (ESA), to provide extensive additional storage detail.

Cloud administrators can use ViPR SRM to understand and manage the impact that storage has on their applications and to view their storage topologies from application to disk, as shown in Figure 4.

![Figure 4. EMC ViPR Analytics with VMware vCenter Operations Manager](image)

Capacity analytics and what-if scenarios in vCenter Operations Manager identify over-provisioned resources so they can be right-sized for the most efficient use of virtualized resources. In addition, Log Insight provides the ability to centralize and aggregate system and application logs. Each system in the solution can be configured to forward logs to Log Insight for event analytics and reporting.

Metering and chargeback

The solution uses VMware IT Business Management Suite™ to provide cloud administrators with comprehensive metering and cost information across all business groups in the enterprise. IT Business Management Suite is integrated into the cloud administrator’s self-service portal and presents a dashboard overview of the hybrid cloud infrastructure, as shown in Figure 5.
Modular add-on components

The EMC Enterprise Hybrid Cloud solution provides modular add-on components for the following services:

- **Application services**
  This add-on solution uses vCloud Automation Center Application Services to optimize application deployment and release management through logical application blueprints in vCloud Automation Center. Users can quickly and easily deploy blueprints for applications and databases such as Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint, Oracle, and SAP.

- **Data protection: Backup**
  EMC Avamar and EMC Data Domain systems provide a backup infrastructure that offers features such as deduplication, compression, and VMware integration. By using VMware vCenter™ Orchestrator™ workflows customized by EMC, administrators can quickly and easily set up multilayer data protection policies that users can assign when they provision their virtual machines.

- **Data protection: Continuous availability**
  A combination of EMC VPLEX virtual storage and VMware vSphere® High Availability (HA) provide the ability to join information across multiple data centers over synchronous distances. With virtual storage and virtual servers working together over distance, the infrastructure can transparently provide
load balancing, real-time remote data access, and improved application protection. Backup operations continue to operate.

- **Data protection: Disaster recovery**
  This add-on solution enables cloud administrators to select DR protection for their applications and virtual machines when they provision their hybrid cloud environment. ViPR automatically places these systems on storage that is protected remotely by EMC RecoverPoint. VMware vCenter™ Site Recovery Manager™ automates the recovery of all virtual storage and virtual machines.

- **Platform as a service**
  The EMC Enterprise Hybrid Cloud solution provides an elastic and scalable IaaS foundation for platform-as-a-service (PaaS) and software-as-a-service (SaaS). Pivotal CF provides a highly available platform that enables application owners to easily deliver and manage applications over the application lifecycle. The EMC Enterprise Hybrid Cloud solution service offerings enable PaaS administrators to easily provision compute and storage resources on demand to support scalability and growth in their Pivotal CF enterprise, PaaS environments.

- **Public cloud services**
  The EMC Enterprise Hybrid Cloud solution enables IT organizations to broker public cloud services. The public cloud solution has been validated with vCloud Air as a public cloud option that users and administrators can access directly from the solution's self-service portal. End users can provision virtual machines while IT administrators can use VMware vCloud Connector to perform virtual machine migration (offline) to vCloud Air from the on-premises component of their hybrid cloud.
Chapter 3 Protection Architecture and Design

This chapter presents the following topics:

- **Overview** ................................................................. 24
- **Avamar backup and recovery services** ................................ 25
- **Solution architecture** ...................................................... 29
- **Software resources** .......................................................... 37
Overview

This modular add-on for data protection provides local backup and recovery services in the EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center solution. This add-on leverages the features and functionality of EMC Avamar, EMC Data Domain, and EMC Data Protection Advisor™ software. Backup and recovery of a multitenant hybrid cloud is a complicated endeavor in which many factors must be considered, including:

- Backup type and frequency
- Impact and interaction with replication
- Recoverability methods and requirements
- Retention periods
- Implementation in a vSphere HA/DR-enabled environment
- Automation workflows
- Interface methods (workflows, APIs, GUI, CLI, scripts, and so on)

vCenter Orchestrator, which is central to all of the customizations and operations used in this solution, manages operations across several EMC and VMware products, including:

- vCloud Automation Center
- VMware vCenter
- EMC Avamar and Data Protection Advisor

This solution focuses on the management and automation aspects of a hybrid cloud, and the data protection implementation that is described represents one possible way of many for meeting the requirements. This solution uses a subset of the advanced capabilities of the Avamar system. EMC strongly recommends that you engage an Avamar product specialist to design, size, and implement a data protection solution that is specific for your environment and business needs.

Key components for data protection

**EMC Avamar backup and recovery**

EMC Avamar backup and recovery is a complete software and hardware solution that is fast and efficient. Equipped with integrated variable-length deduplication technology, Avamar backup and recovery software provides integrated source and global data deduplication that facilitates fast, daily full backups for hybrid cloud environments.

**EMC Data Domain system**

With Avamar backup and recovery, you can choose to direct backups to an EMC Data Domain system instead of to the Avamar server. Data Domain deduplication storage systems deduplicate data inline, so that it lands already deduplicated on disk and requires less disk space than the original dataset. With the Data Domain...
system, you can retain backup and archived data onsite longer to enable quick and reliable data restores from disk.

**EMC Data Protection Advisor software**

With EMC Data Protection Advisor software, you can automate and centralize the collection and analysis of all data across backup applications, replication technologies, the virtual environment, and supporting infrastructure. This provides a single, comprehensive view of your data protection environment and activities. Data Protection Advisor provides a REST API that is used to integrate with vCenter Orchestrator to provide on-demand reporting of backup statistics and performance.

**Data protection workflows for vCenter Orchestrator**

The EMC Federation of companies has created data protection workflows with vCenter Orchestrator to automate Avamar and Data Domain protection of virtual machines. These workflows are added to the vCloud Automation Center virtual machine provisioning blueprints so that users can easily set up protection at provisioning time. In addition, workflows can be used to enable simple or point-in-time restores for a specific virtual machine.

Infrastructure administrators can also use the data protection workflows for complete protection policy setup on Avamar and vCenter systems. This facilitates quick and easy deployment of the infrastructure required to support all end-user protection needs.

**Avamar backup and recovery services**

The underlying technology and efficiencies that support and enable the backup and restore operations in this solution are completely hidden from the cloud users.

