Abstract
This document discusses data protection using VMware vCloud NFV with Dell EMC Avamar and Dell EMC Data Domain.

October 2018
Executive Summary: Data Protection is important to service providers in the telecommunication space for both workload protection and disaster recovery. Typical NFV deployments have a collection of resource clusters bound to a management cluster supporting life-cycle management, controllability and observability. Management cluster is always engineered for high-availability, but non mission critical workloads in resource cluster(s) are not. Disaster recovery on the other hand uses backup as a building block to move all virtual infrastructure from one site to another, with re-orchestration to resume business continuity. Each use-case (e.g. Software Defined Branch) has a different semantic requirement, backend capacity requirement and business continuity need which must be satisfied by the underlying backup solution (e.g. RPO, RTO). Data Protection for the DellEMC Ready Solution for VMware NFV Platform uses Dell EMC Avamar and Data Domain. A specialized vCloud Director plugin facilitates backup programming on a per tenant basis, while Avamar proxies co-located with application infrastructure move backup bits back and forth over the wire to Data Domain backend.

Audience: This white paper is primarily intended to showcase how one can protect NFV workload in the telecom space. Basic knowledge of VMware vCloud NFV, Compression and Deduplication technologies is assumed throughout. Technical knowledge of Avamar and Data Domain products is helpful but not required to understand this.
# Table of contents

Revisions ........................................................................................................................................... 3  
Introduction ......................................................................................................................................... 5  
1 Architecture ..................................................................................................................................... 7  
2 Back up, restore, and replication ......................................................................................................... 8  
3 Software defined branch use case ....................................................................................................... 9  
4 System Integration (VMware vCloud NFV + AVE + DD VE) ................................................................. 10  
5 Network, NTP, and licensing requirements ......................................................................................... 13  
6 VMware vCloud NFV DP configuration best practices ...................................................................... 14  
7 Conclusion ......................................................................................................................................... 16  
A References ....................................................................................................................................... 17
Introduction

Network Functions Virtualization, or NFV, is an architectural framework that is developed by the European Telecommunication Standards Institute (ETSI) Industry Specification Group (ISG) for Network Functions Virtualization (NFV). The NFV framework aims to transform the telecommunications industry through lower costs, rapid innovation, and scale. The framework provides a standardized model that moves away from proprietary silos, and moves towards network functions that are delivered through software virtualization, with the goal of automating service delivery for multiple tenants, extract operational intelligence, and to assure carrier-grade service reliability. The result is a network that is more responsive and better able to respond to the on-demand, dynamic needs of telecommunications traffic and services.

The framework identifies functional blocks and the main reference points between such blocks. Figure 1 shows the ETSI architectural framework that the NFVI Operations Management functional block compliments, which is not part of the standard framework. Management and organization, or MANO, covers the orchestration and life cycle management of physical and software resources. Within MANO, VIM is responsible for controlling, managing, and monitoring the NFVI compute, storage, and network resources. VNFM is responsible for life cycle management of VNFs under the control of NFVO, which is achieved by instructing VIM. NFVO shapes service characteristics by instructing VNFM, forming a closed loop control system. NFVI operations management augments the core NFV infrastructure by facilitating controllability, observability, and the backup.

VMware vCloud NFV includes the essential building blocks to deploy NFVI, VIM, and Operations Management components using the latest VMware releases.

Note: This whitepaper covers Data Protection for the Dell EMC Ready Solution for VMWare NFV Platform using Dell EMC Avamar and Data Domain

The VMware vCloud Director, or vCD, operates on top of other virtualized infrastructure manager components, such as VMware vCenter Server, and VMware NSX Manager. vCD builds secure, multitenant virtual environments by pooling virtual infrastructure resources into virtual data centers and exposing them to users through web-based portals and programmatic interfaces as fully automated, catalog-based services. A key concept of vCD is that of the tenant. A tenant is a logically isolated construct that represents a customer, department, network function, or service, used to deploy VNF workloads. vCD isolates administrative boundaries into NFVI tenants. The pooled resources that vCD uses are grouped into two abstraction layers:

- Provider virtual data center (PvDC): Combines compute and memory resources of a vCenter Server resource pool with the storage resources of one or more datastores available to that resource pool
- Organization virtual data center (OvDC): Provides resources to an NFVI tenant, or organization, by slicing PvDC resources.

OvDCs provide an environment where virtual systems can be stored, deployed, and operated. They also provide storage for virtual media such as ISO images and vApp templates. vCloud NFV Data Protection (vCloud DP) is used for backup, recovery, and replication of vApp in OvDC. vCloud DP can be used for disaster recovery solutions, however this solution requires you to bind the backing of vCloud infrastructure components (not just vApps), and the orchestration in the new site.

