Data Protection for a VMware Horizon VDI Environment using Dell EMC Data Protection Suite

July 2019

H17809

Operations Guide

Abstract

This operations guide provides high-level operational guidance for data protection in a VDI environment. Guidance is based on best practices for corporate data protection.

Dell EMC Solutions

DELL EMC

Copyright

Published in the USA 07/19 Guide H17809.

Contents

Introduction

A robust data protection plan is a key, although often neglected, part of any IT environment. Modern IT environments employ different techniques such as RAID and cluster-level redundancy to provide higher availability. However, hardware failures and user activities can still result in a need for the restoration of user or management environment information and resources.

Solution overview

A Virtual Desktop Infrastructure (VDI) environment consists of three key components:

- Virtual desktops
- VDI management environment
- User profiles and data

Protection of virtual desktops is based on the commonly used, shared golden-image approach. It is important that the data protection methodology used is appropriate for accommodating the nuances of the image deployment process (such as the use of virtual machine snapshots). Regularly test a full backup and restore cycle (including the deployment of a desktop pool) to ensure that the approach functions correctly.

VDI management environment encompasses the pieces of the VDI environment that are used to deploy and manage the user desktops and applications—the connection broker, associated databases, and so on. When selecting a backup and restore methodology for these pieces of the VDI environment, test the methodology to verify that it functions correctly with the environment's virtual desktop base image and with the database formats that are used by the management environment.

User profiles and data contain personalization information for the users and their data. This information may be stored as block-level storage within the storage infrastructure or on a dedicated file workload device. Although protection of this data broadly follows the approach that is used for similar data in a non-VDI environment, ensure that the approach used is consistent with the approaches that are used for the other two components.

Each of the three components of a VDI environment are important parts of the overall environment. Dell EMC recommends that backup and restore of the overall environment be tested at appropriate intervals (such as when the environment is first put in place and after significant version changes) to ensure that the data protection policy meets corporate requirements.

Document purpose

This document provides high-level operational guidance for data protection in a VDI environment from an engineering and technical perspective. The specific backup methodology that is used is based on corporate data protection best practices.

We value your feedback

Dell EMC and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell EMC Solutions team by email or provide your comments by completing our documentation survey.

Authors: Colin Byrne, Peter McCarthy.

Note: The VDI Info Hub for Ready Solutions space on the Dell EMC Communities website provides links to additional documentation for this solution: https://community.emc.com/docs/DOC-69231

Technology overview

The following figure shows the components of a VMware Horizon 7 VDI data protection approach, as described in this guide.

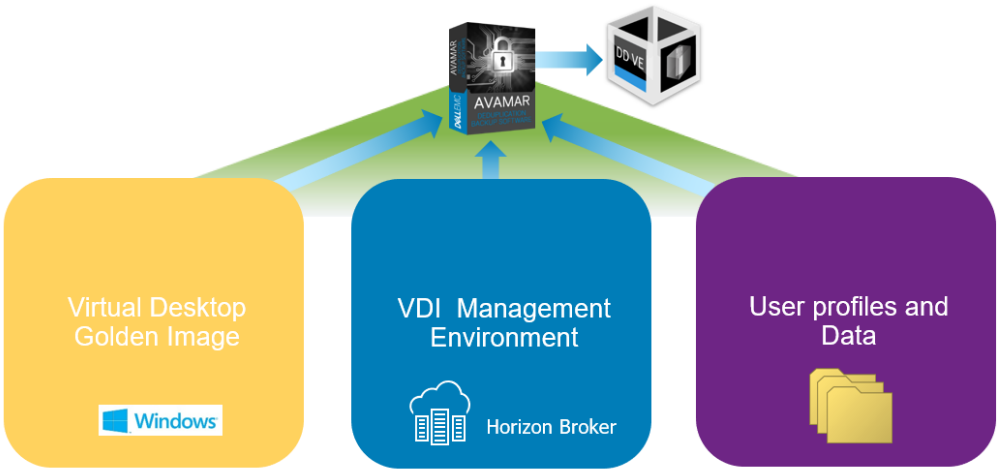

Figure 1. VMware Horizon 7 VDI Data Protection Components

Virtual desktop

Users receive their instance of a virtualized desktop, based on a centralized operating system master/golden image. This optimized operating system image provides a basis for provisioning the virtual desktops. Virtual desktops are provisioned as either persistent or nonpersistent. Persistent desktops are not in the scope of this guide. This guide discusses data protection of nonpersistent desktops which are provisioned using VMware Instant-Clone technology.