This backup solution does the following:

- Abstracts and simplifies backup and restore operations for cloud users
- Uses VMware Storage APIs for Data Protection, which provides Changed Block Tracking (CBT) 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

The Avamar solution fully integrates with the vCenter management utility to gain information that simplifies the management of backup and recovery activities. Integration through the vCenter API enables the Avamar Administrator console to routinely query a vCenter server, which was imported into the Avamar environment, to provide key data protection information on its virtual machines.

The information gathered by Avamar from vCenter, as shown in Figure 6, includes details such as the current protection status of each virtual machine in the vCenter inventory.
Chapter 3: Protection Architecture and Design

With image-based backup functionality, the Avamar system integrates with the VMware vSphere® Storage APIs for Array Integration and Data Protection within the vSphere server. This feature set offloads the backup processing overhead from the client to a backup proxy server running as a virtual machine. To perform an image-level backup, the proxy server communicates with the vCenter server to mount a snapshot of a virtual machine’s Virtual Machine Disk (VMDK) files. This method provides deduplication at the file level and at the VMDK level.

To maximize efficiencies in the backup process, Avamar uses the power of the CBT feature as part of the vSphere Storage APIs for Data Protection. CBT enables the virtual machine image proxy to query the vSphere environment for an intelligent list of which blocks have changed on a specific virtual machine as of its last backup, as shown in Figure 7. With this setup, Avamar only scans and processes the blocks that are included in the changed-block list obtained from CBT in vSphere.

The restoration of virtual machines uses the same CBT functionality to enable more efficient restores, as shown in Figure 8. When a virtual machine recovery is run, the Avamar system queries the vCenter server by using CBT to determine which blocks have changed on the VMDK files of the virtual machine as of the last backup, and then only replaces those particular blocks within the VMDK files. In situations where a large amount of block changes have occurred after the last backup, Avamar automatically evaluates the projected workload between a full image restore and a CBT-based restore, and uses the method that provides the fastest restore time.
Avamar integration with the vCenter database structure provides the flexibility of different virtual machine recovery options. Using the image-level backup of the VMDK file, the Avamar system provides the ability to run a bare-metal restore to replace a virtual machine instance, or to create a new, separate instance of the virtual machine within vCenter if required. The recovery process manages all of the required operations in vCenter. The user only needs to turn on the virtual machine again.

The flexibility of recovery is further extended with Data Domain systems, as shown in Figure 9, where a virtual machine can be mounted and run directly from the backup image, which enables critical time access where required.

**Figure 8.** Avamar virtual machine image-level restore using CBT

**Figure 9.** Run a virtual machine from Data Domain backup with Instant Access

**Note:** Instant Access restore is a manual process and is limited to one restore at a time.

The sequence of events that occurs during the instant access operation is as follows:

1. The Avamar system manages the creation of an NFS datastore using an NFS export of the virtual machine backup image stored on the Data Domain system.
2. The Avamar system interfaces with vCenter to create a new virtual machine entry in the vCenter virtual machine database, along with the relevant virtual machine state and configuration files being recovered.

3. The virtual machine is ready to turn on.

While the virtual machine is running from the backup target, all new I/O is written to a separately tracked virtual machine snapshot file. To complete the recovery of the virtual machine from the temporary NFS datastore export to a production VMFS datastore, use a standard VMware vSphere Storage vMotion® operation.

vCenter Orchestrator is central to this backup and recovery solution for the hybrid cloud, communicating with and managing operations across a range of EMC and VMware components.

As shown in Figure 10, some of the primary component communications and interactions involved in this backup solution are as follows:

- vCloud Automation Center is configured with vCenter as its vSphere endpoint using Lightweight Directory Access Protocol (LDAP) authentication.
- vCenter Orchestrator uses a Secure Shell (SSH) plug-in to run Avamar commands in a particular sequence for all Avamar tasks, such as adding new Avamar clients (service levels in this case), checking the backup/restore task, performing on-demand backup and restores, and so on.
- vCenter Orchestrator uses a vCenter plug-in to create or delete the vCenter virtual machine folders (service levels in this case). The vCenter that is used for all the service levels is added to the Avamar system as a vCenter client.
- The Avamar system is configured as the backup endpoint in Data Protection Advisor, which enables vCenter Orchestrator to gather virtual machine billing and usage information from Data Protection Advisor using REST API.

Component integration

Figure 10. Connection among backup components
vCenter Orchestrator uses the vCenter API to create the required service-level folder on the vCenter, and runs several Avamar MCCLI commands using the SSH plug-in to create Avamar components for the schedule and retention policy of the new service level.

Custom automations can be designed based on vCenter Orchestrator default workflows and run from the workflow engine. Many third-party plug-ins, or plug-ins for standard protocols such as RESTful API, SQL, SSH, are also available.

Solution architecture

This section describes the foundation architecture protected in this hybrid cloud solution. Figure 11 shows the overall architecture of the solution.
A cloud management platform supports the entire management infrastructure for this solution. This platform includes several pods, consisting of VMware ESXi™ clusters that perform solution-specific functions and are used to provide high availability and load balancing as appropriate.

Table 1 describes the sets of resources of the foundation architecture that are required to deploy this hybrid cloud solution.

### Table 1. Cloud management platform resource clusters for Federation Software-Defined Data Center

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Pod</td>
<td>The Core Pod contains the base set of resources required to deploy subsequent cloud automation components such as vCloud Automation Center.</td>
</tr>
<tr>
<td>Network Edge Infrastructure (NEI) Pod</td>
<td>The NEI Pod is used to host all of the VMware NSX Controller™ and VMware NSX Edge™ components of the virtualized network that are responsible for North-South communications.</td>
</tr>
<tr>
<td>Automation Pod</td>
<td>The Automation Pod hosts all of the virtual machines used for automating and managing the cloud infrastructure, with the exception of the Core Pod components, which must exist before the creation of the Automation Pod.</td>
</tr>
<tr>
<td>Tenant resource pods</td>
<td>The tenant resource pods are configured and assigned in vCloud Automation Center as available resources that will host all machines deployed by the various business groups in the hybrid cloud environment.</td>
</tr>
</tbody>
</table>

**Data protection for tenant resource machines**

The vCloud Automation Center user portal is customized to present several service levels of backup to the cloud user, offering both Avamar and Data Domain systems as backup targets.

