White Paper

EMC BACKUP AND RECOVERY FOR END-USER COMPUTING

Scalable client-side deduplication for fast, efficient backup and data loss protection

- EMC Data Protection Suite
- VMware Horizon View
- Citrix XenDesktop

EMC Solutions

Abstract

End-user computing (EUC) environments are complex deployments requiring a comprehensive backup and recovery strategy. EMC® Data Protection Suite™ provides end-to-end backup of both VMware Horizon and Citrix XenDesktop environments.

March 2016

Published March 2016

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

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EUC Backup and Recovery for End-User Computing
White Paper

Part Number H14754

Contents

Executive summary

Business case

End-user computing (EUC) provides many benefits to IT organizations, including reduced costs, increased workforce agility and mobility, and a decreased data center footprint. As the total amount of data stored for virtual desktops sharing common resources increases, traditional backup solutions cannot meet backup windows, putting your data integrity and business continuity at risk.

Virtual desktop environments provide significant business value by enabling companies to centralize management of the desktop experience and provide new ways for employees to access their information. This kind of system is composed of multiple interlocking technologies and, without proper planning, can be difficult to protect from common failure scenarios that are covered by traditional backup approaches in legacy desktop environments.

This paper describes the key components that need to be backed up, the relationships between them, and how to approach a restore scenario in the virtual desktop space.

Solution overview

EMC Data Protection Suite™ provides the tools you need to protect virtual desktop environments from a wide range of failures by enabling the backup and recovery of the individual components of desktop infrastructure. With Data Protection Suite, you can ensure that every aspect of your EUC environment is protected from data loss. With built-in deduplication, Data Protection Suite provides both backup and deduplication, giving you data loss protection and lower storage costs. EMC is the leader in backup and recovery solutions that bring comprehensive protection to your complex infrastructure.

As part of the Data Protection Suite, EMC Avamar® provides client-side data deduplication with extremely fast and efficient backup and recovery, reducing the daily impact on the virtual and physical infrastructure by up to 99 percent compared to traditional full-backup methods. While traditional backup software moves more than 200 percent of the primary backup data on a weekly basis, Avamar moves as little as two percent over the same seven-day period, removing backup bottlenecks and enabling even greater levels of end user experience.

Benefits

Avamar enables organizations to deploy a deduplication backup system optimized for EUC environments. It addresses the challenges associated with backup and recovery for virtualized desktops in VMware Horizon® View™ and Citrix XenDesktop by employing true variable-length deduplication to dramatically reduce backup times and backup storage. Although Avamar needs to back up only unique daily changes, it stores the data in a full daily format to enable file-level restores in a single step. Its purpose-built backup appliance (PBBA), the Avamar Data Store, provides scalability, high reliability, and accessibility through its unique RAIN (Redundant Array of Independent Nodes) architecture. Avamar is also tightly integrated with EMC Data Domain® systems, another software offering from the Data Protection Suite, to add additional performance and scalability for large virtualized environments.

Document purpose

This white paper describes the options for protecting EUC environments such as VMware Horizon View and Citrix XenDesktop using Data Protection Suite.

Audience

This guide is intended for architects, EUC administrators, and backup systems administrators who are responsible for architecting, deploying, and protecting an EUC environment. They must have a working knowledge of the components that comprise an EUC solution based on VMware Horizon View or Citrix XenDesktop and the associated infrastructure.

We value your feedback!

EMC and the authors of this document welcome your feedback on the solution and the solution documentation. Contact EMC.Solution.Feedback@emc.com with your comments.

Authors: Ka-kit Wong, John Moran, Prasanna Rajagopal, Aighne Kearney

Technology overview

Introduction

The Avamar deduplication backup system in combination with Data Domain provides a next-generation global data deduplication solution for EUC implementations. This integrated solution addresses the challenges associated with traditional backup systems in the evolving next-generation data center. To provide fast, efficient protection for most EUC environments, EMC recommends a combination of Avamar and Data Domain products.

