BACKUP AND RECOVERY FOR VDI ENVIRONMENTS

Virtual Desktop Infrastructure (VDI) deployments can deliver substantial savings and productivity gains for users and IT by simplifying management of software updates, endpoint devices, data security, and user access while delivering a consistent user experience. However, backing up and recovering VDI systems, desktops, user data and profiles requires a different approach than backing up typical virtual machines (VMs). This solution overview will describe the unique characteristics of VDI deployments and recommend best practices for implementing VDI backup and recovery.

VDI Has Become Critical to the Business

Organizations usually deploy VDI to simplify large desktop installations and more easily deliver Tier 1 applications. This means thousands of users rely on the applications, so backup and recovery capabilities are critical.

However, many companies lack benchmarks for the processes and time required for restoring physical desktops. Backing up virtual desktops is even more complex. Virtual desktop backup and restoration processes vary greatly, depending on the specific vendors and types of desktops deployed. Ideally, desktop backup and recovery for business-critical VDI infrastructure, applications, and data should not require large effort or expense in addition to processes used for backing up regular desktops and VMs.

FEATURES & BENEFITS

Backing up and restoring VDI environments is inherently different than backing up traditional physical desktop environments or normal VMs.

By understanding that there are three separate components that must be considered—VDI infrastructure, desktops, and user profiles with data—you can more easily identify the best steps to take in designing your VDI backup and recovery options.

EMC VDI backup solutions enable you to use existing assets, such as EMC storage systems and software, to achieve your VDI backup and recovery goals.

VDI Environments are Not Monolithic

Unlike physical applications and desktops, which remain static, VDI desktops are assembled on demand as the user works. VDI environments are built on three primary, highly fluid components. For example, depending on the type of desktops deployed, the master image might change. And unlike physical desktops, virtual user profiles and data do not exist as a unit anywhere in the data center. The three components of VDI deployments that must be backed up and recoverable are the virtual infrastructure itself, virtual desktops, and user profiles and data.

VDI Infrastructure

VDI infrastructure encompasses everything that makes the VDI system work:

- VMware Horizon View or Citrix XenDesktop desktops
- Connection servers that orchestrate the VDI environment
- Database servers that store Horizon View, vCenter, Citrix XenApp, and virtual desktop configuration information
- Storage arrays
- Domain name server (DNS), which is responsible for dynamic host name resolution for the virtual desktops
- Active Directory, which is primarily used for domain authentication and policy enforcement for users and endpoints
- Dynamic Host Configuration Protocol (DHCP) server, which automates dynamic IP assignments

For backup and recovery purposes, each of these components has its own procedures, and specific processes depend on vendor specifications. Each component must be backed up according to its own requirements.

Virtual Desktops

Both VMware and Citrix have their own implementations and technologies, and these desktops are categorized as either non-persistent or persistent.

With non-persistent desktop deployments, each desktop image is not tied to a specific user. The user experience is built on the fly, and any user setting or application customization is lost when the user logs off or the desktop is restarted. Each user receives a clone of the master desktop image.

Persistent desktops maintain the master image with user information, and they preserve user and/or application customizations after logoff or restart. Customization information is stored on a persistence disk for each entity—not per session. There are two types of persistent desktops:

LINKED CLONES: A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. This conserves disk space and allows multiple virtual machines to use the same software installation. Restoring linked clones can be done on the fly.

FULL CLONES: Full clones are independent copies of a virtual machine. Once cloned, they share nothing with the parent virtual machine and their ongoing operation is completely separate from the parent virtual machine.

Restoring non-persistent and persistent desktops results in different outcomes. Non-persistent desktops can be restored to their non-persistent states easily because they are built on the fly each time anyway. Restoring persistent desktops introduces additional complexity. Persistent linked clones can only be restored to persistent full clones, and they lose the linkage to their master image file. Full clones can be restored as full clones, but the restored clones will have to be patched and managed separately.

User Profiles and Data

User profiles contain personalization information for the users as well as their data. Profiles and data are stored in storage arrays, which requires that the specific vendors' storage backup and recovery processes be followed.

