



INDUSTRY

Finance

COMPANY PROFILE

Major Financial Institution.

BUSINESS SITUATION

Internal security audits found that VMware ESX, Red Hat Linux, and Solaris systems lacked an efficient way to control access and securely authenticate users.

SOLUTION

Used Likewise Enterprise and Active Directory to establish one ID per user, centralize user and access administration for VMware ESX, enforce global password and security policies with group policy and sudo. Monitored and reported on access and management activities on individual hypervisors.

BENEFITS

Met organizational security compliance standards.

Reduced workload for server and identity administrators.

Streamlined logon processes for users.

Financial Firm Secures Its Private Cloud

“Likewise Enterprise has been instrumental in our security plan to lock down and audit our VMware systems. Virtualization has become absolutely mission critical to our operations and Likewise has been a perfect complement to our production infrastructure.” — Information Security Manager, *Financial Institution*.

Introduction

As one of the world’s most recognizable financial institutions, this firm serves businesses and other financial organizations throughout the United States and internationally. It provides a range of financial services that requires highly available and recoverable production information systems made possible through VMware virtualization.

An internal security audit revealed that its VMware ESX systems as well as its Red Hat Linux VM guests and Solaris systems were configured with file-based methods of user authentication and access control. The staff responsible for user accounts did not have the expertise to manage and synchronize accounts for every type of operating system. Instead they turned to Likewise Enterprise to help them create a single domain solution that manages accounts in Active Directory and provides each user with a single ID for all their heterogeneous systems.

The information contained in this document represents the current view of Likewise Software on the issues discussed as of the date of publication. Because Likewise Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Likewise, and Likewise Software cannot guarantee the accuracy of any information presented after the date of publication.

These documents are for informational purposes only. LIKEWISE SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

Likewise may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Likewise, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Likewise Software. All rights reserved.

Likewise and the Likewise logo are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software
15395 SE 30th Place, Suite #140
Bellevue, WA 98007
USA

Table of Contents

Situation	4
Solution	5
Summary and Results	6
For More Information.....	8

Situation

Virtualization Benefits Drive Rapid Deployment

Beginning in early 2002, broad changes in the organization's networked financial service offerings led to the rapid growth of web applications. As its customers became increasingly dependent on the high availability of its services, the organization had to add many more physical systems. Red Hat Enterprise Linux was chosen for its stability and high uptime. Maintaining the growing data center became rapidly more costly as it expanded and the earliest hardware started to fail. In 2006, an evaluation of the VMware Infrastructure platform concluded that the firm could reduce administrative costs by aggressively using virtualization to consolidate the physical systems and to provide high availability and disaster recovery.

Starting in 2007, the firm implemented a comprehensive virtualization plan, selecting VMware Infrastructure 3 and VMware ESX bare-metal hypervisors to provide support for a majority of internal and external customer-facing deployment scenarios. When any internal customer requested a new server from the IT department, it would be a VM by default. If server hardware for a hypervisor showed evidence of failure, VMs would be migrated to other hardware without sacrificing service-level agreements. By the end of 2009, more than 80 percent of the application servers would be VMs hosted in VMware and the infrastructure would span more than 30 ESX servers.

Interoperability and Security Challenges

The virtualization initiative solved a great many problems and made the IT team agile and more responsive to customer needs, but as a financial institution, regular security audits and controls are required to ensure that customer information is handled correctly. A comprehensive audit found that both Linux and VMware ESX systems needed to enforce a regular 30-day password change policy. More important, the audit also found that the organization should implement a manageable and secure system for authenticating users and controlling access.

On a day-to-day basis, server administrators require secure access to both Linux operating systems and the ESX systems. Administrators

need to routinely log on ESX servers with an OpenSSH client or a Virtual Infrastructure Client to perform backup operations, deploy virtual machines, and troubleshoot problems. If passwords were constantly changing, the situation could become unmanageable without centralized or synchronized identity.

“Our server administrators began to spend more time using the VMware management tools, but we found it absolutely critical to connect directly to ESX hosts if we had to troubleshoot something beyond the capabilities of vCenter.”

