TECHNICAL WHITE PAPER:
January 2025

VMware Cloud Foundation Cloud Maturity Model – Data Protection and Recovery

Adoption Path for VCF 5.2

Table of contents

Maturity Stage 1: No Data Protection

In this stage, the VCF environment has no protection methods in place to safeguard the critical data assets that make up the business operations.

Maturity Stage 2: Data Protection

In this stage, you have implemented some basic elements of local data protection.

Snapshots and Backups: Performing VM Backups

VM backups are typically performed using 3rd party tools integrated with the vSphere environment, the guest OS, and the applications running on the VMs. The backups might be leveraging disk-based targets for performance benefits for backup as well as recovery tasks. Its best to review the selected backup solution for compatibility with the virtualization environment.

- Support for 3rd party backup vendors – Compatibility Guide

Snapshots and Backups: Best Practices for Snapshots

Snapshots are important because they are one possible way to protect a VM during operations. Snapshots are especially useful for transient scenarios where a reliable “backup” recovery point is desired for a short period of time.

- vSphere Native Snapshots – Best Practices, Overview of virtual machine snapshots in vSphere
- vSAN storage snapshots – vSAN Data Protection

Maturity Stage 3: Disaster Avoidance

Proactive disaster avoidance has two scenarios – local disruption avoidance is the first.

vSphere High Availability (HA): How vSphere HA Works

vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

- How vSphere HA Works
- vSphere HA Admission Control
- Host Failure Types
- VM and Application Monitoring

vSphere HA: Storage Layer with Stretch Clusters

vSAN Fault Domains are a construct that is used when configuring a vSAN stretched cluster: A cluster spanning across two geographical sites. Learn how vSAN uses fault domains to provide site-level resilience for your VMs and data.

- Understanding vSAN Stretched Clusters
- vSAN Stretched Cluster Guide
- vSAN Stretched Cluster Bandwidth Sizing
- Using the vSAN ESA in a Stretched Cluster Topology
- Performance with vSAN Stretched Clusters (OSA)
- vSAN Interactive Infographic
- VMware vSphere Metro Storage Cluster Recommended Practices

Maturity Stage 3: Disaster Avoidance

Proactive disaster avoidance has two scenarios – disruption avoidance to a remote site is the second.

vSphere Replication

- VMware HCX Deployment Considerations and Best Practices
- HCX Availability Configurations and Best Practices
- vSphere Replication – Technical Overview
- VMware vSphere Replication documentation

Maturity Stage 4: Disaster Recovery

Site Recovery

- Hands-On Lab
- Disaster Recovery Solution brief
- VMware Live Site Recovery product information
- VMware Live Site Recovery documentation
- Beyond Data Backups: The Importance of Ransomware and Disaster Recovery Solutions

Maturity Stage 5: Ransomware Recovery

Ransomware Recovery: VMware Live Cyber Recovery

- Hands-On Lab
- Ransomware Recovery Solution Brief
- VMware Live Cyber Recovery product information
- VMware Live Cyber Recovery documentation
- VLR Ransomware Recovery Use Case VCF Field Guide

Ransomware Recovery: VMC on AWS

- VMC on AWS – SDDC IRE (Isolated Recovery Environment)

Ransomware Recovery: Carbon Black

- Carbon Black Cloud NGAV
- Practical guidelines for ransomware resilience – focus on Backup / Recovery section
- Getting Started with Ransomware Recovery Use Case
- Videos
    - Solution Overview
    - Protecting VCF environments
    - Explore 2024 Tutorial Session - Designing and Implementing Disaster Recovery and Ransomware Recovery for VMware Cloud Foundation
    - Explore 2024 Breakout Session - Ransomware Recovery Practices for VMware Cloud Foundation — Technical Deep Dive
    - Cyber Recovery for VMware Cloud Foundation
    - Demo: VMware Ransomware Recovery

vmware by Broadcom

Item No: vmw-bc-wp-tech-temp-uslet-word-2024 1/24