EMC Avamar

Unlike traditional backup solutions, Avamar identifies redundant data segments at the client before they are transferred across the network. By moving only new and unique sub-file data segments, Avamar delivers fast daily full backups while reducing the required daily network bandwidth by up to 99 percent. This capability allows companies to use existing network bandwidth for backup and data recovery (DR) of remote offices and data centers, despite slow or congested networks and infrastructure. Avamar can encrypt data both in flight and at rest for added security, while centralized management makes it easy to protect hundreds of remote offices efficiently.

Avamar Data Store

Avamar Data Store is the easiest and fastest way to deploy a physical Avamar server. It combines EMC-certified hardware and Avamar deduplication backup and recovery software in a fully integrated, scalable, purpose-built backup appliance. Data Store eliminates the inconvenience and complexity of working with multiple vendors for hardware, software, and support. As a turnkey solution, Data Store significantly reduces on-site configuration time, while providing a single point of contact for purchasing, deployment, and service.

Avamar client software and plug-ins

The deployment of Avamar client software and plug-ins to virtual desktops in EUC environments delivers enterprise-class backup and recovery capabilities while enabling end users to recover their own data without IT staff intervention. Avamar's client software and plug-ins are easy to install and manage and can scale across your entire organization, while integrated data deduplication uses existing network links to significantly reduce backup storage costs.

Avamar NDMP Accelerator

Avamar delivers an innovative solution for NAS backup, recovery, and DR. Unlike traditional methods, the integrated deduplication that Avamar offers reduces the size of backup data before it is transferred across the network and stored to disk. As a result, Avamar provides fast, daily full backups using existing network links, without the need for a dedicated, high-speed network data management protocol (NDMP) backup network.

With an Avamar NDMP Accelerator node, a level-0 backup is performed only once, during the initial full backup. Subsequent daily full backups are achieved by requesting only level-1 incremental dumps, enabling Avamar to dramatically reduce backup times and the impact on NAS resources and networks. Avamar thus provides the freedom to consolidate storage and optimize NAS systems, without limiting the number and size of files or volumes due to backup performance limitations.

EMC Data Domain

Data Domain systems are disk-based inline deduplication appliances that provide data protection and DR in the enterprise environment. Avamar source-based deduplication to a Data Domain system is facilitated through the Data Domain Boost library, giving Avamar a view into some of the properties and capabilities of the Data Domain system. This enables Avamar to control backup images stored on Data Domain systems and to manage maintenance activities and control replication to remote Data Domain systems.

Beginning with Avamar 6.0, Avamar and Data Domain are integrated through a single user interface, Avamar Administrator. Avamar and Data Domain system integration provides the following benefits:

- Data Domain systems are a target for Avamar backups
- Avamar can manage one or more Data Domain systems
- Avamar clients use the Data Domain Boost software option to use Data Domain systems as backup targets
- A backup policy on Avamar sets the backup data target destination at the dataset level
- The interface provides transparent user interaction to the backup target (Avamar or Data Domain)

EUC architecture

Overview

An EUC architecture typically encompasses components that require backup and recovery to protect a desktop environment, including:

