Security Configuration and Hardening Guide

VMware ESXi 8.0.3
VMware vCenter 8.0.3
VMware vSAN 8.0.3

vmware by Broadcom

Table of Contents

Revision History

Date	Description of Change
October 10, 2022	Initial Release for IA (8.0.0): • A “System Design” tab containing security controls that require deeper system design consideration and enablement. • A “Hardware Configuration” tab which has guidance for configuring server hardware. • An “Implementation Priorities” column, a way to help organizations figure out what’s most important so they can do those things first. In general, we’d suggest doing the “P0” things first, “P1” second, and “P2” last. For more information see the “Column Definitions” tab in the spreadsheet. • Updated product defaults. • Updated to reflect industry best practices, such as guidance from NIST 800-63B.
June 13, 2023	Major update for vSphere 8 Update 1 (8.0.1): • New format, single sheet for security controls, with filterable headings. • Inclusion of a second worksheet tab – “Changes Highlighted” – making it easier to see what changed since the last revision. Updated cells appear in yellow. The background table formatting continues to alternate blue & white and does not convey meaning. • Product & Feature mappings to make it easier to consume as we add feature-specific data. • The addition of an “Advanced” implementation priority. This designation gives us the ability to denote new security controls that may have serious operational considerations but are interesting to organizations wishing to pursue deeper security. As these controls mature they will become P0. • Revision of control IDs, descriptions, and discussion to reflect VMware guidelines on use of language, and standardizing on more generic descriptions for commonality with forthcoming regulatory compliance guidance. We apologize to everyone that must update their downstream information. • Addition of mappings to DISA STIG. This is not comprehensive, as DISA has more stringent requirements, but where there is baseline overlap with the STIG it is noted. • Inheritance of some STIG controls. Most notably there are FIPS controls now present in the baseline. We weigh this heavily, because not all organizations require FIPS. However, FIPS support is in many ways synonymous with better TLS cipher suites, which are desirable. Most of these items are enabled by default anyhow, requiring only an audit to confirm. • Removal of the “Removed” tab to avoid confusion. See Appendix A. • Updated PowerCLI examples to correct compatibility with PowerCLI 13.0. • Updated Default and Suggested values to better reflect exactly what the product parameters are. • Updated Security.PasswordHistory guidance to reflect an improved product default of “5” older passwords. • Updates Security.PasswordMaxDays and other password age parameters to “9999” to reflect limits in the UI, while still respecting the spirit of NIST 800-63B. • Host Image Profile Acceptance has returned to “PartnerSupported or Higher.” As long as you are not at CommunitySupported there will be cryptographic protections for ESXi VIBs. • Addition of many more logging parameters. Updated local log storage guidance for discussion about storing data on less-resilient SD and USB flash boot devices. • Addition of deeper guidance for VMware Tools. • Correction of Implementation Priority and Action Needed errata. • Correction of sched.mem.pshare.salt errata, the recommended guidance has been updated. • Addition of VMware.vSphere.SsoAdmin PowerCLI examples where available. • Spreadsheets have been saved as “read only” to prevent inadvertent editing.