Note: Disaster recovery is outside the scope of this white paper. Workload protection is integrated to VMware vCloud NFV as a plug-in to vCD.
Figure 1   ETSI NFV reference model with FCAPS functional elements
1 Architecture

VMware vCloud NFV Blueprint calls for the clustering of virtual assets that are based on management, and edge/resource roles. FCAPS, VIM, and ancillary components like DNS and OSS/BSS are mapped to (a), while application and edge infrastructure are mapped to (b). There can be multiple edge and resource clusters that are bound to one and only one management cluster.

Data Domain (DD) system performs target deduplication through DD operating system software. Avamar source-based deduplication to a DD system is facilitated using the DD Boost library. The Avamar proxy uses the DD Boost library through an API-based integration to access and manipulate blocks in DD file system. The DD Boost API gives Avamar visibility into the properties and capabilities of the DD system. This enables Avamar to control backup images stored on DD systems. It also enables Avamar to manage maintenance activities and control replication to remote DD systems, such as across the WAN in remote Amazon S3 buckets. Even though DD is used as backup target, backup metadata is always parked in the Avamar server, which lives in the VMware vCloud NFV management cluster. Multiple Avamar proxies is possible, with one per edge and resource cluster, however, only one Avamar server is available in the VMware vCloud NFV management cluster. The vCloud DP architecture, as shown in Figure 2, integrates virtual editions of Avamar (AVE) and DD (DD VE) to vCloud NFV. The key advantage of applying virtual editions is discrete specification of backup capacity needs based on backup characteristics.

![Diagram](image)

Figure 2 VMware vCloud NFV 2.0 two pod architecture with vCD plug-in
2 Back up, restore, and replication

Backup, Restore, and Replication form the fundamental primitives for vCloud DP. While the ability to back up and restore are necessary features, the option for replication, if present, improves system reliability in the sense that Avamar proxies pull data from replicas when the primary DD system crashes. The back-up feature is configured for periodic operation, or is event driven. The Restore function within the pre-defined retention window is always event driven, and the Replication function programmed for periodic operation. Back up programming can be on a per tenant basis, but Replication programming is tenant unaware. Avamar proxies move bits back and forth from the DD system, based on the metadata specification in the Avamar server.
3 Software defined branch use case

SD-WAN solutions include headend infrastructures with high-availability support in the headquarters. The headend infrastructures control and manage Software Defined Branches (SDBR) which serve the distributed enterprise. SDBRs scale rapidly, and have service pipelines whose context, control, and configurations morph frequently to support consistent QoE. A typical branch fuses WAN connectivity, Wi-Fi, and network security into a single service pipeline. Many distributed organizations such as retail stores, banks, and restaurants rely on operations at their branch locations to drive revenue and increase customer satisfaction. For these organizations, the deployment and management of WAN connections from their branch locations is a critical IT function. Simplified, Figure 3 shows the interplay between SDBRs and the rest of the network. Notice the presence of hub branch to back up SDBR context, control, and configurations using a hub-and-spoke model. The backup frequency is matched to business continuity needs, and backend capacity in the hub can be discretely adjusted using predictive analytics.

Figure 3  SDBR use case
4 System Integration (VMware vCloud NFV + AVE + DD VE)

The test bed consists of four clusters:

- One vCloud NFV management cluster
- One edge/resource cluster
- Two DD clusters, one of which is used as replica

All vCloud NFV infrastructure components, including Avamar server and vCD plug-in components, live in the management cluster. The SDBR workload and the associated Avamar proxy, live in the edge/resource cluster. Each DD complex is a cluster which includes one DD VE instance. In this implementation, a single node is used, although the underlay size can be adjusted to match backend capacity needs. The symmetric nodes each have a Dell EMC PowerEdge R730 server with four 10 GbE ports. Each node uses the Intel 710 or Intel 520 NIC, 5 TB of hard drive capacity, and 2x 1 GbE LOM ports for iDRAC and remote access.

Application and replication traffic demand high bandwidth. Link aggregation is achieved by spanning a pair of Dell EMC Networking S4048-ON switches, where 20 Gbps (Lag2) is available for application traffic. 20 Gbps is available for VMware vSphere vMotion and vSAN traffic (Lag1) using VLAN trunking, and 40 Gbps is available for fast high-frequency DD replication. The Avamar/DD pipe must negotiate compressed incremental updates. Use of the 1 GbE interface is sufficient for SDBR use-case, although in other use cases, VLAN trunking for replication and back up is possible.