- Virtual desktop infrastructure
- Virtual desktop
- User profile and data

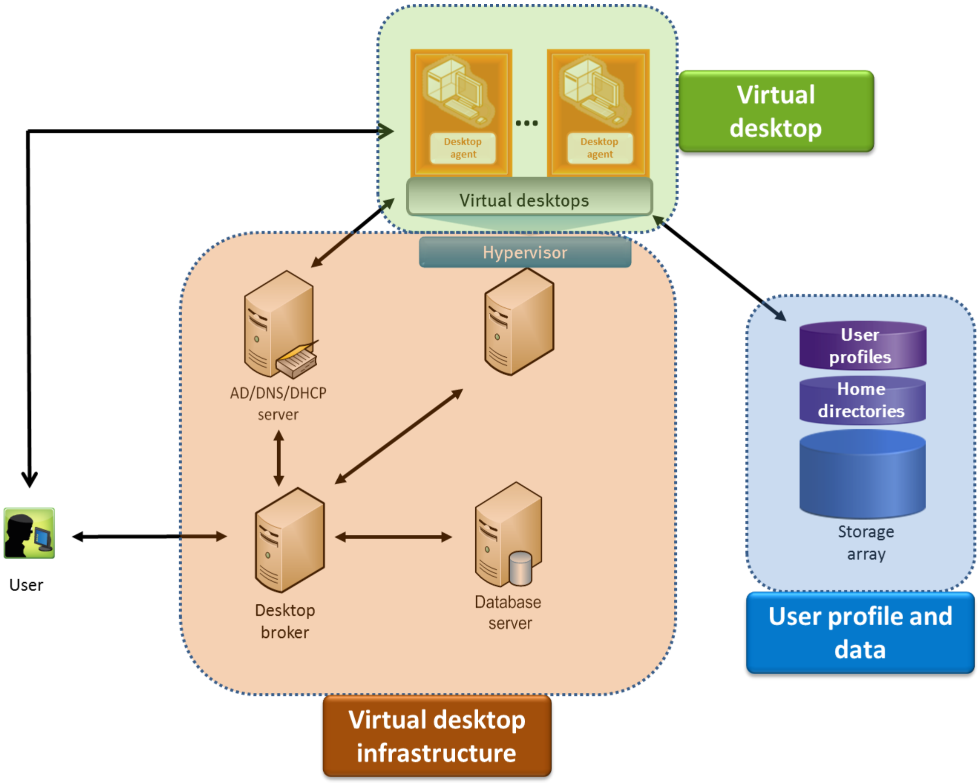


Figure 1. EUC architecture

Virtual desktop infrastructure

Active Directory, DNS, and DHCP server are the foundation of an EUC environment. Active Directory is primarily used for domain authentication and policy enforcement for both users and computers, DNS is responsible for dynamic host name resolution for the virtual desktops, and DHCP automates their dynamic IP assignments. These servers can reside on the same system or on multiple systems for redundancy and scalability purposes.

The virtual desktop infrastructure of an EUC environment comprises the desktop brokers that handle desktop lifecycle management and, optionally, an external database system to keep track of the broker and desktop configurations.

Virtual desktops

Virtual desktops can be categorized as either non-persistent or persistent. In this document, non-persistent means that customizations of user settings or applications are lost after logout or restart. Persistent desktops preserve user or application customizations after logout or restart.

User profile and data

Windows user profiles contain custom user settings and folders that can reside locally on a desktop (local profiles) or be redirected to a NAS repository (roaming profiles). Desktop broker technology may provide its own built-in profile management that coexists with or enhances a Windows roaming profile. As an alternative to the redirected folders in user profiles, you can create home directories to store user data centrally in a NAS repository.

Backup and recovery best practices

Environment infrastructure

Follow the Microsoft recommendations for the backup and recovery of Active Directory described in the Microsoft Technet topic, AD DS Backup and Recovery Step-by-Step Guide.

If you need to restore Active Directory data, ensure that Active Directory is fully restored and synchronized before proceeding with the restoration of virtual desktops. Core infrastructure services such as Active Directory, DHCP, DNS, and NTP must be fully operational before virtual desktop recovery can be completed.

Virtual desktops

For non-persistent desktops, do not attempt to back up the desktop environment directly. Instead, plan to back up the master image and re-provision the desktop on recovery.

For persistent desktops, consider decoupling user settings and local installed apps from the desktop operating system if possible so that only user customization changes require backup. This helps to minimize the backup size and window.

For more information, refer to Chapter 9 of *Avamar Operational Best Practices*.

User profile and data

Use profile redirection, either roaming profiles or profile management from the desktop broker, to decouple the user environment from the desktop. This avoids the loss of user settings when the desktop broker updates the desktop image and enables a more streamlined recovery.

Ensure that user data is mapped to a shared folder outside the desktop virtual machine so that the affected files can be protected by features designed for that use case.