September 21, 2023	Update for VMware vSphere 8 Update 2 (8.0.2): • Addition of Solution mapping information, to make it easier to handle VMware product groupings like VMware vSphere (which is a combination of VMware vCenter Server, VMware ESXi, and other components) or VMware Cloud Foundation. • Synchronization of control titles and recommended values, where feasible, with DISA STIG guidance and downstream regulatory compliance guidance. • Expansion of feature-specific guidance. For example, our guidance still recommends not enabling SSH on ESXi, but if you do there are additional controls that should be audited. Auditors who use this guidance should first survey the environment for use of specific features covered by this guide. • Addition of controls present in DISA STIG and downstream regulatory compliance guidance. • Addition of DISA STIG Suggested Values. The DISA STIG, delivered from public.cyber.mil, should always be considered the reference if there is a discrepancy between the guides. • Addition of VMware Configuration ID mappings, to help align downstream regulatory compliance guidance. • Addition of VCF Compatibility information, denoting parameters that should be used with care in a VMware Cloud Foundation environment. • Reintroduction of esxi-8.timekeeping-services, ensuring that timekeeping services such as NTP or PTP are enabled and running, separate from the configuration controls. In general, the approach moving forward is to have one programmatically auditable setting per control. • Reintroduction of esxi-8.ad-auth-proxy. • Addition of "Hardening" to the SCG name. While it will continue to be referred to as the SCG, its name is now the VMware vSphere Security Configuration & Hardening Guide. • Various PowerCLI example updates. Thank you to those who have submitted feedback. • Numerous minor updates for clarity. • Reference to product versions with the build version, such as 8.0.2, versus other names such as "Update 2." • The tables have been fixed so that they sort all columns correctly & together.
September 25, 2023	Minor updates to synchronize 8.0.2 guidance with current 7.0.3 guidance where applicable: • Implementation priority for esxi-8.lockdown-dcui-access & esxi-8.lockdown-exception-users changed to P2 (default configuration is secure). • Implementation priority for vcenter-8.etc-issue changed to P1 to match other login banner guidance (product is secure by default but setting could be improved by the administrator). • Implementation priority for vcenter-8.vami-administration-password-expiration changes to P0 (product default needs to be examined and/or changed). • Feature/component for guest-8.secure-boot changed to Virtual Machine. • Slight wording change to esxi-8.hw-virtual-nic to clarify that it is a virtual NIC between ESXi and the management controller, not the out-of-band management controller NIC. • The Table of Contents page numbers were not accurate in the 802-20230921-01 release.

October 5, 2023	• Introduction of PowerCLI-based auditing tools (see “Tools” directory and PDF). • Addition of a column to show whether the auditing tools check the control. • esxi-8.memeagerzero changed to P0 to reflect threat landscape. • vcenter-8.administration-sso-lockout-policy-unlock-time changed to P0 to reflect threat landscape. • vcenter-8.etc-issue changed to P1 to synchronize with other banners’ priorities. • vcenter-8.vami-administration-password-expiration corrected to P0. • vm-8.deactivate-non-essential-3d-features and vm-8.vmrc-lock defaults corrected for VM Hardware 21 (vmx-21). Older versions of VM Hardware may have other defaults and require auditing. • vcenter-8.network-restrict-discovery-protocol values adjusted to reflect PowerCLI output. • Numerous PowerCLI auditing examples updated to improve formatting and specificity of output. • Assignment of the Apache License, Version 2.0.
August 13, 2024	• Comprehensive revision of auditing tools, and addition of sample remediation scripts. See “Tools” directory and PDF for more information. • Addition of a column to show whether the sample tools remediate the control. • Update of the permalink to https://bit.ly/vcf-scg • Addition of “Changes” tabs to highlight updates to the guidance. • Spreadsheets are no longer read-only, but the sheets are protected. Use “Review -> Unprotect Sheet” to make them editable. There is no password. • Addition of design-8.boot-device to help guide users towards persistent boot volumes which ease logging. • Addition of design-8.native-key-provider to help users understand the tradeoffs between key providers when it comes to physical security. • Addition of design-8.network-isolation-vsan-icsci-target to guide users towards isolation for vSAN iSCSI services. • hw-8.hardware-tpm updated with new PowerCLI assessment capabilities. • Addition of esxi-8.key-persistence. • Separation of functionality between esxi-8.secureboot and a new control, esxi-8.secureboot-enforcement. • Addition of esxi-8.tls-profile. • Deprecation of esxi-8.tls-protocols, largely obsolete now with the new TLS profiles. This control will be removed in a future SCG release. • Modification of esxi-8.tpm-configuration to apply to the “TPM” feature, in an attempt to indicate that it only applies to hosts with TPM capabilities (which is recommended). • Addition of vcenter-8.network-mac-learning. • Addition of vcenter-8.tls-profile. • Addition of vcenter-8.vami-firewall-restrict-access. • Addition of vm-8.efi-boot-types. • Addition of vsan-8.data-at-rest, vsan-8.data-in-transit, vsan-8.file-services-access-control-nfs, vsan-8.file-services-authentication-smb, vsan-8.force-provisioning, vsan-8.iscsi-mutual-chap, vsan-8.object-checksum, vsan-8.operations-reserve. • Updates to numerous PowerCLI examples. • Addition of a column that indicates DISA STIG recommended values. • Addition of a column that indicates whether DISA STIG recommended values exceed that of the SCG. • Addition of a column that indicates PCI DSS 4.0 recommended values. • Addition of a column that indicates whether PCI DSS 4.0 recommended values exceed that of the SCG. • Updates to values in the “VCF Compatible” column.