Higher service levels provide more frequent backups and longer-term retention policies compared to the lower-level service tiers. During the provisioning process for virtual machines in the vCloud Automation Center user portal, the cloud user is presented with a list of these backup service levels, from which one must be selected. All virtual machines are automatically backed up in accordance with the selected backup service level.

On-demand backup and on-demand restore operations can also be run on a virtual machine from either of the vCloud Automation Center user portals by a cloud user or administrator or by the backup administrator using the Avamar Administrator console. Virtual machines using the Data Domain system as their backup target can use the Instant Access feature that enables virtual machine restore in seconds in a production environment.

**Note:** Instant Access restore is a manual process and is limited to one restore at a time.
For usage and billing information, the vCloud Automation Center user portal is further customized to provide a cloud user or cloud administrator with the ability to gather virtual machine backup details using integration with EMC Data Protection Advisor.

**Data protection for cloud management platform**

While the virtual machines within the tenant resource pods are automatically protected at provisioning time with customizations between vCloud Automation Center and Avamar, virtual machines on the cloud management platform are manually protected in the more traditional manner, using the Avamar Administrator console.

To protect the vCenter server located in the infrastructure cluster, use Avamar guest-level backup with the client agent with the Avamar plug-in for SQL Server. The SQL Server instance in the infrastructure cluster also hosts the databases to support vCloud Automation Center IaaS on the cloud management platform. Avamar guest-level backup can co-exist with image-level backup of the same virtual machine.

Figure 12 illustrates data protection services for all management and tenant components of this solution.

**Figure 12.** Data protection for Federation Software-Defined Data Center components

**Avamar proxy server configuration**

At least one Avamar proxy server must be available to each vSphere cluster managed by vCenter. In this solution, an Avamar proxy server is created and placed
on each ESXi server in each vSphere cluster, using vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to ensure availability across all ESXi servers.

The backup or Avamar administrator can configure Avamar proxy servers to be dedicated to specific backup service levels if required. By default, the Avamar proxy servers are available to service operations of all backup service levels and are automatically selected at the time of backup.

When new storage devices are created and assigned to a vSphere cluster, the Avamar or backup administrator must manually add them to the list of datastores protected by the Avamar proxy servers.

**Solution connectivity**

This solution uses the following networks:

- **Fibre Channel and NFS**—Connects all of the block and file storage devices to the respective server hardware
- **Backup network**—Transports all data between the Avamar proxy server in the production cluster and the Avamar grid
- **Infrastructure network**—Connects all the hardware components of the solution
- **Management network**—Connects all the cloud management virtual machines
- **Business group networks**—Serve as dedicated networks for each business group

**Network design**

A dedicated backup network is configured and used for all backup traffic in this solution.

The network and security architecture is designed for VMware NSX™ for vSphere®. The network services showcased in this solution with vCloud Automation Center are supported with NSX for vSphere.

To support infrastructure operations, we configured networking on each ESXi host throughout the environment to enable connectivity to the backup, NFS, and vMotion networks. To enable this, we configured a VMkernel for NFS and vMotion on each ESXi host, and we created a port group for the Avamar proxy virtual machines on the cloud management VMware vSphere® Distributed Switch™ (VDS) to complete the network connectivity.

Table 2 lists the edge networks configured to support this solution.
Table 2.  Edge network connectivity

<table>
<thead>
<tr>
<th>Edge network</th>
<th>Configured component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi management</td>
<td>ESXi host</td>
<td>Management of ESXi hosts</td>
</tr>
<tr>
<td>EMC Enterprise Hybrid Cloud 2.5.1, Federation</td>
<td>Management VDS</td>
<td>Hosting of EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Automation and Core Pod virtual machines</td>
</tr>
<tr>
<td>Software-Defined Data Center automation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup infrastructure</td>
<td>Management or Production VDS</td>
<td>Connectivity between Avamar server and proxy appliances</td>
</tr>
<tr>
<td>vMotion</td>
<td>ESXi host</td>
<td>Migration of workloads</td>
</tr>
<tr>
<td>NFS</td>
<td>ESXi host</td>
<td>File storage</td>
</tr>
</tbody>
</table>

The high levels of deduplication and compression provided by the Avamar solution contribute to minimal data being sent across the LAN. However, in the interest of best practice design for performance, availability, and security, this environment contains a dedicated network, separate from production networks, within which the Avamar server nodes and proxy virtual servers reside.

All Avamar proxy servers are configured with an isolated Private VLAN ID, so they can communicate with only the Avamar server nodes and no other system on the backup network. The backup infrastructure resources are further protected by the isolation of the network from other Layer 3 networks. Where communications must be allowed to enable the solution to function correctly—for example, in the management of the Avamar system by backup administrators and control communications with Data Protection Advisor, vCloud Automation Center, vCenter Orchestrator, and vCenter servers—a firewall mediates the access attempt and permits the connection if authorized, as shown in Figure 13. This means that, by separating production and backup data on the networks, an attacker who gains control of a virtual machine would not be able to compromise additional systems by using the backup network.
In this solution, access between the production network and the backup network is permitted only through a firewall policy restricting access to the Avamar management and control planes by authorized administrators and orchestration processes.
Chapter 3: Protection Architecture and Design

**Backup service levels**

The backup service levels in this solution are used to differentiate between the level of protection required by different virtual machines and applications. The backup service levels are only relevant to backup protection and are not related to or influenced by the storage service levels used by the virtual machines.

Based on the higher-level service tiers having more frequent backups and longer-term retention policies compared to the lower-level service tiers, the main properties that define these backup service levels are:

- Backup target
- Backup schedule
- Retention period for the backup

The backup service levels defined for this solution, shown in Table 3, are suggestions only and can be tailored to the specific requirements of a particular customer environment.

**Table 3. Suggested backup schedule and retention policies for backup service levels**

<table>
<thead>
<tr>
<th>Backup service level</th>
<th>Backup target</th>
<th>Schedule</th>
<th>Retention</th>
<th>Final backup retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataDomain-Daily:3years</td>
<td>Data Domain</td>
<td>Daily</td>
<td>3 years</td>
<td>5 years</td>
</tr>
<tr>
<td>Avamar-Daily:1year</td>
<td>Avamar</td>
<td>Daily</td>
<td>1 year</td>
<td>3 years</td>
</tr>
<tr>
<td>Avamar-Weekly:6months</td>
<td>Avamar</td>
<td>Weekly</td>
<td>6 months</td>
<td>1 year</td>
</tr>
</tbody>
</table>

**Note:** Final backup retention is the period the final backup before the removal of the virtual machine is preserved.

For this environment, we selected the Data Domain system as the backup target for the premium level of backup because of its ability to restore production virtual machines quickly with its Instant Access functionality. Because both Avamar and Data Domain backup operations are managed through Avamar, either target can be selected to support a backup service level where appropriate.

