

Deploying Authenticated VMware Virtual Desktop Infrastructure (VDI) Solutions using EMC Celerra Storage and RSA SecurID

Applied Technology

Abstract

This white paper describes an EMC[®] Solution for VMware Virtual Desktop Infrastructure (VDI) that utilizes the EMC Celerra[®] multi-protocol storage platform and RSA SecurID authentication to deliver an efficient, reliable, and secure VDI storage solution.

September 2008

Copyright © 2008 EMC Corporation. All rights reserved.

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

All other trademarks used herein are the property of their respective owners.

P/N H5718

Table of Contents

Executive summary	4
Introduction	4
Audience	4
Overview	4
VMware Virtual Desktop Infrastructure (VDI)	5
Securing the desktop: the business challenge	5
What is VDI?	5
EMC Celerra: extending the value of VDI	6
Rapid desktop deployment.....	6
Market leading infrastructure for user data	6
Enterprise availability for the desktop	6
Further reductions in cost.....	6
RSA SecurID authentication: ensuring user identities for VDI.....	7
Two-factor authentication	7
Integration with VMware’s VDI management platform.....	7
Integrating VMware VDI, EMC Celerra and RSA SecurID	8
EMC Celerra storage system.....	8
iSCSI LUNS.....	9
User “Virtual Drives”	9
RSA SecurID.....	9
VDM 2 SecurID authentication requirements.....	9
Operating system support	9
VDM 2.....	9
Conclusion	10
References	11

Executive summary

As companies seek to control cost and ensure data security, they must address the desktop environment of their PCs and laptops. The combination of an increasingly mobile workforce and stricter compliance requirements is driving businesses to seek more efficient methods for delivering a secure desktop environment that has the most up-to-date software and user applications, and is fully compliant with company standards.

VMware Virtual Desktop Infrastructure (VDI) is an end-to-end solution for server-based virtual desktop computing that leverages thin client architecture and centralizes client desktop images as Virtual Machines (VMs) within a VMware infrastructure. By centralizing VDI information infrastructure in the data center, businesses realize lower costs through a significant reduction in desktop administrative and management tasks. IT can quickly add or patch applications, security is centralized, and the data is easier to safeguard and back up. VDI allows corporations to deliver a robust enterprise support model for company PCs and laptops.

VMware's VDI provides tremendous value to its users but also requires a reliable and cost-effective storage infrastructure. Businesses must ensure that this newly centralized information infrastructure platform is used efficiently and that the data is protected and backed up properly. The EMC® solution for VDI includes the EMC Celerra® IP storage platform and two-factor user authentication through RSA SecurID. Using Celerra SnapSure™ technology, administrators can rapidly deploy hundreds or thousands of virtual desktops while delivering enterprise class reliability and data protection. RSA SecurID uses a strong authentication policy that verifies the identities of users and protects sensitive data and applications.

Introduction

This white paper describes an EMC Solution for VMware Virtual Desktop Infrastructure that utilizes the EMC Celerra multi-protocol storage platform and RSA SecurID authentication to deliver a reliable and secure VDI storage solution.

The topics covered in this white paper include:

- VMware Virtual Desktop Infrastructure
 - Defining the solution
 - Extending the value of VDI
 - Authenticating users through RSA SecurID
- Integration of VMware VDI, EMC Celerra, and RSA SecurID

Audience

The audience for this paper includes security, storage and VMware administrators, technical architects, and IT managers. A basic knowledge of VMware, Celerra, and RSA SecurID concepts is assumed.

Overview

Managing desktop computing assets has always been a time-consuming and challenging task. Whether IT is managing remote users, rolling out patches and upgrades, protecting and backing up data, or ensuring users do not install unlicensed and personal software, it is easy to understand how managing desktops can sap IT resources.

To reduce these management challenges, many organizations are adopting virtualization technology for their desktops using a VMware VDI. The VDI replaces traditional PCs with lightweight thin client hardware and virtual desktops that run on servers in the data center. Administrators can provision new desktops in minutes, give users their own personalized desktop environments, and eliminate the need to maintain a distributed desktop environment. This approach helps to simplify the management of desktop

infrastructure by centralizing critical computing and storage resources. It also extends the life cycle of the hardware and helps IT to respond more quickly to business needs.

VMware Virtual Desktop Infrastructure delivers end-to-end desktop control and manageability but also requires that customers build a secure, reliable, and cost-effective storage infrastructure. This centralized computing and storage platform is a critical asset that IT must manage to prevent unauthorized data access, while minimizing cost and the risk of storage outages.