Although user profiles are created locally by default, consider profile redirection using roaming profiles or profile management provided by the desktop broker. In addition to the advantages described above, this also makes it easier to protect the profiles when they are centrally managed. In addition, some profile management systems provided by the desktop broker include enhancements that minimize user logout time by accessing only a required portion of a profile. These profile management systems also address the “last write wins” issues that are inherent in roaming profiles.

VMware Horizon View backup and restore

Horizon View architecture overview

Horizon View provides personalized virtual desktops to end users. With Horizon View, administrators can virtualize the operating system, applications, and user data while gaining control, efficiency, and security by having desktop data in a data center. As Figure 2 shows, Horizon View has several components that work together to deliver a robust EUC environment.

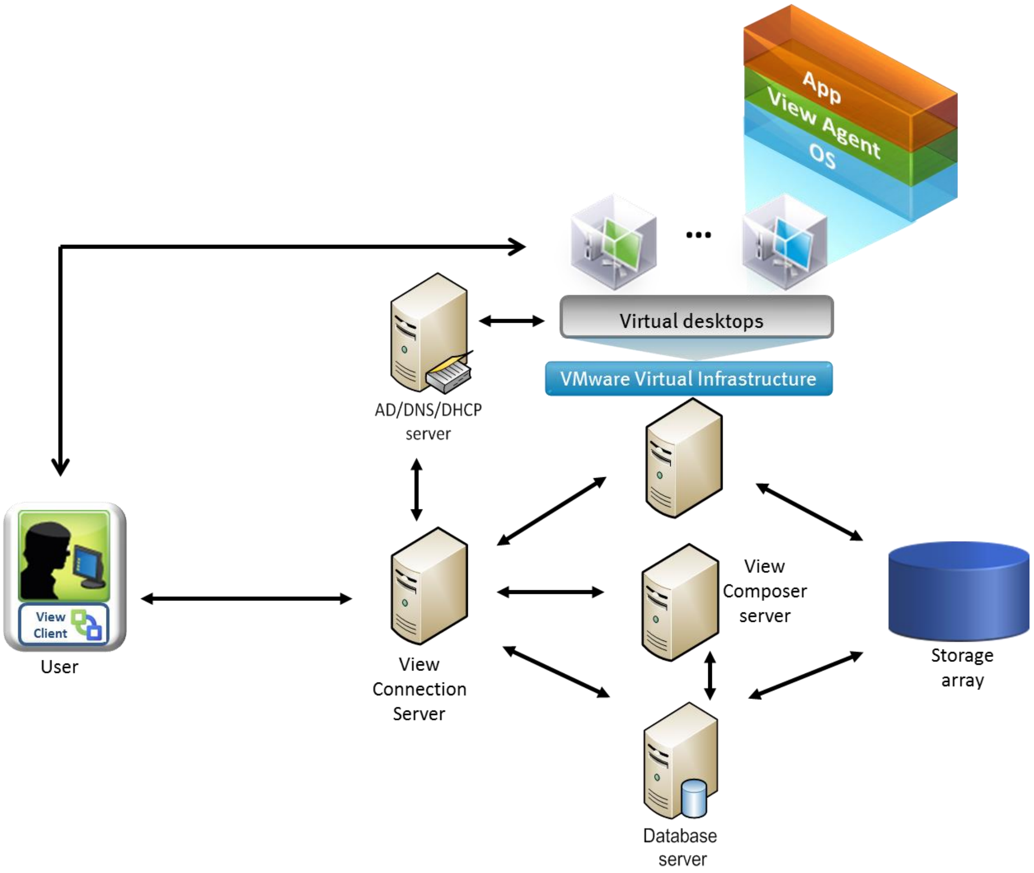


Figure 2. Horizon View architecture

- **View Connection Server** orchestrates the EUC environment. It assigns virtual desktops to users, authenticates users, monitors the state of the virtual desktops, and starts and stops desktops based on demand and the administrative configuration.
- **View Composer server** works directly with vCenter server to deploy, customize, and maintain the state of the virtual desktops when linked clones are used.
- **AD/DNS/DHCP server** provides:
    - IP addresses to virtual desktops using DHCP
    - Secure communication between users and virtual desktops using Active Directory

