Guidance Document

Securing Alliance Key Manager for VMware

THIS DOCUMENT IS DIVIDED INTO TWO SECTIONS. The first section addresses general security recommendations for the VMware environment as a whole and is based on guidance provided by standards organizations (Payment Card Industry, Cloud Security Alliance, etc.), VMware (the company), and independent security assessment companies and individuals. The second section addresses specific recommendations for securing Alliance Key Manager for VMware.

Townsend® SECURITY

www.townsendsecurity.com

724 Columbia Street NW, Suite 400 • Olympia, WA 98501 • 360.359.4400 • 800.357.1019 • fax 360.357.9047 • www.townsendsecurity.com

Introduction

VMware customers benefit from the many operational and cost efficiencies provided by VMware virtualization technologies both in traditional IT infrastructure and in cloud environments. As VMware customers deploy data encryption solutions as a part of their defense-in-depth strategy, the need for encryption key management can present barriers to a good encryption implementation. The Alliance Key Manager for VMware (AKM) solution from Townsend Security, Inc. can help VMware customers deploy proper encryption key management within their VMware infrastructure without the need for traditional hardware security modules (HSMs) when this approach is appropriate to the security needs of the organization. This paper provides high level guidance on how deploy and protect Alliance Key Manager for VMware within your VMware environment. This guidance is designed to be general in nature; actual VMware deployments of Alliance Key Manager for VMware will use different VMware applications and architectures to meet specific user, application, and security needs.

Section 1: General VMware Recommendations

Identify and Document Trusted and Un-Trusted Applications

Properly identifying application groups based on the level of trust is critical for a secure implementation of virtualized applications and encryption key management services. Create and isolate a management cluster for your core VMware applications such as vSphere, vShield, etc. Identify application groups and their associated level of trust, and isolate applications into appropriate application workgroups. Avoid mixing trusted and untrusted applications in a workgroup.

You should consider creating a security workgroup to contain your third party security applications such as encryption key management, authentication services, active directory, system logging, and other applications whose primary function is to assist in securing your VMware environment. Encryption key management services provide by Alliance Key Manager should be implemented in this separate security workgroup used for critical, non-VMware security applications.

In preparation for properly securing these environments, create an inventory of all Virtual Machines managed in each workgroup. For each workgroup and virtual machine, identify the security controls that will be required for each one (network segmentation, storage segmentation, system logging, active monitoring, etc.). VMware flow tools can assist with this documentation.

Restrict Physical Access

Fundamental to all IT security implementations is proper security of the physical environment. This means proper physical security controls and physical monitoring of the data center as well as good auditing and procedural controls. These physical controls should also apply to access to VMware management and security applications. You can look to the PCI Data Security Standards and guidance for information on appropriate physical controls. You can also refer to standard security guidance in SOC 2 and SOC 3 assessments for information on physical controls. When deploying on a cloud platform it is always a good idea to ask the Cloud Security Provider (CSP) for a copy of the PCI letter of attestation, or an SOC 2 / SOC 3 report.

Isolate Security Functions

Because security applications are often a target of cybercriminals, you should isolate them into their own security workgroup and implement the highest level of VMware security. Only trusted VMware administrators should have access rights to Alliance Key Manager, system logs, and audit reports. Be sure to actively monitor access to and use of all encryption key management, key retrieval, and encryption services.

Change VMware Default Passwords

Review all VMware applications used to secure and manage your VMware environment and change the default passwords as recommended by VMware. The failure to change default passwords is one of the most common causes of security breaches.

Implement Network Segmentation

Network segmentation is easy to accomplish with VMware network management and security applications and you should implement network segmentation to isolate applications that process sensitive information from applications that do not require as high a level of trust. Additionally, you should provide network segmentation for all third party security applications such as Alliance Key Manager. Network segmentation should include all high availability and business recovery infrastructure. Do not rely on virtual network segmentation alone; use firewalls that are capable of properly securing virtual networks.