This paper describes an EMC Solution for VDI that utilizes the EMC Celerra IP storage platform and RSA SecurID authentication to deliver a reliable and secure VDI storage solution. With its 99.999 percent availability and enterprise-class snap and replication capabilities, the Celerra system offers customers a cost-efficient and reliable platform for rapidly creating virtual machine operating system (OS) images, minimizing OS storage requirements. It provides a single platform that also delivers a common storage solution for user-specific data through the Celerra system's multi-protocol support for CIFS, NFS, and iSCSI. Integrating VDI with RSA SecurID two-factor authentication ensures that users are who they claim to be and reduces the risk of improper access to sensitive information.

VMware Virtual Desktop Infrastructure (VDI)

Securing the desktop: the business challenge

Key challenges facing many corporations include controlling costs and ensuring data security and protection. As businesses continue to move their critical support functions offshore, look to enable workforce mobility, or merely look to exercise greater levels of control of their distributed IT assets, the issue of controlling, managing, and securing the desktop environment becomes an increasing challenge.

What is VDI?

VMware Virtual Desktop Infrastructure is an end-to-end solution for server-based virtual desktop computing that improves control and manageability while providing end users with a familiar desktop experience. VDI leverages thin client architecture and centralizes client desktop images as VMs within a VMware infrastructure in the data center. IT benefits include a significant reduction in desktop administrative and management tasks. Applications can quickly be added, deleted, upgraded, and patched; security is centralized; and data is easier to safeguard and back up. VDI allows corporations to deliver a robust enterprise support model for company PCs, laptops, and their data. VDI offers companies the following benefits:

- Like VMware, VDI offers consolidation, dynamic resource management, high availability, and optimized infrastructure management solutions, extended to the desktop.
- Placing desktop images close to centralized IT resources improves fault isolation and remediation and thus improves responsiveness.
- Desktop data resides on a secure network and users do not store data locally, leading to improved security.
- Centralized management allows the application of data-center-class data management, backup and protection practices to desktop data.
- Standardizing on desktop deployment templates simplifies management, allows rapid deployment, and provides a real desktop OS so applications run natively, with no customization.
- Implementing a pooled, shared model for desktop images reduces the total number of systems to be supported, managed and patched, and so on.

EMC Celerra: extending the value of VDI

VMware Virtual Desktop Infrastructure provides tremendous value to its users, and the information infrastructure supporting VDI ensures the most optimal deployment. The EMC Celerra IP Storage platform extends the value of VDI with:

- Rapid desktop deployment
- Market-leading infrastructure for user data
- Enterprise availability for the desktop
- Further reductions in cost

Rapid desktop deployment

Challenge: Even though building VMs for each desktop is far more efficient than building individual physical desktop images, the process introduces an unprecedented challenge of scale to VMware administrators as the environment grows.

Solution: Typically, the basic desktop images are identical for each user in a business unit. Rather than build each VM image in VMware, leverage Celerra SnapSure technology to create array-based replications of VMs very quickly: up to 100 VMs in less than 10 minutes. Each “snapped” image consumes essentially no storage in the array. SnapSure is included with all Celerra systems at no cost.

Market leading infrastructure for user data

Challenge: Effectively manage end user data to maximize user productivity and minimize costs.

Solution: EMC Celerra complements the VDI solution by delivering a centralized platform for storing user files. Not only can Celerra be used to rapidly create the desktop images, it can also be leveraged to provide a “companion” data store for each individual’s user data. And because the data is presented as a personal folder, and stored centrally, you can further reduce cost by implementing centralized backup and archiving. Further flexibility is provided by allowing end users to perform file restores, and centralized controls can be applied such as quotas and file filtering of unauthorized data types, like MP3 files.

Enterprise availability for the desktop

Challenge: When consolidating hundreds of desktops onto a single storage solution, it is critical that the solution provide high availability and advanced data protection options.

Solution: The Celerra architecture provides no single point of failure and 99.999 percent availability to support the largest VDI implementations. EMC’s Celerra Replicator™ provides a remote replication solution for offsite disaster recovery (DR) purposes, and is fully integrated with VMware Site Recovery Manager. Celerra Replicator provides a cost-effective, single DR solution for VDI and user data.

Further reductions in cost

Challenge: VDI Solutions may require support for different tiers of storage as well as need large amounts of space for hundreds of copies of desktop images, typically around 5 to 10 GB each in size.

Solution: EMC Celerra support all protocols supported by VMware and VDI in a single platform: FC, iSCSI, or NFS. Celerra delivers flexible, tiered storage with support for SATA or FC disks in a single system, allowing you to match your requirements to the appropriate storage technology.