**Note:** While all standard restore operations from both Avamar and Data Domain targets can be initiated from the user portal, Instant Access restore operations are manual processes that must be managed by an Avamar or backup administrator.

Each service level represents a virtual machine folder in vCenter, as shown in Figure 14, which can be viewed in the Virtual Machines window of vSphere Client. These folders, or service levels, are added as Avamar clients that are protected with backup schedules and retention policies. Virtual machines provisioned into these service-level folders are automatically backed up according to the schedule defined at the folder level and are retained as defined in the retention policy of the service level.
The creation of the service levels for backup is a one-time task per service level. This functionality is available only to the cloud administrator from the vCloud Automation Center service catalog, as shown in Figure 15.

**Figure 14.** vSphere Client views of backup service-level folders in vCenter

**Figure 15.** Data protection services for cloud infrastructure administrators
The Create Backup Service Level operation is executed using vCenter Orchestrator, which automates all the required tasks across vCloud Automation Center, vSphere, and the Avamar system using the service-level name, schedule, and retention policy information provided by the user. The cloud administrator can also display and delete existing backup service levels from the service catalog.

Software resources

**EMC Enterprise Hybrid Cloud software resources** For information about qualified components and versions required for the initial release of EMC Enterprise Hybrid Cloud 2.5.1, Federation Software-Defined Data Center Edition, refer to the *EMC Enterprise Hybrid Cloud 2.5.1 Software-Defined Data Center Edition: Foundation Infrastructure Reference Architecture*. For the current supported version information, refer to EMC ELab's *EMC Simple Support Matrix: EMC Hybrid Cloud 2.5* at elabnavigator.emc.com.

**EMC sizing** For all EMC Enterprise Hybrid Cloud sizing operations, refer to the EMC Mainstay sizing tool at mainstayadvisor.com/go/emc.
Chapter 4 Data Protection Services

This chapter presents the following topics:

- Hybrid cloud self-service ................................................................. 40
- Backup and recovery services ......................................................... 41
- Use cases ......................................................................................... 44
- Summary ......................................................................................... 65
Hybrid cloud self-service

Overview
vCloud Automation Center provides a unified self-service portal for delivering infrastructure, applications, data, or anything as a service (XaaS). The self-service portal streamlines the ability of cloud users to request services and access to virtual machines.

Through the self-service portal, vCloud Automation Center provides a highly flexible means for customizing machine configurations while integrating the machine provisioning and management with other enterprise-critical systems.

Federation Software-Defined Data Center self-service portal
The self-service portal in this hybrid cloud solution presents users with a service catalog of customized and approved services and applications. These catalog items are the result of pre-engineered storage and infrastructure services that have been customized to meet the many needs of the business. All the service specifications and policies can be preconfigured and approved by higher-level cloud administrators, allowing end users of the cloud to provision, manage, and dispose of their own systems.

In this solution, through the integration of vCloud Automation Center, EMC ViPR, and EMC Avamar, cloud users have access to storage and data protection services through the self-service portal, where:

- IaaS and fabric group administrators can create and manage storage and data protection services.
- End users can request, manage, back up, and restore their own virtual machines.

Figure 16 depicts the self-service portal and service catalog.

Figure 16. Self-service portal and service catalog overview
The self-service portal offers cloud users a range of cloud operations, including:

- A catalog of storage and data protection services
- A catalog of systems and applications
- Streamlined deployment of systems and applications
- Automatic protection of business and mission-critical machines
- On-demand backup, restore, and billing operations

The self-service portal provides users with a simple and efficient process removed from the complexities of the underlying technologies that support and enable the services within the hybrid cloud.

**Backup and recovery services**

Cloud infrastructure administrators as well as cloud end users consume the backup and recovery services available with this hybrid cloud solution.

**Managing backup service levels**

As shown in Figure 17, vCloud Automation Center cloud administrators use their service catalog to create the backup service levels that are later chosen by cloud users to protect their virtual machines.

![Service Catalog](image)

**Figure 17. vCloud Automation Center service catalog**

The data protection options available to cloud administrators when they are creating a backup service level in the vCloud Automation Center service catalog map directly to the inputs required to create an Avamar policy.

The cloud administrator is required to specify a backup service-level name, select the appropriate target backup system, apply a schedule, and specify a retention period. After the backup service level has been created, it is available to end users to select when deploying their virtual machines.
Users of virtual machines deployed with data protection can use a number of virtual-machine-level, on-demand actions, such as backup, restore, and reporting.

All virtual machine backup and restore operations are managed through EMC Avamar, while all reporting information is provided by EMC Data Protection Advisor.

Both Avamar and Data Domain systems are used as targets for regular backups of virtual machines. The option to configure backup protection is presented through the vCloud Automation Center self-service portal at provisioning time for virtual machines. At provisioning time, cloud users can choose to protect their machines with a predefined backup service level, as shown in Figure 18.

The deployment of the virtual machine is based on a vCloud Automation Center blueprint, and its compute resources are controlled by the scope of the resource limitations specified in the blueprint. The selection of a backup service level has no bearing on the configuration of the virtual machine, nor is it influenced by the size or capability of the virtual machine.

Virtual machine backup

After a user selects a backup service level and the virtual machine is provisioned, backups automatically run in accordance with the schedule defined by the service level.
A virtual machine can be backed up on demand if required, outside the rotation of its scheduled backups. On-demand backup is requested through the vCloud Automation Center self-service portal. Figure 19 highlights the on-demand virtual machine actions for data protection.

Figure 19. On-demand data protection actions for virtual machines

Each individual backup of a virtual machine is retained for the duration specified by the service level. You can change the backup service level after the virtual machine is provisioned, in which case the virtual machine follows the backup schedule of the new backup service level. The previously accumulated backups are retained according to the retention policy applied at the time of the first backup of the virtual machine.

Virtual machine restore

Cloud users can initiate on-demand restores for their virtual machines from the vCloud Automation Center self-service portal, where the user can select from previous backups to restore to the desired point in time.