  - IP host name resolution using DNS

- **Database server** stores the Horizon View, vCenter, and virtual desktop configuration information in a database.
- **VMware Virtual Infrastructure** hosts the virtual desktops. VMware View Composer uses the built-in capabilities of VMware Virtual Infrastructure to manage and configure virtual desktops.
- **View Agent**® provides communication between View Connection Server and the virtual desktops. It also provides a direct connection between virtual desktops and end users through the Horizon View client.
- **View Client** (the user endpoint) communicates with the View Connection Server and View Agent to authenticate and connect to the virtual desktop.
- **Storage arrays** provide storage to the database and VMware Virtual Infrastructure, Virtual Desktop storage, and user data.

Horizon View backup and restore procedures

Virtual desktop infrastructure

This section introduces the methods that this EUC solution uses to protect and restore data for Horizon View.

Table 1 lists the infrastructure components that require backup, along with references and links to the corresponding procedures.

Table 1. Backup and recovery options for infrastructure components

Infrastructure component	Reference	Backup and recovery options
Active Directory	MSDN library	Avamar VADP VM image backup
DNS server	TechNet library	Avamar VADP VM image backup
DHCP server	TechNet library	Avamar VADP VM image backup
SQL server database	*Avamar 7.2 for SQL Server User Guide*	Avamar client plug-in for SQL
Oracle database	*Avamar 7.2 for Oracle User Guide*	Avamar client plug-in for Oracle
vCenter server	VMware KB article	Avamar VADP VM image backup
View connection server	VMware Documentation Center	Avamar VADP VM image backup
View composer server	VMware Documentation Center	Avamar VADP VM image backup

Virtual desktop

View Composer linked clones are provisioned in one of the following ways:

- **Floating user assignment**—Each user is randomly assigned to a desktop from a nonpersistent pool. The desktops are considered nonpersistent and the user may be mapped to another desktop from the pool upon subsequent logins. Because of their disposable nature, there is no need to back up nonpersistent desktops. Ensure that there is a backup for the master virtual machine so its snapshot can be used to regenerate the desktop pool.

- **Dedicated user assignment**—Each user is always assigned to the same desktop, and user settings like Windows profiles may be redirected to a user data disk (also known as persistent disk). If Windows profiles are redirected to the persistent disks, the profiles must be backed up as well as the master virtual machine. Also, a persistent linked clone desktop could have unique data that is not stored in the persistent disk. In this case, it is important to protect the entire desktop using a backup client running on the desktop.
- **Full clone**—Each (persistent) desktop is an instance of a master virtual machine template. Once cloned, each desktop inherits a full copy of the master template and becomes an independent copy of that template.

Table 2 lists the backup and restore options for each Horizon View desktop type.

Table 2. Backup and recovery options for Horizon View

Provisioning method	Desktop type	Components requiring backup	Backup and recovery options
Linked clone – floating	Nonpersistent	Master virtual machine	Avamar VADP VM image backup
Linked clone – dedicated	Persistent	Master virtual machine and persistent disks	Avamar VADP VM image backup and client agent backup
Full clone	Persistent	Full clone desktop virtual machines	Avamar VADP VM image backup and client agent backup

User profile and data

VMware View Persona Management preserves user profiles and dynamically synchronizes them with a remote profile repository. View Persona Management does not require configuration of Windows roaming profiles, eliminating the need to use Active Directory to manage View user profiles.