RSA SecurID authentication: ensuring user identities for VDI

With VDI, users access the virtual desktops and applications from a desktop PC client or thin client using a remote display protocol. They get direct access to data and features as if the applications were loaded on their local systems, with the difference being that the applications reside on a centralized storage infrastructure.

Allowing many users access to a centralized repository of applications and data introduces security challenges. How do users authenticate? Does the user have permission to view or use sensitive company data? RSA SecurID extends VDI security by maintaining a consistent, strong authentication policy that assures the identities of users and protects sensitive company applications and data. RSA SecurID authentication protects the VDI environment against the unexpected and improves performance and scalability with:

- Two-factor authentication
- Integration with VMware's VDI management platform

Two-factor authentication

Challenge: In this time of data breaches and hackers, companies need to protect important resources from unauthorized use. If the wrong person accesses a user's desktop image, there could be significant damage to the individual and company.

Solution: Two-factor authentication helps to positively identify users before they interact with mission-critical data and applications. With two-factor authentication, the user enters his or her PIN (this is factor 1: something the user knows) and a one-time password generated from an authenticator (this is factor 2: something the user has) to access protected systems.

RSA SecurID is the market-leading, two-factor authentication system. The RSA SecurID system generates a new one-time password every 60 seconds, which ensures that a hacker cannot guess the combined PIN and SecurID password. VMware's VDI management platform offers native support for RSA SecurID strong authentication, extending security from the data center to the end user. This integration allows customers to protect access to the virtual desktop by requiring that employees use two-factor authentication to access the management console for their desktop image, ensuring that users are who they claim to be.

Integrating the VMware VDI solution with two-factor authentication from RSA therefore ensures that users are who they claim to be, reducing the risk of improper access and distribution of sensitive information.

Integration with VMware's VDI management platform

Challenge: Effectively deliver employee authentication while managing costs and assuring a trouble-free integration process

Solution: VMware's VDI management platform (VDM) offers native support for RSA SecurID two-factor authentication. This ensures that customers will have an integration process that is as trouble-free as possible and that their enterprise data will be protected no matter what else changes in their environment.

Figure 1 provides an overview of RSA SecurID in a VDI environment.