VDI management environment

The heart of Horizon 7 infrastructure is the connection server which acts as the brokering software for the client connections. The connection server authenticates client connections and then redirects incoming user requests to the appropriate desktops. Horizon 7 stores connection server configuration and related metadata in the View LDAP repository. Administrators can schedule backups of this database file or manually create backups using Horizon command-line utilities.

User profiles and data

User profiles and user-level file data are stored centrally and roam with users for a consistent user experience. Folder redirection is the main mechanism that ensures user data availability.

Software components

This section describes the software components of a VDI data protection plan.

Horizon 7

Horizon 7 provides a streamlined approach to delivering and managing virtual desktops and applications, providing a consistent user experience across devices and locations while keeping corporate data secure and compliant. The Horizon 7 environment delivers virtualized desktops and application services including Microsoft Remote Desktop Services (RDS) Hosted Apps and packaged applications with VMware ThinApp and SaaS Apps. End users can access these services from a single platform across devices such as desktops, laptops, thin clients, tablets, and smartphones.

Horizon 7 unifies end users' desktops and applications in the data center so that IT teams can centralize desktop management, making the management of desktops simple and agile. Because the virtual desktops are managed in the data center, the organization's intellectual property (IP) remains secure and compliant within the perimeters of the organization.

Horizon 7 with VMware Just-in-Time Management Platform (JMP) can provision and deliver virtual desktops and applications in a fast, flexible, and personalized manner. JMP uses components like VMware vSphere Instant Clone Technology for instant provisioning of desktops, VMware App Volumes for dynamic deployment of applications, and VMware User Environment Manager for personalizing user settings.

Horizon 7 uses Blast Extreme and PCOIP as remote display protocols, providing an excellent user experience in low-latency networks. The Blast Extreme protocol uses both H.264 and JPG/PNG codecs and can select the most suitable codec based on the varying network conditions. With H.264, the protocol can offload the encoding and decoding of the codec to hardware, providing a better user experience. You can offload the H.264 encoding to servers in the data center that are fitted with GPU hardware.

The following table shows the recommended VDI infrastructure:

Table 1. Recommended VDI infrastructure

Hypervisor	Broker and provisioning	Avamar	DataDomain	Client Plugin
ESXi 6.5 U2	Horizon 7.6.0 build-9823717	Avamar VE Edition 18.1.0-33	DD Model 4.0 Virtual Edition 6.1.2.5-595467	Avamar Client Plug-In Version 18.1.100-33

Deployment

For best practice recommendations for deploying Horizon 7, see the *VMware Horizon 7 Installation Guide*.

For specific data protection VDI configurations, see the Environment prerequisites section of this guide.

Avamar and Data Domain Virtual Edition

This section describes the features of Dell EMC's Avamar Virtual Edition and Data Domain Virtual Edition software.

Dell EMC Avamar Virtual Edition

Dell EMC Avamar Virtual Edition (AVE) software brings fast, efficient backup and recovery to a virtualized environment. AVE integrates the latest edition of Avamar deduplication backup software in a virtual appliance that can be deployed on a VMware vSphere platform or Microsoft Hyper-V hypervisors.

Variable-length deduplication technology makes data protection more efficient. Avamar identifies and stores only the data that has changed since the previous backup. AVE is optimized for the backup and recovery of virtual and physical servers, enterprise applications, remote offices, and desktops or laptops. AVE provides both guest and image-level backup and recovery and offers comprehensive security using AES-256 encryption to secure data in flight or at rest.