The vCloud Automation Center self-service portal is customized to provide the cloud user with an on-demand restore operation for a particular virtual machine, as shown in Figure 20.

Figure 20. On-demand restore functionality in vCloud Automation Center user portal
Each virtual machine deployed as a member of a multimachine blueprint can be restored individually. When restoring a virtual machine, a cloud user can select from a list of available point-in-time backups to restore to.

Retired virtual machines can also be restored if required. When a virtual machine is retired in vCloud Automation Center, a final backup is taken with a long-term retention policy. This final backup enables a future restore of the virtual machine as a new virtual machine. If the virtual machine is deleted from vCenter, the restore of the virtual machine can be performed with the Avamar management console. The virtual machine must be discovered by vCloud Automation Center to be included in the inventory.

**Multimachine data protection operations**

For multimachine blueprints deployed with vCloud Automation Center, the backup service level is applied to each virtual machine within the individual blueprints.

All on-demand operations are managed at the individual virtual machine level and applied to single virtual machines, whether or not they were part of a multimachine deployment.

**Use cases**

The following use cases provide an overview of some of the infrastructure and user tasks involved in the protection of virtual machines in this Federation Software-Defined Data Center solution.

**Use case 1: Create backup service level**

The cloud administrator, not necessarily the vCloud Automation Center cloud administrator, can create a backup service level when needed to match business requirements. The creation of a backup service level is a one-time task run from the cloud administrator’s vCloud Automation Center service catalog. In this solution, the administrator uses the Create **Backup Service Level** catalog item to establish the name of the service level, target device, schedule, and retention policy.

The cloud administrator follows these steps to create a backup service level:

1. Log in as a cloud administrator, click **Catalog**, and then click **Request** on **Create Backup Service Level**, as shown in Figure 21.
2. Under **Request Information**, type a description of the service level, as shown in Figure 22.

3. Under **Backup Service Level**, type a name for the new backup service level and select the backup target from the list of available targets, such as Avamar and Data Domain, as shown in Figure 23.
4. Select a backup schedule.

You can select **Daily**, **Weekly**, or **Monthly** backups. When a daily schedule is selected, as shown in Figure 24, single or multiple time intervals are acceptable (for example, 03:00, 03:30).

5. Create a retention policy appropriate for this backup service level.

Several types of retention policies can be created. You can:

- Retain the backups forever
- Retain the backups for a certain number of days/weeks/months/years
- Retain the backups until a certain date
- Define a custom retention period
To keep the backups for a certain number of days, weeks, months, or years, select the **for** option, enter a number, and select **days, weeks, months, or years** from the menu, as shown in Figure 25.

**Figure 25. Create Backup Service Level: Specify retention period**

To define a backup retention period of forever, select **forever** from the list. To keep the backup until a certain date, select the **Until** option, which allows you to choose any future date.

A long-term retention policy, which defines the length of time that the final backup of a virtual machine is retained, can be applied.

A custom retention schedule can be applied based on each of the backup types by making selections from all of the possible parameters available, as shown in Figure 26.
6. Click **Submit** when you have completed the schedule.

The preceding steps are all that is required of the cloud administrator to create a new backup service level. The following section details the native operations that are automated after the request is submitted.

**Native tasks required to create backup service level**

The workflow, as shown in Figure 27, runs several vCenter Orchestrator and Avamar tasks in sequence to create the service level. The workflow also creates or updates the service-level property for the cloud users.
The vCenter Orchestrator workflow to create a backup service level describes the creation of a new vCenter folder, which is treated as a new service level, as shown in Figure 28.

Figure 27. Create Backup Service Level workflow: vCenter Orchestrator workflow detail

Figure 28. New backup service level (virtual machine folder)
This new folder created in the Cloud vCenter server is added as a new Avamar client in the Avamar Administrator console, as shown in Figure 29. The new client is added with **Dynamic Virtual Machine Container Inclusion** and **Enable changed block tracking** options. All operations are completed with the required Avamar MCCLI commands.

The following Avamar objects are created as part of the new service-level process:

- Avamar dataset
- Avamar schedule
- Avamar retention policy

The new Avamar dataset defines what to back up and where to store the backup. In this example, CBT is used to create a new dataset for image-level backup of a Windows and Linux virtual machine, using the Data Domain system as the backup target.

Figure 30 displays the options added to enable this dataset to protect the Windows and Linux virtual machines at image level. The first Data Domain server is used as the backup target and CBT is enabled.
The new Avamar schedule is created based on the backup service level created by the cloud administrator, as shown in Figure 31.

![New Avamar schedule for the new backup service level](image)

**Figure 31. New Avamar schedule for the new backup service level**

A new Avamar retention policy is created based on the retention level designated when the backup service level was created, as shown in Figure 32.

![New Avamar retention policy for the new backup service level](image)

**Figure 32. New Avamar retention policy for the new backup service level**

A new group is created and activated as a placeholder for all these Avamar objects (dataset, schedule, retention policy, and client). The **Avamar Daily:3years** backup service level is selected here. To perform the image backup of a virtual machine, an Avamar proxy server is required; therefore, this new group is also configured with a list of the Avamar proxies available for it to use.

Figure 33 shows the name of the group that matches the service level and status of the group.
Chapter 4: Data Protection Services

Figure 33. Avamar group created and enabled

The Dataset tab, highlighted in Figure 34, shows the dataset details.

Figure 34. Dataset showing the data type to back up: Virtual disks
The **Schedule** tab shows the backup interval and time, as highlighted in Figure 35.

![Figure 35. Schedule showing the backup interval and time](image)

The **Retention Policy** tab shows how long the backups need to be retained, as highlighted in Figure 36.

![Figure 36. Retention policy showing the retention period](image)

The **Proxies** tab indicates the proxies that are used by the client in this group, as highlighted in Figure 37.
Chapter 4: Data Protection Services

After the required Avamar objects are created, the vCenter Orchestrator workflows create or update the service-level property in the vCloud Automation Center custom dictionary with the new backup-service-level name.

The CreateServiceLevel vCenter Orchestrator workflow also creates a build profile and a backup property in the property dictionary. If a CreateServiceLevel workflow is unsuccessful for any reason, then the user sees this immediately in vCenter Orchestrator. The user can then run the DeleteServiceLevel workflow to clean up the environment before resolving the issues and again attempting the CreateServiceLevel operation. The vCenter Orchestrator logs provide visibility into any issues encountered during the workflow.