It Takes All Three

With three separate—yet interdependent—components in VDI deployments, all three must be correct to successfully back up and restore desktops. If the user profile is not correct, you can't rebuild the desktop. If you have all the data but no View controller, the desktop cannot be rebuilt. Unless your enterprise operates with at least two data center locations configured in an active-active scenario, desktops can be lost in the event of an outage because user data and personalization reside on the desktop instead of on a server.

Everything is Vendor-Specific

The final challenge in implementing backup and recovery for VDI deployments is the fact that each virtual infrastructure, desktop, and service element has its own vendor-recommended backup method. Therefore, a critical step in creating your VDI strategy is to plan for backup and recovery. In backup and recovery, the first step is to back up each element according to its vendor's recommendations. In addition, you must be aware that your choice of desktop—non-persistent, linked, or full clone—determines your options for recovery.

EMC Backup and Recovery Solutions for VDI

EMC leads the physical backup market. We back up more stored assets than anyone, and we enable customers to back up any system, ranging from smallest to largest without special licensing. In the Gartner Magic Quadrant, EMC is positioned above all vendors in its ability to execute. We are committed to delivering new capabilities for protecting data and applications wherever they live, whatever happens. The EMC Data Protection Suite offers comprehensive protection from continuous availability to archiving—including coverage for on-premises, virtualized, hybrid cloud, and born-in-the-cloud applications—from a single vendor.

The EMC Data Protection Suite and its tight integration with EMC Data Domain, EMC's enterprise backup and recovery software, provide you with a proven solution for VDI backup on your own premises with virtualized infrastructure.

EMC VDI Backup Solutions

The EMC Data Protection Suite offers a suite of data protection software solutions that make it easier to back up and restore VDI environments:

EMC AVAMAR: Gain fast, efficient backup and recovery through a complete software and hardware solution. Equipped with integrated variable-length deduplication technology, Avamar facilitates fast, daily, full backup and restoration of your VDI infrastructure, desktops, and user profiles and data.

EMC DATA DOMAIN: Rely on highly scalable protection storage that provides high-speed deduplication for backup, archiving, and disaster recovery. Data Domain systems support backup and archive data simultaneously, eliminating the need to buy and manage a separate archiving platform. They also enable global deduplication across both backup and archive data. The Data Domain system can be a consolidated target for backup and archiving, simplifying workflow for management efficiency.

EMC NETWORKER: Gain a full range of traditional and next-generation data protection, including backup to disk, ProtectPoint backup, snapshot and replication management, and tape—under a common management interface. EMC Networker provides complete, centralized application backup and recovery.

EMC XTREMIO: All-flash arrays back up primary storage, virtual infrastructure, and desktop images. XtremIO supports complete, enterprise-scale VDI for all your users across all desktop types. It offers a consistent user experience and data reduction efficiencies for more cost effective storage.

EMC VNX: This flexible, unified hybrid flash storage solution backs up virtual infrastructure and desktop images. It enables you to cover the widest range of mixed workloads with a mix of flash, capacity, and application-aware software.

EMC ISILON: EMC Isilon safeguards data assets and is tightly integrated with VMware ESX and vCenter. It enables use of commercial, off-the-shelf hardware to store, manage, protect, and analyze unstructured data and backs up user profiles and data.

EMC Recommendations for Backing Up VDI Environments

For successful VDI backup and recovery, each VDI component should be protected according to its role in the VDI environment. EMC recommends combining best practices with EMC Data Protection technologies so that VDI environment can be protected from failure.

Backing Up VDI Infrastructure

Each VDI component must be backed up before desktops and user profiles and data can be restored. Follow all Microsoft recommendations to back up, restore, and synchronize Active Directory before proceeding with virtual desktop restoration. In addition, core infrastructure services such as DHCP, DNS, and Network Time Protocol (NTP)—a networking protocol for clock synchronization between computer systems—must be fully operational before virtual desktop recovery can be completed. Table 1 illustrates the infrastructure elements that must be backed up and the EMC backup solutions that can be used.