Dell EMC Data Domain Virtual Edition

Data Domain Virtual Edition (DD VE) is the software-defined version of Dell EMC Data Domain. The key features of DD VE include data deduplication, replication, data integrity, and encryption. DD VE brings efficient, reliable data protection to remote and branch offices and to entry-level and cloud environments.

The DD VE virtual appliance runs on your choice of hardware or public cloud and works with your existing backup, archiving, and enterprise applications. DD VE can scale up to 96 TB of capacity in increments of 1 TB. DD VE also includes features like Data Domain Boost, which accelerates backups by 50 per cent, Data Domain Encryption which provides inline encryption for data at rest and Data Domain Replicator which significantly reduces bandwidth requirements.

Deployment information

For best practice recommendations, see the *Dell EMC Avamar Installation Guide* and *Dell EMC Data Domain Installation Guide*.

For specific data protection VDI configurations see Environment prerequisites.

Environment prerequisites

This section describes the environment prerequisites for specific data protection VDI configurations.

Virtual Desktop prerequisites

Master/golden image state

Recommendation: For each master/golden image of the virtual desktop pools that requires data protection and contains shared PCI devices (GPUs), best practice is that the master/golden image is powered off prior to initiating a backup cycle.

Snapshots

Because snapshot technology is heavily used during the data protection cycle, administrators must be aware of the complex interaction between master/golden image snapshots, host hypervisors, and the data protection software and follow process recommendations.

Recommendation: For each master/golden image requiring data protection, perform the following steps:

1. For the example `master_image_1` {containing_snapshot}, participating in brokered VDI desktops, duplicate master_image_1 by using hypervisor clone technology. See the instructions in *Clone a Virtual Machine* .
2. This action produces two master/golden images:
   - `master_image_1` {containing_snapshot} participates in brokered VDI desktops
   - `master_image_clone_1`, without snapshot. The `master_image_clone_1` participates in the data protection cycle.

VDI management environment prerequisites

Numerous data protection methodologies are available to provide a protection strategy that best suits the requirements of the organization.

Business Continuity and Disaster Recovery for Horizon 7 are outside the scope of this guide.

Implement these recommendations to deploy an application-consistent data protection strategy for Horizon broker software:

1. Schedule a backup of the Horizon Connection Server configuration database. For instructions, see *Schedule Horizon Configuration Backups*.
2. Install the Avamar windows client on the Horizon Connection Server. Follow the instructions in the *Dell EMC Avamar for Windows Servers User Guide*.

User profiles and data prerequisites

The Windows file share contains user profiles and user-level file data.

To protect this data, we recommend that you install the Avamar windows client on the Windows file share server. For instructions, see the *Dell EMC Avamar for Windows Servers User Guide*.

Core VDI data protection

This section describes how to deploy core VDI data protection to back up virtual desktops, the VDI management environment, and user profiles and data.

Back up the virtual desktops

Follow these steps to back up the virtual desktops:

1. Follow the steps in the Environment prerequisites section for Desktop configuration preparation.
2. Initiate backup of the required master/gold image through a suitable Avamar interface.
3. Initiate and monitor the backup of the previously cloned master/gold image, as described in the *Dell EMC Avamar Administration Guide*. Use the default backup wizard configuration. The image that is backed up is `master_image_clone_1`, as described in the preceding section.

Back up the VDI management environment

For broker configuration preparation, see Environment prerequisites. Several methods are available to back up a Horizon Connection Server. Manual, scheduled, or scripted methods might be suitable, depending on the specific circumstances. Follow the *Dell EMC Avamar Administration Guide* to initiate and monitor backup of a previously enabled scheduled backup of a Horizon Connection Server.

To initiate backup of the Horizon Connection Server by using a suitable Avamar interface:

1. In the Avamar Clients tab, specify the server that is hosting the Horizon Connection Server instance.
2. Specify the target location of the 'connection server configuration database file' in the *Horizon 7 Configuration Backup Settings*.