This use case requires that all added backup service levels are visible to the cloud users.

During this use case, the cloud user adds the virtual machine to the correct backup service-level virtual machine folder in vCenter, and the virtual machine automatically inherits the backup schedule of the backup service-level folder.

The cloud user follows these steps to deploy a virtual machine with automatic data protection:

1. From the vCloud Automation Center self-service portal, select a blueprint from which to deploy a virtual machine and then select the required backup service level from a list of those already created by the cloud administrator.

2. Log in to your account on the self-service portal, click Catalog, and select a blueprint from the list of available blueprints, as highlighted in Figure 38.
Note: Cloud users receive the name of the virtual machine in an email notification from the administrator after the provisioning process is successfully completed.

Service Catalog
Browse the catalog for services you need.

Figure 38. Create new request in vCloud Automation Center self-service portal

3. At Select Backup Service Level, select the required backup service level, as highlighted in Figure 39.

Figure 39. Select a backup service level for the virtual machine

You can also select the number of virtual machines to deploy and increase or decrease virtual machine resources, depending on their entitlements.

4. Review and edit the storage options for the virtual machine, view Cost Summary, and then click Submit.
Chapter 4: Data Protection Services

The virtual machine is provisioned into the relevant folder defined in vCenter for the service level, and it inherits the backup schedules defined by the service level. When the virtual machine is provisioned, an email notification advises the user to wait a set period of time before attempting to access the newly deployed virtual machine. The customization operations, which are required to automatically protect the virtual machine, are run during that time.

Use case 3: Request on-demand backup

This use case describes how a cloud user can request an on-demand backup of a virtual machine, whenever required, from the vCloud Automation Center self-service portal. The user does not have to wait for the completion of the backup task. An email notification of the backup status is automatically generated when the task is completed, whether the task succeeded or failed.

After logging in to the vCloud Automation Center-self-service portal, a cloud user can select On Demand Backup from the Actions menu for a virtual machine, as highlighted in Figure 40.

![Figure 40. Select on-demand backup for the virtual machine](image)

When the on-demand backup request is submitted, the relevant vCenter Orchestrator workflow is initiated. The workflow, as shown in Figure 41, performs the on-demand backup using the dataset and retention policy that the backup service level uses.

![Figure 41. On-demand backup workflow in vCenter Orchestrator](image)
When the task is completed, the user receives an automated email notification with the status of the task. The email status workflow runs asynchronously; therefore, the user does not need to wait for the completion status of the backup.

A cloud user can request a list of the available point-in-time backups for a particular virtual machine.

After logging in to the vCloud Automation Center self-service portal, the cloud user can request the available backups by clicking **Get Backup Status** under **Actions**, as shown in Figure 42.

**Use case 4:**
**Request list of backups available for a virtual machine**

**Figure 42.** Request list of all available backups of a virtual machine

Behind the scenes, an Avamar MCCLI command is run within a vCenter Orchestrator workflow, **ListBackupsOfVM**, requesting that all of the available backups for a virtual machine be emailed to the cloud user, as shown in Figure 43.

**Figure 43.** Workflow in vCenter Orchestrator

When the workflow is completed, the cloud user receives an email notification that lists all the backups available for the virtual machine.
Use case 5: Request an on-demand restore

This use case describes how the cloud user requests an on-demand restore of a virtual machine from the vCloud Automation Center self-service portal, where the user can choose to restore from a list of the available backups.

To be restored successfully, the virtual machine must be powered off.

**Restore to latest available backup**

Follow these steps to restore the virtual machine to the latest available backup:

1. Log in to the vCloud Automation Center self-service portal and browse to **Item**.
2. Select the virtual machines to be restored and click **On Demand Restore** under **Actions**, as shown in Figure 44.

![Figure 44. Select on-demand restore of a virtual machine](image)

The On Demand Restore request wizard, as shown in Figure 45, opens.

![Figure 45. On Demand Restore request wizard: Enter request information](image)

3. Under **Request Information**, type a description of the request in the **Description** field.
4. Under **Choose Backup Point**, select from the available backups in the list box, as shown in Figure 46.

![New Request](image)

**Figure 46.** On Demand Restore request wizard: Select backup point-in-time to restore

After requesting the on-demand restore, the cloud user receives an email notification that indicates the success or failure status of the job, including the reason for a failure if applicable, and how long it took to restore the backup.

If, for example, a virtual machine is powered on, causing the restore operation to fail, the cloud user receives the status email notification showing not just the failure, but also the reason for the failure.

**Use case 6:** Decommission virtual machine

This use case describes how a cloud user or cloud administrator can request the decommissioning of a virtual machine that is no longer required. The cloud user can use the vCloud Automation Center self-service portal to request that a virtual machine be retired or destroyed, as shown in Figure 47.

![Item Details: ITDEV0054](image)

**Figure 47.** Destroy a virtual machine

When the request is made, several tasks are performed. Based on the service level of the virtual machine, a final backup is taken and the virtual machine is retired in the Avamar system, meaning that the virtual machine is permanently deleted from the service-level folder. A retired virtual machine can be restored as a new virtual machine if required at a later stage before expiration. Retired virtual machine backups expire according to the retention policy of the service level, but the last
backup expires according to the long-term retention policy applied at the time of retirement. Retired virtual machines do not participate in any further backup schedules after they have been retired.

During the retirement process, the virtual machine is moved from its service-level folder to a temporary folder where the virtual machine is backed up with a long-term retention policy. When backup is complete, the virtual machine is retired in the Avamar system and the virtual machine is moved back to its original service-level folder. VMware vCloud Automation Center deletes this virtual machine permanently and reclaims the resources that it previously used. Although the virtual machine is retired, all of its backups expire according to the retention policy of the service level, except the last backup, taken when the virtual machine is retired, which expires according to the long-term retention policy.

Figure 48 shows the vCenter Orchestrator workflow that orchestrates the various tasks required to decommission a virtual machine.

Figure 48. vCenter Orchestrator workflow RetireVM used to decommission a virtual machine

The steps in the vCenter Orchestrator workflow RetireVM are as follows:

1. **Create Retire VM folder**—A temporary virtual machine folder is created with a unique string. The name of the folder also contains the long retention name and the virtual machine name. This is achieved using a VMware vCenter API call.