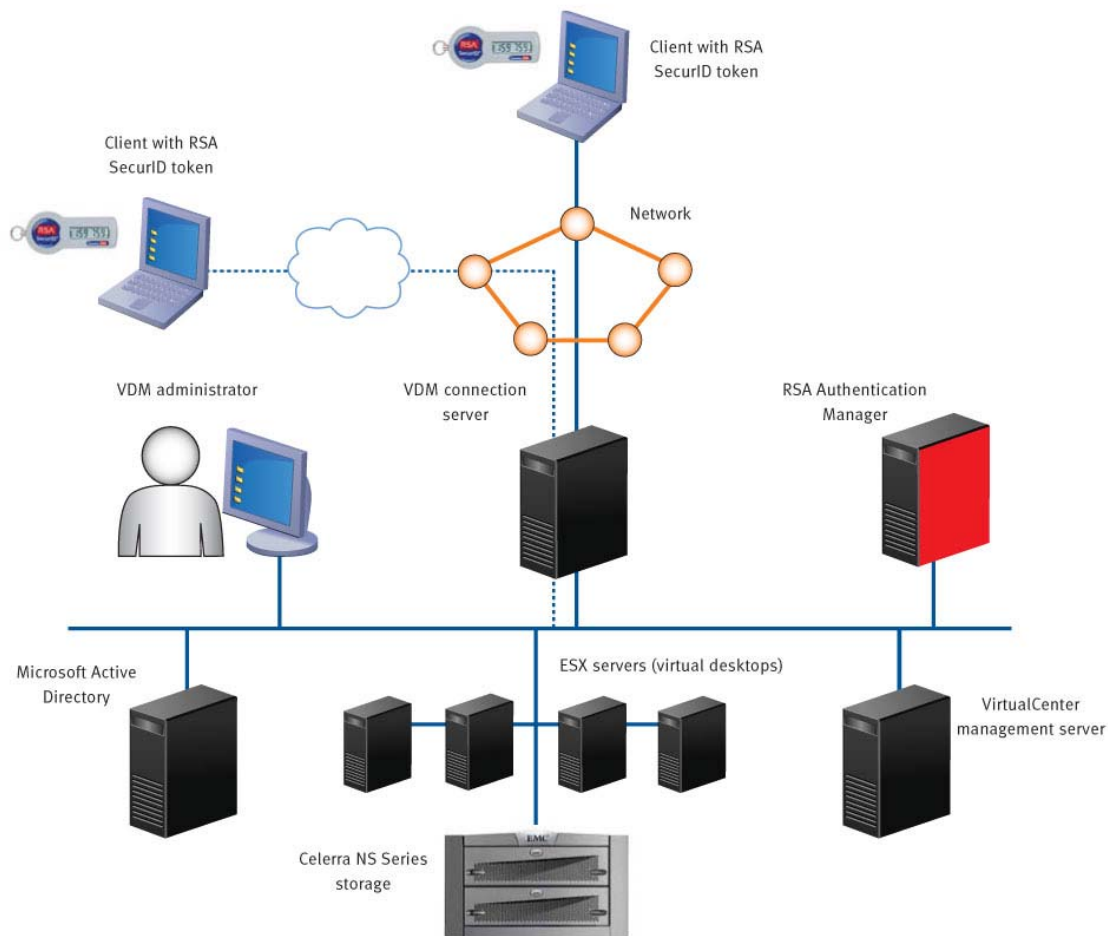


Figure 1 RSA SecurID in a VDI environment

Integrating VMware VDI, EMC Celerra, and RSA SecurID

Configuration best practices for Celerra usage with VMware VDI are covered in greater detail in other documents and are beyond the scope of this paper. However, configuration considerations that are relevant when using VDI and RSA SecurID are referenced briefly in the following sections:

EMC Celerra storage system

The EMC Celerra storage system leverages the following capabilities to integrate seamlessly with VDI for rapid deployment of virtual images and for reliable storage provisioning and data mobility.

- The Celerra storage system provides multi-protocol networked storage using iSCSI target LUNs, NFS exported file systems, and CIFS shares.
- Celerra iSCSI LUNs provide the support for the Virtual Machine File System (VMFS) and leverage the virtual provisioning aspects of the product to minimize the amount of space required to support the VMs.

-
- Local iSCSI LUN replicas can instantly create additional copies of the VMFS Datastores and the VDI Virtual Desktop images. This provides a data mobility option for easily replicating and presenting images to the VDI environment.
 - Virtual Desktop Infrastructure provides for policy management and access to the VMs in the environment.

iSCSI LUNS

In a VDI configuration, the Celerra system is responsible for serving I/O to iSCSI LUNs that provide a “Virtual Boot Disk” to each virtual desktop. This approach not only simplifies the management of the boot images, but also delivers almost unlimited scalability and uninterrupted user access.

Additionally, EMC’s Celerra provides support for virtually provisioned storage devices that typically use very little allocated disk space. The Celerra can create VMFS Datastores and near instantaneous VDI Virtual Desktop images with very little storage burden on the storage system. In the case of VDI, an automated script can be used for snap provisioning and LUN association.

Celerra provides iSCSI termination through one or more iSCSI targets. The iSCSI target presents iSCSI LUNS to the ESX environment using standard Ethernet connectivity. Each iSCSI target on Celerra can support up to 255 LUNs. This allows for significant scalability in that the system can support additional connectivity points by associating additional targets with unused network interfaces, and scaling addressable capacity by increasing the number of LUNs associated with the target.

User “Virtual Drives”

Celerra also stores user data, packaged virtual applications and application data on “Virtual Drives” (iSCSI, CIFS or NFS) that are available to the VMs. By storing all data on a single platform, customers can minimize storage complexity while simplifying the management of data replication, backup and restore, and advanced features such as tiered storage and load management.

Figure 2 provides an overview of Celerra NS Series storage and RSA SecurID in a VDI environment.

RSA SecurID

VDM 2 SecurID authentication requirements

RSA SecurID authentication is a standard feature of VMware VDM 2. An RSA Authentication Manager server is required and must be directly IP network accessible from each VDM Connection Server. To use RSA SecurID token authentication, each user must have a SecurID token that is registered with the RSA Authentication Manager. The SecurID token will generate a one-time password that can be used to access the virtual machines created by VDI.

Operating system support

VDM 2 Connection Server must be installed on a server running Microsoft Windows Server 2003. This server must be joined to an Active Directory domain.

VDM 2

VDM Connection Server is normally implemented on multiple servers to provide high availability and to meet scalability requirements. Each VDM Connection Server can be individually configured for RSA SecurID authentication.

If RSA SecurID is enabled on a VDM Connection Server, then users of this server are first required to supply their RSA SecurID username and password. If they are not authenticated at this level, access is

denied. If they are correctly authenticated with RSA SecurID, they continue as normal and are then required to enter their Active Directory credentials.