Implementing a directory-based solution was a clear candidate for securing the entire infrastructure. The firm was using Active Directory 2003 R2 for its Windows servers. The administrators attempted to implement Active Directory authentication on their ESX hosts by using VMware’s configuration scripts. Although Active Directory’s Kerberos authentication provided single sign on, it provided only part of the desired solution.

“When we incorporated Kerberos authentication on our ESX hosts, we had some of the correct pieces in place, but it had limitations. Every time we changed the status of a VMware administrator, our Windows-oriented user accounts managers would have to update /etc/passwd files. It became a maintenance problem that had the potential to expose security gaps. And we had to treat the ESX systems differently from our Red Hat guests.”

Solution

The company began testing commercial AD-bridge software products that would support all the operating systems in its data center, including its VMware ESX servers. In addition to providing Kerberos authentication that is compatible with Active Directory, AD-bridge software also provides security policy management and audit and reporting functions.

Likewise Enterprise stood out for several reasons:

- Ability to integrate VMware ESX and other operating systems into Active Directory for access control and authentication.
- Account administration is completely transparent with such tools as Active Directory Users and Computers.
- Ability to control security and sudo with group policies and Active Directory’s hierarchy of organizational units.
- Ability to audit access and activity on VMware ESX systems.

- Likewise's exceptional support and professional service offerings.
- Likewise's strong partner relationship with VMware in current and future products.

Moving completely to Active Directory for user management saved the institution significant time in provisioning new users.

"Likewise provided the best solution overall. It was stable and endured our rigorous testing process. We were also impressed that it didn't displace any packages on our ESX servers. The reporting features are now a big part of our quarterly security audit reporting process. We saved a lot of time and effort by going with Likewise."

Summary and Results

A prominent financial institution simplified how it managed privileged user access to its VMware ESX infrastructure by using Likewise Enterprise to integrate its hypervisors with Active Directory. The Likewise solution eliminated costs associated with password resets and user account turnover that would otherwise have required reconfiguring more than 30 VMware ESX systems on a 30-day schedule.

The firm was able to implement a hierarchical security policy across all its systems with both standard domain security policies and sudo policy configured for domain identities, allowing the firm to lock down its systems.

Finally, with Likewise Enterprise's features for auditing and compliance, the firm was able to validate its virtualization security with regular reporting and respond to security exceptions through consolidated event-log analysis.

- **Comprehensive Platform Support – Systems Joined to Active Directory**
 - 30-plus VMware 3.5 ESX Servers were joined to Active Directory.
 - 50-plus Red Hat guests were joined to Active Directory.
 - Additional Solaris and AIX systems were joined to Active Directory.
- **All VMware accounts managed through Active Directory**
 - Windows-based account administrators use Windows default tools for all operating systems, including VMware.
 - Active Directory organizational units are used to limit group access to hosts.
- **Privileged User Access Controlled with Group Policy**

- All day-to-day on-box activities controlled through sudo policies.
- Access to admin and root accounts on VMware disabled, reducing internal threat risks and the possibility of human errors.
- **Enterprise Single Sign-On**
 - GSS-enabled SSH, SFTP, F-Secure and PuTTY used with current credentials – users are not required to enter credentials.
- **Reporting and Audit**
 - Quarterly reports include audits of users, access and activities while passing strict security guidelines for financial organization information.
 - Audit events provide quick response to potential threats or management exceptions.

For More Information

For more information, visit the Likewise web site at <http://www.likewise.com>.

For general questions, call 800-378-1330 or email info@likewise.com.

ABOUT LIKEWISE

Likewise® Software solutions improve management and interoperability of Windows, Linux, Mac OS X, and Unix systems with easy-to-use software for cross-platform identity management.

Likewise provides familiar Windows-based tools for system administrators to seamlessly integrate Linux and Unix systems into Microsoft Active Directory. This enables companies with mixed networks to use existing Windows skills and resources, maximize the value of their Active Directory investment, strengthen the network security, and lower the total cost of ownership of Linux and Unix servers.

Likewise Software is a Bellevue, WA-based software company funded by leading venture capital firms Ignition Partners, Intel Capital, and Trinity Ventures. Likewise has experienced management and engineering teams in place and is led by senior executives from leading technology companies such as Microsoft, F5 Networks, EMC and Mercury.