2. **Move VM to Retire folder**—The virtual machine is moved to the Retire folder from its service-level folder.
3. **Perform on-demand backup**—Because this virtual machine will be retired permanently and no further backups of this virtual machine are possible, a final backup is taken with a long-term retention policy based on the service level.

4. **Retire Client**—After the backup finishes, the client is retired in the Avamar system. This removes the virtual machine from the regular Avamar backups, and no further backups are performed on this virtual machine. The virtual machine is also removed from the active view of the Avamar client folder.

5. **Move VM back to Service Level folder**—The virtual machine is moved to its original service level and the vCloud Automation Center destroy process deletes it permanently from vCenter.

6. **Delete the temporary SL folder**—As a clean-up process, the temporary virtual machine folder is deleted from vCenter.

**Use case 7: Request cost and usage reports for a virtual machine**

Cloud users can request cost and usage information of any of their virtual machines from the vCloud Automation Center - self-service portal by selecting **Get Backup Summary** from the virtual machine **Actions** menu, as highlighted in Figure 49.

![Figure 49. Request virtual machine cost details from the self-service portal](image)

The cloud user receives an email notification containing the relevant cost and backup usage information, as shown in Figure 50.
Chapter 4: Data Protection Services

Use case 8: Request backup report for a virtual machine

Cloud users can request a report containing comprehensive backup details specific to any of their virtual machines. A user can run this operation from the self-service portal by selecting the virtual machine and clicking **Get Backup Detailed Report** in the **Actions** menu, as highlighted in Figure 51.

This backup report contains the following information categories:

- Job Summary
- Failed Jobs

**Figure 50.** Email report to cloud user with virtual machine cost summary

**Figure 51.** Request virtual machine backup status from the self-service portal
The cloud user receives an email message containing a report with backup information specific to the virtual machine, as shown in Figure 52.

**Figure 52.** Backup status report emailed to cloud user on request
Use case 9: Delete a backup service level

The cloud administrator can delete an existing backup service level by selecting the option from the vCloud Automation Center service catalog, as shown in Figure 53.

![Figure 53. Delete Backup Service Level request in self-service portal](image)

The cloud administrator must type a brief description of the request before being presented with a list of the existing service levels, as shown in Figure 54.

![Figure 54. Select the service level to be deleted](image)

The cloud administrator selects the service level to be deleted and then must confirm the operation before the system deletes the service level.

**Note:** This operation deletes the virtual machines, backups, and vCenter and Avamar objects for that service level.
Summary

The data protection in this Federation Software-Defined Data Center solution provides automated image-level backup services for virtual machines within a single organization or multi-organization hybrid cloud environment.

The vCloud Automation Center -self-service portal is customized to present several service levels of backup to the cloud user, offering both Avamar and Data Domain backup targets.

This solution offers data protection of cloud resources, using the cloud infrastructure to automatically back up data to a shared, rather than dedicated, backup infrastructure. Cloud administrators can offer BaaS to end users who want a flexible, on-demand, and automated backup infrastructure without having to purchase, configure, and maintain it themselves.
This chapter presents the following topics:

**Overview** ...................................................................................................................... 68

**Monitoring and reporting** ............................................................................................ 68
Overview

The EMC Avamar infrastructure supporting the data protection services for this hybrid cloud solution can be monitored natively with the Avamar Administrator console as well as with EMC Data Protection Advisor and VMware vCenter Log Insight.

Management and monitoring details of the data protection infrastructure are not provided to end users of the Federation Software-Defined Data Center. This level of visibility and information is appropriate to infrastructure and backup administrators supporting the hybrid cloud environment.

Monitoring and reporting

The EMC Avamar infrastructure can be managed and monitored natively using the Avamar Administrator console, as shown in Figure 55.

![Figure 55. EMC Avamar Administrator console: Dashboard](image)

The Avamar Administrator console provides a dashboard with basic information from which the user can further examine the various areas of interest, as shown in Figure 56.
Figure 56. Examination of Avamar appliance through Avamar Administrator console

The Avamar Administrator console can provide details such as hardware health status as well as details on available and protected capacities.

Data Protection Advisor enhances Avamar monitoring and reporting by providing full visibility into the technologies used to protect data in the Federation Software-Defined Data Center, including backup software, backup devices, and virtual infrastructure.

Data Protection Advisor can use analysis policies, as shown in Figure 57, to provide automatic alerts based on specified conditions relevant to the backup component or service.

Figure 57. Data Protection Advisor: Analysis Policies
Chapter 5: Monitoring and Reporting

The Data Protection Advisor reporting engine provides highly customizable reports to highlight problems within the environment. It enables the user to perform capacity management, service-level reporting, chargeback, change management, and troubleshooting.

Data Protection Advisor can quickly identify the health status of relevant components or operations that might be critical to cloud data protection operations. These can range from successful backup or restore operations to the status of required system components such as Avamar proxy clients, as shown in Figure 58.

![Figure 58. On-demand view of active and failed EMC Avamar clients](image)

The Data Protection Advisor predictive analysis engine provides early warning of problems and generates alerts that enable the user to resolve problems sooner and reduce negative business impact.

The report wizard in Data Protection Advisor, as shown in Figure 59, provides the user with a wide range of report templates that can be run on demand or scheduled.

![Figure 59. EMC Data Protection Advisor report wizard: Select Report Template](image)
These reports cover backup clients, objects, and jobs across the entire backup domain and, for virtual machines, contain similar information to the virtual-machine-level reports that cloud users obtain from their vCloud Automation Center self-service portal.

Centralized log management

Avamar and Data Protection Advisor can be integrated with Log Insight to deliver automated log management for the data protection components in this hybrid cloud environment. With an integrated cloud operations management approach, Log Insight provides the operational intelligence and enterprise-wide visibility needed to proactively enable service levels and operational efficiency in dynamic cloud environments, as shown in Figure 60.
Log Insight can analyze log events from any vCloud Suite or Federation Software-Defined Data Center component that can forward syslog feeds. You can configure all components of the cloud management clusters and infrastructure to feed their logs into Log Insight. Some of this log-forwarding configuration is enhanced using prepackaged VMware and EMC content packs.