Implement Defense in Depth

The VMware management and security applications provide for a high level of security and monitoring. They also provide hooks and integration with third party security applications that provide system log collection, active monitoring, intrusion detection, etc. Encryption is a critical part of a defense-in-depth strategy, and protecting encryption keys is the most important part of an encryption strategy. Regardless of the operating systems in your application Virtual Machines, Alliance Key Manager will provide encryption key management, key retrieval, and encryption services for your business applications and databases running in your VMware infrastructure.

Monitor VMware Administrative Activity

Use an appropriate SIEM solution to collect VMware application and ESXi hypervisor system logs and perform active monitoring. The log collection and SIEM active monitoring solutions should be isolated into a security workgroup that contains other third party security applications such as Alliance Key Manager.

Section 2: Securing Alliance Key Manager for VMware

Implement VMware Network Security

Use a combination of hardware and VMware virtual firewalls to segment and protect applications. The appropriate use of both hardware and virtual firewalls is critical for security in a VMware environment. In addition to traditional firewall rules consider implementing stateful packet inspection and detailed logging for applications that contain highly sensitive information. The protection of encryption keys is considered one such application; you should consider this level of protection for Alliance Key Manager virtual machines.

Alliance Key Manager uses a specific and limited number of ports. By default these ports are 6000 for encryption key retrieval, 6001 for encryption key management, 6002 for key mirroring, 6003 for encryption services, 3886 for server management via the web interface, and 22 for the SSH service. During active use of AKM block access to ports that are not needed. In most cases only ports 6000, 6002 and 6003 should be open for key retrieval or encryption services.

Use Network Address Translation (NAT) to hide the actual IP addresses of AKM servers including any remote AKM servers used for business recovery or high availability.

Change the Alliance Key Manager Password

On first deployment of Alliance Key Manager in a VMware environment, change the server management password and use a strong password. The server management password is used to log in to the web interface and configure the key server IP address, logging options, and other network configurations. Once you have changed the password and completed network configuration, consider de-activating the web interface and using firewall rules to block access to the web interface.

Do Not Mix Production and Test/Development Environments

A single Alliance Key Manager virtual machine should not be implemented to serve both production and non-production environments such as test, development, software quality assurance (QA), and User Acceptance Testing (UAT). Instead, implement AKM as a virtual machine in each of these environments and use VMware management and security applications to provide isolation between production and non-production AKM virtual machines.

Enforce Least Privilege

Review access privileges for Alliance Key Manager virtual machines. Use VMware management applications to create user roles and only allow management access to AKM virtual machines by those VMware users you designate for this responsibility. You can also assign user roles for applications that require access to Alliance Key Manager for key retrieval or encryption services.

In a cloud environment you should never allow general, public access to the Alliance Key Manager virtual machine. The management and security applications within the VMware application suite will complement the access controls implemented directly within the AKM application.

Limit Outbound Connections

Alliance Key Manager is a single purpose security device. You should carefully control outbound connections and traffic. In most cases the only outbound traffic from AKM would include:
Transmission of system log information to a SIEM solution or log collection server, usually to port 514 on the destination system.

- Transmission of encryption key mirroring information to one or more failover AKM servers, usually to port 6002 on the remote key server.
- Transmission of backups to a secure FTP or SSH sFTP server. In the case of SSH transfers this would be to port 22 of the destination system.
- Synchronization of the system time to an internal or external NTP server.

All network traffic that is not explicitly allowed should be denied by firewall rules.

Note that Alliance Key Manager for VMware implements firewall controls as a part of the virtual machine's Linux operating system and these controls can complement and augment VMware network security controls.

Enforce Separation of Duties

The implementation of Separation of Duties (sometimes called "Segregation of Duties") is an important concept in financial, medical, military, and IT environments. Wherever there are sensitive operations in mission critical systems, separation of duties provides an important layer of security and this is appropriate with encryption key management systems used to protect data assets. Identify those Crypto Officers who will have encryption key management responsibilities and ensure that they do not have VMware administrative access. Identify highly privileged application users (DBAs, etc.) and ensure that they do not have authority to VMware administrative functions nor to encryption key management functions. Use VMware access controls and monitoring to prevent a violation of separation of duties. Use staging options for configuration changes. For example, require that changes to VMware firewall rules be approved before implementation.