EMC recommends redirecting all user profiles and home directories to file shares that are centrally managed and protected. When these shares reside on EMC NAS devices such as VNX® File or Isilon®, Avamar NDMP backup with accelerator node can support file system backup and file-level restore for both platforms. Alternatively, you can use built-in file system snapshot capability for both platforms to perform file-level restore. For more information, refer to the following documents:

- *EMC Avamar 7.2 NDMP Accelerator for EMC NAS systems User Guide*
- *Using VNX SnapSure 8.1*
- *Isilon OneFS – Web Administration Guide*

Citrix XenDesktop backup and restore

XenDesktop architecture overview

Citrix XenDesktop transforms Windows desktops into an on-demand service for any user, using any device, in any place. XenDesktop securely delivers any type of virtual desktop application to the latest PCs, Macs, tablets, smartphones, laptops, and thin clients. Refer to the Citrix XenDesktop product documentation website for details.

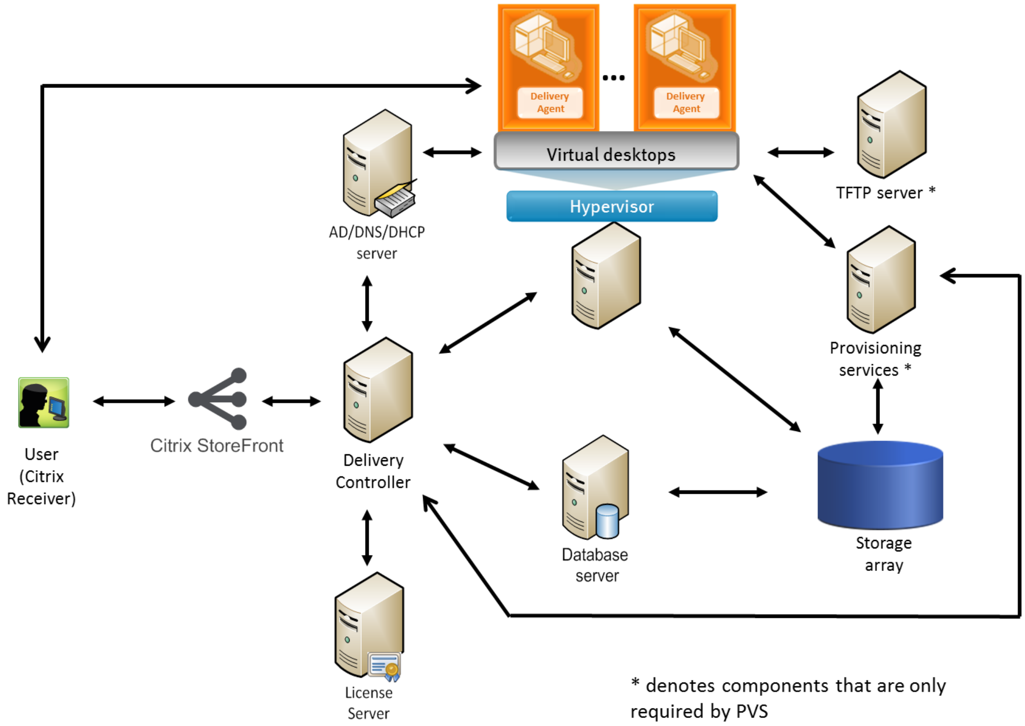
XenDesktop has two provisioning methods:

- Machine Creation Services
- Provisioning Services (PVS)

Machine Creation Services (MCS) is a desktop provisioning mechanism that is integrated with Citrix Studio, the XenDesktop management interface, to provision, manage, and decommission desktops throughout the desktop lifecycle management from a centralized point of management.

PVS uses the streaming technology to provision virtual desktops. PVS uses a single shared desktop image to stream across all the virtual desktops. This approach enables organizations to manage virtual desktop environment using fewer disk images.

Figure 3 shows the key components of XenDesktop infrastructure with MCS and PVS.



* denotes components that are only required by PVS

Figure 3. Citrix XenDesktop infrastructure

- **Citrix Receiver—**Citrix Receiver provides users with quick, secure, self-service access to documents, applications, and desktops from any of the user's devices including smartphones, tablets, and PCs. Receiver provides on-demand access to Windows, web, and software-as-a-service (SaaS) applications.