EMC provides a content pack for Avamar as well as for VNX, VMAX, and XtremIO storage arrays. The content packs provide dashboards and user-defined fields specifically for their respective EMC products, and the dashboards in the content packs assist administrators in conducting problem analysis on their backup and storage infrastructure.

Content packs are immutable, or read-only, plug-ins to Log Insight that provide predefined knowledge about specific types of events, such as log messages. The goal of a content pack is to provide knowledge about a specific set of events in a format easily understandable by administrators, engineers, monitoring teams, and executives. Each content pack is delivered as a file that can be imported into any instance of Log Insight.

Dashboards and widgets can be manually created for those components for which content packs do not already exist.

Each widget provided by a content pack can be cloned and added to a personalized dashboard to contain only the views required by the user. Figure 61 provides an example of this, where the hybrid cloud dashboard contains widgets from each of the content packs installed for this solution.

Figure 61. Customized hybrid cloud dashboard using multiple content packs
Log Insight ships with the vSphere content pack, which when used with Log Insight, provides deep knowledge of and insight into vSphere logs. Content packs are also available for vCenter Operations Manager and vCloud Automation Center.

For Windows-based hybrid cloud components, such as those hosting Data Protection Advisor, the SMI-S server, or SQL Server databases, Log Insight 2.0 can collect data from Windows systems with an easy-to-deploy Log Insight Windows Monitoring Agent.

**EMC Avamar content pack**

The EMC Avamar content pack, as shown in Figure 62, contains a single dashboard with multiple widgets. Each widget details activities that have occurred in Avamar. These activities can be related to backup, restore, and replication. Each of these activities includes fields with properties such as the following:

- Virtual machine name
- Backup duration
- Total bytes scanned/protected
- Total new bytes (source deduplicated and new to the backup appliance)
- Message summary

The activities focus on events that have already occurred rather than the current status.

---

**Figure 62. Sample of the dashboard view: Avamar content pack**

---

**Note:** The EMC Avamar content pack is not officially supported but is available for use.
**Configuring Syslog on EMC Avamar for Log Insight**

To configure Syslog:

1. From the Avamar Administrator console, Select **Tools** > **Manage Profiles** from the Avamar Administrator console.

   A new profile must be created to forward events to Log Insight, as highlighted in Figure 63.

![Image](image.png)

**Figure 63.** Create new profile for Log Insight

2. Confirm that the only notification selected is Syslog, and that SNMP trap and email notifications are not selected.

3. Click **Finish**.

   The new profile appears in the tree list, where it can be edited to include the Syslog information, as shown in Figure 64.
Figure 64. Configure syslog server information for the Log Insight profile

4. Click **Syslog Notification** and type the IP address or name of the Log Insight server. Ensure that **Include extended event data** is selected and **User** is the facility.

5. Select **Event Codes**.

The only events used in the **Summary** column begin with **Activity**.

6. Select **Notify** next to the events that will be sent to Log Insight, as shown in Figure 65.
Chapter 5: Monitoring and Reporting

Figure 65. Select event codes to be sent to Log Insight

**Note:** Events other than Activities can be classified under Interactive Analysis, so that Log Insight can properly parse the message and related fields. More or fewer events might be shown, depending on your version of Avamar.

7. Install the Avamar content pack in Log Insight if it has not already been installed.

**References**

More information on available content packs and downloads for Log Insight is available on the VMware Solution Exchange at [https://solutionexchange.vmware.com/store/loginsight](https://solutionexchange.vmware.com/store/loginsight).
This chapter presents the following topic:

Data protection sizing guide ................................................................. 78
Data protection sizing guide

The sizing of the data protection environment is governed by a number of factors, including how much information is to be protected, the data retention policy, and the frequency of data protection.

Most organizations deploy Avamar in a multinode configuration to protect the primary cloud environment, backing up both the workload and management environments. Sizing the Avamar environment requires an understanding of how information should be protected and managed. Multiple factors govern how the information is protected and influence the size of the datastore. A cloud environment contains a mixture of data types consisting of protected virtual machines and file-level data, either within a virtual machine or as traditional stored file types.

Consideration should be given to how both of these categories impact the data; different data types in an environment offer different efficiencies:

- **Unstructured**—File systems generally offer good deduplication rates because of the repetitive nature of data in the file type.
- **Structured**—Database and email offer lower deduplication rates due to the unique nature of the data types.
- **Media**—Movies and music, although unstructured, offer lower rates because of the uniqueness of the data within the file.
- **Compressed data**—This data type has a lower deduplication rate because the algorithms used to compress the data result in unique data that is deduplicated at the file level.
- **Encrypted data**—By its very nature, this data type disguises the true file structure, resulting in uniqueness, and, therefore, has a lower deduplication rate.

Also, consider the following environmental factors of the data:

- The volumes of each type of data to be protected
- The retention period of at-rest data and protected virtual machines
- The service-level agreement for return on investment and recovery point objective
- The number of anticipated agents connecting to the datastore

For details on the challenges faced by service providers deploying data protection using Avamar, refer to *EMC Avamar – Technical Deployment Considerations for Service Providers*. Hybrid clouds face similar challenges, as enterprises effectively become internal service providers. Therefore, many of the key concepts are identical for an enterprise and service provider.
Hardware sizing for an environment requires support from an EMC Technical Consultant because most of the sizing tools and documentation are only available internally in EMC. For internal EMC personnel (for reference only) the tools and documentation are on the DPAD Sizing Home Page on Inside EMC. The documents consider the deployment of either an environment with Avamar only or, similar to the example used in this Solution Guide, of a hybrid Avamar and Data Domain environment.
Chapter 7: Conclusion

This chapter presents the following topic:

**Conclusion** ........................................................................................................82
Conclusion

This hybrid cloud solution enables customers to build an enterprise-class, scalable, multitenant platform for complete infrastructure service lifecycle management. The solution provides on-demand access and control of infrastructure resources and security while allowing customers to maximize asset utilization. Specifically, the solution integrates all the key functionality that customers demand of a hybrid cloud and provides a framework and foundation for adding other services.

This solution provides the following features and functionality:

- Automation and self-service provisioning
- Multitenancy and secure separation
- Data protection
- Workload-optimized storage
- Elasticity and service assurance
- Monitoring
- Metering and chargeback

The solution uses the best of EMC and VMware products and services to empower customers to accelerate the implementation and adoption of hybrid cloud while still enabling customer choice for the compute and networking infrastructure within the data center.