Back up user profiles and data

For user file data preparation, follow the Environment prerequisites section. The Avamar windows client allows backup at folder and file level.

We recommend that you initiate the backup of user-level data by using a suitable Avamar interface.

To initiate and monitor backup of the required file locations on the previously configured Windows file server, follow the steps in the *Dell EMC Avamar Administration Guide*.

1. In the Avamar Clients tab, specify the Windows file server of the hosting file share service.
2. Specify the target location of the required file share/location for:
   a. User profiles
   b. User file level data

Restoring data

Restoring a virtual desktop:

1. Follow the Environment prerequisites section for Desktop configuration preparation.
2. Initiate a restore procedure of the required master/golden image by using a suitable Avamar interface.
3. Initiate and monitor the restore of the required master/gold image, as described in the *Dell EMC Avamar Administration Guide*. Use the restore wizard default configuration.

   Optionally:

   a. Restore to New Virtual Machine

   b. Restore to Original Virtual Machine

   c. Restore to the Original Virtual Machine, for example `master_image_clone_1`.
4. To add the restore master/golden image to the desktop pool, see *Creating Virtual Desktop Pools in Horizon Console*.

Note: Create a snapshot of the restored image. Horizon 7 requires a snapshot to broker an image.

Restoring the VDI management environment

To prepare to restore a broker configuration, follow the Environment prerequisites section. This task consists of two parts:

- Restore the connection server configuration database backup file
- Import the connection server configuration database

Restore the Horizon Connection Server database file through a suitable Avamar interface by following these steps:

1. Follow the *Dell EMC Avamar Administration Guide* to initiate and monitor restoration of the required Horizon connection server database backup file.

   a. In the Avamar Clients tab, specify the server hosting Horizon connection server instance.

   b. Specify a suitable target location of the connection server configuration database file. A temporary location is sufficient.
2. Import the Horizon connection server database.
3. To initiate and monitor restoration of the required Horizon connection server database, see *Backing Up and Restoring Horizon 7 Configuration Data*.

   a. Follow the steps to restore the connection server configuration data.

   b. For authentication configurations, see the VMware Knowledge Base article *Restoring Horizon connection Server from LDAP backup*.

Restoring user profiles and data

To prepare user file data for restoration, follow the steps in the Environment prerequisites section. The Avamar Windows client allows restoration at folder and file level. Before beginning the restoration process, coordinate a suitable user-level data restoration strategy to avoid potential data inconsistencies.

Initiate restore of user-level data using a suitable Avamar interface.

To initiate and monitor restore of the required folder/file to a specified location, follow the steps in the *Dell EMC Avamar Administration Guide*.

1. In the Avamar Clients tab, specify the Windows file server of the hosting file share service.
2. Specify the target location of the required file share/location for:
   a. User profiles
   b. User file level data

References

Dell EMC documentation

The following Dell EMC documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell EMC representative.

- *Dell EMC Backup and Recovery for VDI Environments*

VMware Horizon documentation

The following VMware documentation provides additional and relevant information:

- *Horizon 7 Installation*
- *Horizon Clone Virtual Machine*
- *Backing Up and Restoring Horizon Configuration Data*
- *Schedule Horizon Configuration Backups*
- *Horizon 7 Configuration Backup Settings*
- *Creating Virtual Desktop Pools in Horizon Console*
- *Restoring Horizon Connection Server from LDAP Backup* (access requires login credentials)

Avamar documentation

The following Avamar documentation provides additional and relevant information:

- *Dell EMC Avamar Virtual Edition for VMware Installation and Upgrade Guide*
- *Dell EMC Avamar Administration Guide*
- *Dell EMC Avamar for Windows Server User Guide*

Data Domain documentation

The following Data Domain documentation provides additional and relevant information:

- *Dell EMC Data Domain Virtual Edition Installation and Administration Guide*
- *Dell EMC Data Domain Operating System Administration Guide*