- **Citrix StoreFront—**StoreFront provides authentication and resource delivery services for Citrix Receiver. It enables centralized control of resources and provides users with on-demand, self-service access to their desktops and applications.
- **Delivery Controller—**Installed on servers in the data center, Delivery Controller consists of services that communicate with the hypervisor to distribute applications and desktops, authenticate and manage user access, and broker connections between users and their virtual desktops and applications. Delivery Controller manages the state of the desktops, starting and stopping them based on demand and administrative configuration. In some editions, the controller enables you to install profile management to manage user personalization settings in virtualized or physical Windows environments.
- **License Server—**License server assigns a user or device license to the XenDesktop environment. Install License server along with other Citrix XenDesktop components or on a separate virtual or physical machine.
- **Virtual Delivery Agent (VDA)—**Installed on server or workstation operating systems, the VDA enables connections for desktops and applications. For remote PC access, install the VDA on the office PC.
- **AD/DNS/DHCP server—**Provides the following:
  - IP addresses to virtual desktops using DHCP
  - Secure communication between users and virtual desktops using Active Directory
  - IP host name resolution using DNS
- **Database server—**Database that stores all the XenDesktop site configuration and session information. Microsoft SQL server is required as a database server.
- **Hypervisor—** VMware vSphere used to host virtual desktops.
- **Storage array—** Provides storage to the database and the hypervisor.
- **TFTP server (PVS only)—** Used by the virtual desktop to boot from the network and download the bootstrap file. The bootstrap file has the information to access the PVS server and stream the appropriate desktop image.
- **Provisioning services (PVS only)—**Used to stream the desktop image to the virtual desktops. The PVS server has a special storage location called vDisk that stores all the streaming images.

Citrix XenDesktop backup and restore procedures

Virtual desktop infrastructure

This section introduces the methods that this EUC solution uses to protect and restore data for Citrix XenDesktop.

Table 3 lists the infrastructure components that require backup, along with links to the corresponding procedures.

Table 3. Backup and recovery options for Citrix XenDesktop

Infrastructure component	Reference	Backup and recovery options
Active Directory	MSDN library	Avamar VADP VM image backup
DNS server	TechNet library	Avamar VADP VM image backup
DHCP server	TechNet library	Avamar VADP VM image backup
SQL server database	*Avamar 7.2 for SQL Server User Guide*	Avamar client plug-in for SQL
vCenter server	VMware KB article	Avamar VADP VM image backup
Delivery controller	Citrix support article CTX135207	Avamar VADP VM image backup
Provisioning services database	Citrix support article CTX130499	Avamar VADP VM image backup
Provisioning services vDisk	Citrix product documentation	Avamar NDMP backup with accelerator node

Virtual desktop

When non-persistent desktops are provisioned using MCS or PVS, there is no need to back up individual desktops because of their disposable nature. For MCS, as long as there is a backup for the master virtual machine from which the machine catalog is created, the backup can be used to regenerate the machine catalog if the machine catalog becomes corrupted or its machines need to be recreated. For PVS, as long as there is a backup for the master vDisk image, nonpersistent desktops can be regenerated by recreating a new set of PVS target devices.

When persistent desktops are provisioned using MCS or PVS, we recommend storing the persistent data on Personal vDisk (PvDisk). In addition to backing up the master virtual machine for MCS or the master vDisk image for PVS, each PvDisk must also be backed up to save the user's settings for each desktop. For more information, refer to the Citrix XenDesktop product documentation on managing personal vDisks.

Table 4 summarizes the backup and restore scenarios for Citrix XenDesktop types.

Table 4. Backup and restore options for Citrix XenDesktops

Provisioning method	Desktop type	Components requiring backup	Backup/restore options
MCS	Nonpersistent	Master virtual machine	Avamar VADP VM image backup

Provisioning method	Desktop type	Components requiring backup	Backup/restore options
MCS	Persistent	Master virtual machine and PvDisk	Avamar VADP VM image backup
PVS	Nonpersistent	Master vDisk	Avamar NDMP backup with accelerator node
PVS	Persistent	Master vDisk and PvDisk	• Avamar NDMP backup with accelerator node for master vDisk on CIFS • Avamar VADP VM image backup for PvDisk

User profile and data

Citrix Profile Management preserves user profiles and dynamically synchronizes them with a remote profile repository. Profile Management downloads a user's remote profile dynamically when the user logs in to XenDesktop, and applies personal settings to desktops and applications regardless of the user's login location or client device.