VMware Horizon with View Infra-structure Elements Requiring Backup	Citrix XenDesktop Infrastructure Elements Requiring Backup	EMC Backup and Recovery solutions
Active Directory	Active Directory	Avamar, XtremIO, VNX
Database server	DNS server	Avamar, XtremIO, VNX
DNS server	DHCP server	Avamar, XtremIO, VNX
DHCP server	SQL server database	Avamar, XtremIO, VNX
SQL server database	vCenter server	Avamar, XtremIO, VNX
Oracle database	Delivery controller	Avamar, XtremIO, VNX
vCenter server	Provisioning services database	Avamar, XtremIO, VNX
View connection server	Provisioning services vDisk	Avamar, XtremIO, VNX
View composer server		Avamar, XtremIO, VNX

Table 1. VDI Infrastructure Components and EMC Backup Solutions.

Backing Up VDI Desktops

Desktop brokers from different vendors have their own implementations and technologies for deploying persistent or non-persistent desktops. For non-persistent desktops, 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, if possible, from the desktop operating system. This will minimize the backup size and window by only backing up user customization changes.

Table 2 describes EMC solutions for backing up VMware and Citrix desktops.

VMware Horizon with View Desktop Type and Components Requiring Backup	Citrix XenDesktop Provisioning Method, Desktop Type, and Components Requiring Backup	Back up and Recovery Options
• Non-persistent, linked clone—floating —Master virtual machine	• Non-persistent MCS —Master virtual machine	**VMware:** Avamar VADP VM image backup **Citrix:** Avamar VADP VM image backup
• Persistent, linked clone—dedicated —Master virtual machine and persistent disks	• Persistent MCS —Master virtual machine & PvDisk	**VMware:** Avamar VADP VM image backup and client agent backup **Citrix:** Avamar VADP VM image backup
• Persistent full clone • Full clone desktop virtual machines	• Non-persistent PVS —Master vDisk	**VMware:** Avamar VADP VM image backup and client agent backup **Citrix:** Avamar NDMP backup with accelerator node
	• Persistent PVS —Master vDisk and PvDisk	**Citrix:** Avamar NDMP backup with accelerator node for master vDisk on CIFS Avamar VADP VM image backup for PvDisk

Table 2. VDI Desktops and EMC Backup Solutions.

Backing Up User Profiles and Data

VMware View Persona Management and Citrix Profile Management preserve user profiles and dynamically synchronize them with remote profile repositories. In both cases, a user's profile is downloaded dynamically when the user logs in, and personal settings are applied to desktops and applications regardless of the user's login location or client device.

Windows user profiles contain custom user settings and folders that can reside locally on a desktop as local profile or be redirected to a NAS repository. There are many different ways to back these up.

Profile redirection decouples the user environment from the desktop for either roaming profiles or profile management from the desktop broker. Redirection maintains user settings when the desktop broker updates the desktop image and enables a more streamlined recovery. For redirected profiles, make sure that user data is mapped to a shared folder outside the desktop virtual machine so that other data protection features can protect data.

When user profiles are created locally by default, consider profile redirection instead. In addition to decoupling user profiles from desktops, redirection 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 logon time by accessing only a required portion of a profile and address “last write wins” issues that are inherent in roaming profile.

Summary

Backing up and restoring VDI environments is inherently different than backing up traditional physical desktop environments or typical server VMs. By understanding that there are three separate components that must be considered—the virtual infrastructure itself, desktops, and user profiles with data—you can more easily identify the best steps to take in designing your VDI backup and recovery options. EMC VDI backup solutions enable you to use existing assets, such as EMC storage systems and software, to achieve your VDI backup and recovery goals.

For More Information

For more information about EMC VDI and data protection, visit http://www.emc.com/data-protection/index.htm?nav=1.

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller, visit www.emc.com, or explore and compare products in the EMC Store

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.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

Part Number H14938