Implement Dual Control for Encryption Key Management

While VMware provides a wide array of options for securing and monitoring virtual machines, Alliance Key Manager for VMware provides an option for Dual Control of encryption key management activities. When enabled, AKM dual control requires that at least two different Crypto Officers authenticate to AKM before any encryption key management functions can take place. Activate this option and protect the credentials used by the key management administrators.

Monitor and Apply Available AKM Software Updates

Townsend Security may release periodic software updates and patches to address application errors or security vulnerabilities. If you are contacted by Townsend Security and advised to apply a software update, you should review the recommendations and schedule a software update using the procedures described in the patch letter

Secure Encryption Key Backups

Alliance Key Manager supports both manual and periodic, automated backups of the key server including data encryption keys (DEK), key encryption keys (KEK), applications, and configuration files. Backup sessions are encrypted using TLS encryption. You should deploy a virtual server to receive these backups within your security workgroup and protect the backup server with the same level of security you use for the encryption key manager. You may also make backups to tape or cartridge storage media for off-site storage. Be sure that all backups are encrypted using industry standard encryption such as 256-bit AES.

Monitor Key Management Configuration Changes

Once Alliance Key Manager is configured and you have a basic set of encryption keys to protect sensitive data, there should be very little need to change the configuration. All server configuration changes (network interfaces, firewall, system logging, basic key manager options, etc.) are logged to the system log files. All encryption key management configuration changes are logged to the AKM audit file. Be sure that AKM operating system logs and audit files are transmitted to your SIEM solution for active monitoring. You should highlight and validate that all AKM configuration changes are expected and documented. Note that it is not possible to disable AKM audit logging through configuration changes.

Protect Dormant VMs and Snapshots

Alliance Key Manager is designed to provide highly available encryption and key retrieval services across multiple VMware workgroups and in geographically redundant locations. The key management servers should be active in order to support high availability. Dormant AKM virtual machines or snapshots should be backed up to secure encrypted storage and removed from the VMware environment. This will reduce the chance of the loss of encryption keys through inactive, dormant AKM virtual machines or snapshots.

Install and Protect the AKM Administrative Console

The AKM Administrative Console is used by Crypto Officers to create and manage encryption keys on an AKM server. This is a Windows GUI application that can be installed on one or more Windows desktop virtual machines. It is recommended that you include these Windows desktop virtual machines as a part of your VMware security workgroup and protect them with appropriate VMware access controls and monitoring. When implementing Dual Control for Alliance Key Manager be sure that different Crypto Officers are restricted to the appropriate Windows desktop with the AKM Administrative Console and assigned credentials.

Cloud and Hybrid Environments

When deploying Alliance Key Manager as a VMware virtual machine in a cloud environment, be sure to isolate the AKM virtual machine to the specific vCloud Virtual Data Center (vDC). Allowing access to an AKM virtual machine across multiple cloud virtual data centers should only be undertaken after careful consideration of the potential security impacts.

Resources

[Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0]

[PCI DSS Virtualization Guidelines, Version 2.0]

[VMware Solution Guide for PCI]

[VMware PCI DSS 2.0 Validated Reference Architecture]

[VMware Architecture Design Guide for PCI]

[PCI DSS Compliance and VMware by Coalfire]

Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, DIACAP, SOX, and other regulatory compliance requirements.

You can contact Townsend Security for an initial consultation at the following locations:

Web:	www.townsendsecurity.com
Phone:	(800) 357-1019 or (360) 359-4400
International:	+1 360 359 4400
Email:	info@townsendsecurity.com

DISCLAIMER:
THIS DOCUMENT CONTAINS GENERAL GUIDELINES FOR DEPLOYING THE ALLIANCE KEY MANAGER FOR VMWARE SOLUTION AND SHOULD NOT BE CONSTRUED AS A GUARANTEE OF SECURITY OR COMPLIANCE WITH ANY SPECIFIC COMPLIANCE REGULATION. VMWARE IMPLEMENTATIONS VARY A GREAT DEAL AND YOU SHOULD CONSULT WITH A VMWARE SECURITY SPECIALIST AND YOUR COMPLIANCE AUDITOR FOR SPECIFIC GUIDELINES FOR YOUR ENVIRONMENT.