We recommend redirecting all user profiles and home directories to file shares that are centrally managed and protected. When these shares reside on EMC NAS devices such as VNX File or Isilon, Avamar NDMP backup with accelerator node can support file system backup and file-level restore for both platforms. Alternatively, you can use built-in file system snapshot capability for both platforms to perform file-level restore. For more information, refer to the following documents:

- *EMC Avamar 7.2 NDMP Accelerator for EMC NAS systems User Guide*
- *Using VNX SnapSure 8.1*
- *Isilon OneFS – Web Administration Guide*

Sizing considerations

Introduction

A number of factors determine how to size the Avamar/Data Domain system for an EUC environment, including:

- The type of data in the EUC environment

  EUC user data such as home directories or roaming profiles stored on file systems are considered unstructured data that generally yield very good deduplication rates because of the repetitive nature of data across productivity type files. Backing up infrastructure virtual machine images or desktop images might yield a lower deduplication ratio.

- The amount and change rate of data for each data type

  The master desktop image is typically more static and grows more slowly than the desktops themselves. After it is configured, it is only updated occasionally. The desktops themselves are frequently updated and modified, and therefore likely to generate a higher change rate and larger data set size.

- The retention period of each data set

  Longer retention periods produce larger data sets. Determining the retention policies based on the customer's Service-Level Agreement (SLA) can help size the Avamar/Data Domain system requirements for an EUC environment.

- The number of client agents connecting into Avamar

  When configuring an Avamar system, look at capacity and throughput requirements for backup ingestion and data restoration, as well as the limitation of the number of users and groups (domains) that can be assigned to an Avamar system.

- The customer's Recovery Point Objective (RPO) and Recovery Time Objective (RTO) SLA

  The RPO will determine how often a backup is needed. The RTO must be defined in the planning phase to ensure the data recovery objectives recovery can be successfully met within the defined time period.

This list of sizing parameters provides crucial inputs for the EMC account team to help customers size their unique EUC environment appropriately for data protection.

Conclusion

Summary

Any data loss poses a risk to your business. A comprehensive data loss protection technology combined with deduplication gives you both peace of mind and lower costs. EMC Data Protection Suite offers a comprehensive solution to protect your EUC environment. The topic at ww.emc.com/data-protection/avamar.htm provides more information about EMC Data Protection Suite.

Findings

The various components of an EUC environment must be protected individually, with consideration given to their roles in the environment. Applying the best practices described in this paper in combination with EMC data protection technologies enabled us to back up and restore each of the components so that the system as a whole was protected from failure.

References

EMC documentation

The following documents, located on EMC.com or EMC Online Support websites, provide additional relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your EMC representative.

- *EMC Avamar 7.2 Administration Guide*
- *EMC Avamar 7.2 for VMware User Guide*
- *EMC Avamar 7.2 for SQL Server User Guide*
- *EMC Avamar 7.2 for Oracle User Guide*
- *EMC Avamar 7.2 NDMP Accelerator for EMC NAS systems User Guide*
- *EMC Avamar 7.2 and EMC Data Domain System Integration Guide*
- *EMC Avamar Integration with EMC Data Domain Systems – A Detailed Review*
- *EMC Avamar—Technical Deployment Considerations for Service Providers*
- *EMC Avamar 7.2 Operational Best Practices*
- *Using VNX SnapSure 8.1*
- *Isilon OneFS – Web Administration Guide*

VMware documentation

Refer to the following document on the VMware website:

- *VMware View Backup Best Practices*

Other documentation

XenDesktop product documentation is available on the Citrix website.