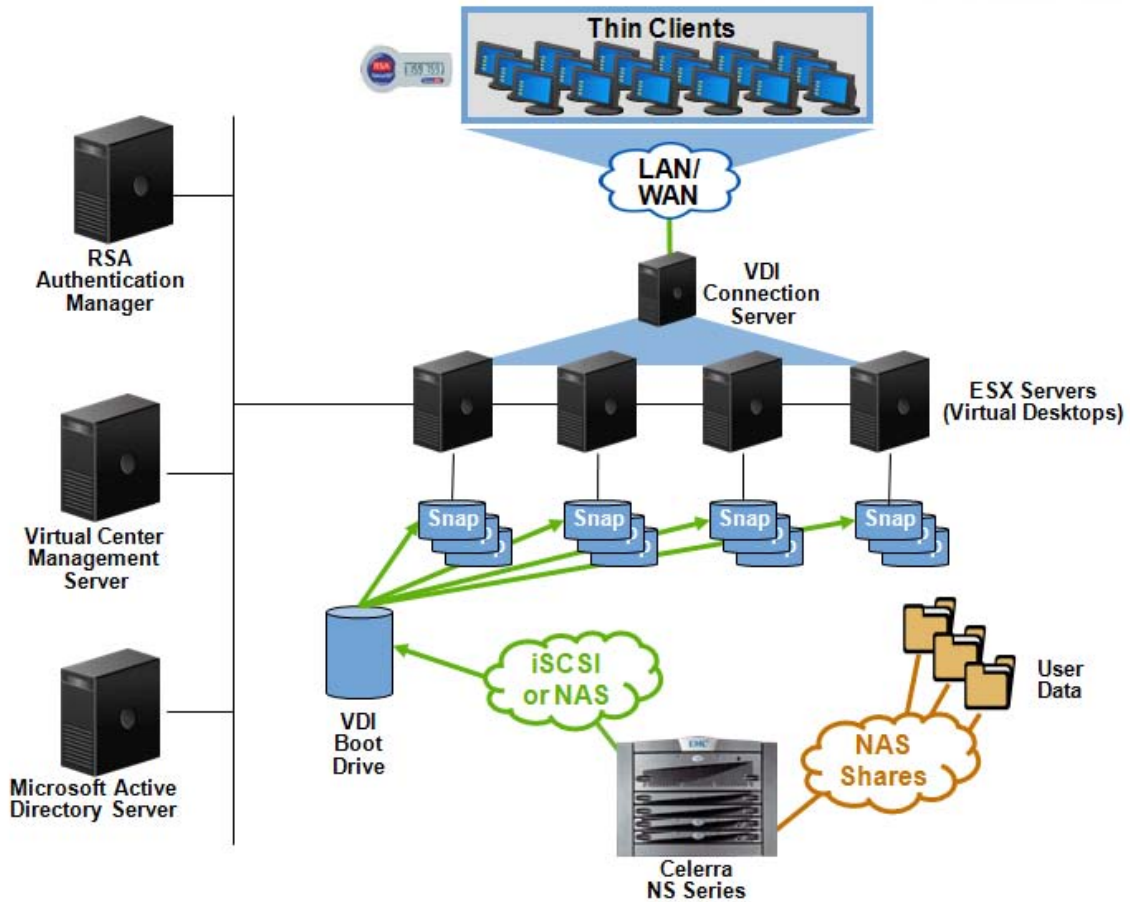


Figure 2 Celerra NS Series storage and RSA SecurID in a VDI environment

Conclusion

VMware's Virtual Desktop Infrastructure helps businesses to control costs, ensure data security, and provide a uniform user experience in desktop environments. Because it centralizes data in one location, VDI requires a reliable and cost-effective storage infrastructure that properly backs up and protects the data. The EMC solution for VDI includes the EMC Celerra IP storage platform and two-factor user authentication through RSA SecurID. Using Celerra SnapSure technology, administrators can rapidly deploy hundreds or thousands of virtual desktops while delivering enterprise-class reliability and data protection. RSA SecurID uses a strong authentication policy that verifies the identities of users and protects sensitive data and applications.

References

The following documents provide additional, relevant information. You can access these documents at www.emc.com or by contacting your EMC representative:

- *Solution Overview: Desktop Manageability: VMware Virtual Desktop Infrastructure and EMC Celerra*
- *Celerra with VMware VDI Provisioning Demo*
- *Solution Guide: VMware ESX Server Using EMC Celerra Storage Systems*

The following documents are available at www.rsa.com:

- *RSA Partner Brief: VMware Virtual Desktop Infrastructure - Securely Deliver Virtual Desktops from the Data Center*
- *RSA SecurID Authenticators Solution Brief*
- *RSA Authentication Manager 7.1 Solution Brief*