Kuok (Singapore) Limited

KSL VMWare ESXi Hardening Guide

This document provides prescriptive guidance for establishing a secure configuration posture for VMware ESXi 7.0 servers deployed within KSL.

This guide is adapted from the CIS benchmark listed below, incorporating controls that provides adequate security protection without compromising operational stability of the servers. Details about each of the controls listed in the "Controls" tab of this guide, can be found in the CIS benchmark.

CIS VMware ESXi 7.0 Benchmark v1.1.0 (Level 1)

Classification	INTERNAL
Document Reference	
Document Version	1.0
Document Status	FINAL

Authors	
Name	**Title**
Krishna Mohan Singh	Assistant Manager, Infrastructure
Jonathan Ong	General Manager, Cybersecurity

Revision History		
Version	**Date**	**Summary of Changes**
1.0	19-May-23	First Copy

Control No.	Control Name	Baseline	Comments
1.1	1.1 Ensure ESXi is properly patched	Yes	
2.1	2.1 Ensure NTP time synchronization is configured properly	Yes	
2.2	2.2 Ensure the ESXi host firewall is configured to restrict access to services running on the host	Yes	
2.3	2.3 Ensure Managed Object Browser (MOB) is disabled	Yes	
2.5	2.5 Ensure SNMP is configured properly - 'community name public does not exist'	Yes	
2.5	2.5 Ensure SNMP is configured properly - 'community name private does not exist'	Yes	
2.6	2.6 Ensure dvfilter API is not configured if not used	Yes	
2.8	2.8 Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory	Yes	
3.2	3.2 Ensure persistent logging is configured for all ESXi hosts	Yes	
3.3	3.3 Ensure remote logging is configured for ESXi hosts	Yes	
4.2	4.2 Ensure passwords are required to be complex	Yes	
4.3	4.3 Ensure the maximum failed login attempts is set to 5	Yes	
4.4	4.4 Ensure account lockout is set to 15 minutes	Yes	
4.5	4.5 Ensure previous 5 passwords are prohibited	Yes	
4.7	4.7 Ensure only authorized users and groups belong to the esxAdminsGroup group	Yes	
4.8	4.8 Ensure the Exception Users list is properly configured	Yes	
5.1	5.1 Ensure the DCUI timeout is set to 600 seconds or less	Yes	
5.2	5.2 Ensure the ESXi shell is disabled	Yes	
5.3	5.3 Ensure SSH is disabled	Yes	
5.4	5.4 Ensure CIM access is limited	Yes	
5.5	5.5 Ensure Normal Lockdown mode is enabled	Yes	
5.8	5.8 Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less	Yes	
5.9	5.9 Ensure the shell services timeout is set to 1 hour or less	Yes	
5.10	5.10 Ensure DCUI has a trusted users list for lockdown mode	Yes	
6.1	6.1 Ensure bidirectional CHAP authentication for iSCSI traffic is enabled	Yes	
6.3	6.3 Ensure storage area network (SAN) resources are segregated properly	Yes	
7.1	7.1 Ensure the vSwitch Forged Transmits policy is set to reject	Yes	
7.2	7.2 Ensure the vSwitch MAC Address Change policy is set to reject	Yes	
7.3	7.3 Ensure the vSwitch Promiscuous Mode policy is set to reject	Yes	
7.4	7.4 Ensure port groups are not configured to the value of the native VLAN	Yes	
7.5	7.5 Ensure port groups are not configured to VLAN values reserved by upstream physical switches	Yes	
7.6	7.6 Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT)	Yes	
7.7	7.7 Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector	Yes	
7.8	7.8 Ensure port-level configuration overrides are disabled.	Yes	
8.1.1	8.1.1 Ensure informational messages from the VM to the VMX file are limited	Yes	
8.2.1	8.2.1 Ensure unnecessary floppy devices are disconnected	Yes	
8.2.3	8.2.3 Ensure unnecessary parallel ports are disconnected	Yes	
8.2.4	8.2.4 Ensure unnecessary serial ports are disconnected	Yes	
8.2.5	8.2.5 Ensure unnecessary USB devices are disconnected	Yes	
8.2.6	8.2.6 Ensure unauthorized modification and disconnection of devices is disabled	Yes	
8.2.7	8.2.7 Ensure unauthorized connection of devices is disabled	Yes	
8.2.8	8.2.8 Ensure PCI and PCIe device passthrough is disabled	Yes	
8.3.1	8.3.1 Ensure unnecessary or superfluous functions inside VMs are disabled	Yes	
8.3.2	8.3.2 Ensure use of the VM console is limited	Yes	
8.3.3	8.3.3 Ensure secure protocols are used for virtual serial port access	Yes	
8.3.4	8.3.4 Ensure standard processes are used for VM deployment	Yes	
8.4.1	8.4.1 Ensure access to VMs through the dvfilter network APIs is configured correctly	Yes	
8.4.21	8.4.21 Ensure VM Console Copy operations are disabled	Yes	
8.4.22	8.4.22 Ensure VM Console Drag and Drop operations is disabled	Yes	
8.4.23	8.4.23 Ensure VM Console GUI Options is disabled	Yes	
8.4.24	8.4.24 Ensure VM Console Paste operations are disabled	Yes	
8.6.2	8.6.2 Ensure virtual disk shrinking is disabled	Yes	
8.6.3	8.6.3 Ensure virtual disk wiping is disabled	Yes	
8.7.1	8.7.1 Ensure the number of VM log files is configured properly	Yes	
8.7.3	8.7.3 Ensure VM log file size is limited	Yes	