In vCD-plugin v3.0.1, besides vcpcells (which are logical extensions to vCD cells), there is a need to deploy both backup gateways to bridge vcpcells to Avamar proxies, and vcpUI for DP programming is necessary. For configuration and management, a pair of appliances is used - a virtual provisioning appliance, or vPA, for configuration, and a vMA appliance for operational management. Deployment of the RabbitMQ message Broker agent software assists with the passing of messages between the vCD and vCP. For back-up policy storage, the POSTGres appliance is necessary. Tools exist to check appliance interoperability and configuration. In this test bed, RabbitMQ and POSTGres have been packaged into a single CentOS 7 VM. This plug-in provides a way to program and run backups from the vCD dashboard at sub-vCenter level granularity. Figure 4 shows the management cluster topology, and Figure 5 displays the vCD dashboard with organizations in an SDBR.
vCD in a management cluster is used to deploy SDBR in the edge/resource cluster. Typically, each SDBR has multiple organizations, each of which has multiple external connections for ingress, egress, and for the configuration traffic that is collectively captured in the vApp template. The back-up and restore are done on a per-organization basis. The DP plug-in is realized using vCP cells (1:1 with vCD cell). The plug-in uses the
bridge gateway to connect vCP to Avamar components and other infrastructures for plug-in configuration. vCP cells connect to vCD cells using RabbitMQ infrastructure.

Each of the two DD complexes has a DD VE instance that is deployed using vCenter. One DD VE instance serves as a primary backup, and another is used for replication, in case the primary crashes. Since this is a single node DD complex, the vSAN datastore was not used. For production deployment, use of the complex is recommended for scalability and fault tolerance. In this reference architecture, DD VE v3.1 and Avamar 7.5.1 have been integrated to vCD v8.20 which includes the vCD v3.0.1 plug-in for integration to VMware vCloud NFV v2.

![VMware vCloud Director](image)

Figure 6 SDBR organizations using vApp template
Network, NTP, and licensing requirements

Each instance of AVE and DD VE requires a separate license. Each DD VE license also requires feature and capacity attributes enabled. For VMware vCloud NFV integration, DD Boost, replication, and encryption require enablement. AVE, DD VE, and Avamar proxies require use of the same NTP server, and FQDN specification is required for all vCD, DD, and Avamar entities. Conformity to port usage and firewall programming is required. DD capacity requirements vary by use-case, retention time, and deployment scale, although with predictive analytics, it can be automatically managed.
VMware vCloud NFV DP configuration best practices

The manual configuration of vCD, the vCD plug-in, Avamar, and DD are as important as the connection setup between them. Avamar requires the following:

- Knowledge of the vCenter it belongs to
- Primary DD where bits are deposited
- If there is a failure, the secondary DD which assumes the primary role and replicates the primary DD state
- All relevant credentials for trusted access
- Reporting mechanism for exception events

Figure 7 shows the Avamar setting for an SDBR workload backup. Configuration of DD ensures that Avamar can use the DD Boost protocol with encryption, and can access the replication to peer DD.

Key vCP configurations include:

- Backup gateway and Avamar proxy
- Setup of retention windows
- Policies for unscheduled or periodic backups
- Periodic replications
- Unplanned restoration

The vCP Toolkit provides mechanisms to test the interworking between all seven elements. Figure 8 shows successful configuration of the Avamar proxy and backup gateway, while Figure 9 shows the manual backup of Org1 and the restoration from the last backup. More features to protect the telecom infrastructure are available, however, vCloud requires automation for vCloud profile of vCP, and optimization to accommodate the crowded management cluster.

Figure 7 Avamar Administration main menu
Figure 8  vCPU element configurations

Figure 9  vCPU showing backup of SDBR workload
7 Conclusion

Disaster recovery and workload protection are important for telecommunication service delivery. This white paper explains the function of Avamar and Data Domain for VMware vCloud NFV integration for data protection, using Software Defined Branch as use-case.
References

vCloud NFV Reference Architecture VMware vCloud NFV 2.0

Dell EMC Ready Solution for VMware NFV Platform Solution Brief

Dell EMC Avamar Release 7.5 Administration Guide

Dell EMC Data Domain Virtual Edition v3.1 Installation and Administration Guide

Versa Networks Software-Defined Branch

Dell EMC Avamar for VMware Users Guide

EMC vCloud Director Data Protection Extension Installation Guide

Dell EMC Avamar Data Domain System Integration Guide

Dell EMC vCloud Director Data Protection Extension REST API (v3.0.1)

Dell EMC vCloud Director Data Protection Extension Administration Guide