October 18, 2024	• Update to download URL, license, support, disclaimer, and feedback mechanisms. • Protected the workbook sheets (no password, unprotect with Review -> Unprotect Sheet). • Renaming the documents to remove serial numbers, in favor of Git-based revision control. • Separation of changes from previous major SCG release into their own workbook.

Introduction

The VMware vSphere Security Configuration & Hardening Guide (SCG) is the baseline for hardening and auditing guidance for VMware vSphere itself. It has long served as guidance for virtualization administrators looking to protect their infrastructure.

Security is always a tradeoff, and turning on all security features, to their highest levels of security, often impedes day-to-day administration efforts. The goal of this guide is to be a core set of security best practices that inform administrators. It is not a catalogue of all available security controls, but instead a reasonable baseline on which to build.

Disclaimer

This kit is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided "AS IS." Broadcom makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

This material is provided as is and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright holder or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage. The provider makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of this sample. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations. You acknowledge that there may be performance or other considerations, and that these examples may make assumptions which may not be valid in your environment or organization.

License

What is Included?

The Security Configuration & Hardening Guide is a kit that includes several artifacts:

- VMware vSphere Security Configuration Guide 8 – Guidance.pdf (this document)
- VMware vSphere Security Configuration Guide 8 – Controls.xlsx (spreadsheet with the security hardening baseline controls, discussion, and PowerCLI automation examples for auditing and remediating vSphere objects)
- VMware vSphere Security Configuration Guide 8 – Control Changes.xlsx (spreadsheet noting changes from the last major SCG release)
- A "Tools" directory with sample vSphere auditing scripts, based in VMware PowerCLI (PowerShell), and separate documentation.

Download the Latest Version

This guide was developed with VMware vSphere 8 Update 3 (8.0.3) and supersedes all earlier versions and guidance. We strongly encourage readers to stay current with patches and updates as a major part of a good security posture. The most up-to-date version of this document can be found at:

https://github.com/vmware/vcf-security-and-compliance-guidelines

That link also contains numerous additional resources to help your security and compliance efforts.

Intended Audience

The audience for the vSphere Security Configuration Guide is VMware vSphere customers who have implemented this version of VMware vSphere directly. There are many engineered data center & hybrid cloud infrastructure products that implement VMware vSphere as part of their solutions. If this is how you consume vSphere you should check with those products' support before implementing these ideas.

Future versions of this type of guide will cover VMware Cloud Foundation (VCF) more directly. If you desire VCF guidance now, use the DISA STIG for VMware Cloud Foundation, and only choose the product controls which can be set without editing components inside the virtual appliances.

Additionally the "VCF Compatible" column in this guidance indicates whether a control is compatible with VCF.

VMware Appliances

VMware appliances, such as the vCenter Server Appliance (VCSA), are tested and qualified in known configurations. Altering the configuration of appliances may affect support. Avoid upgrading the appliance virtual hardware versions except under the guidance of VMware Global Support Services.

The VMware vSphere Cluster Services VMs have been hardened with guidance present here and take advantage of vSphere default settings. If your security scanner identifies missing parameters check to ensure that they actually need to be set.

VM Hardware Versions

There are varying opinions within the greater VMware community about upgrading virtual machine hardware versions. Newer virtual machine hardware versions introduce new feature and guest OS support, better compatibility and performance with CPU vulnerability mitigations, better support for modern CPU security features, better security defaults, and so on.

Upgrading virtual machine hardware changes the virtual hardware presented to the guest operating system, just as if a boot device in a physical server was placed in a newer physical server. Changes like this can vary in risk, may require more than one reboot, and may require human interaction to complete.

Note that a virtual machine snapshot will capture the virtual hardware version. This means that reverting a snapshot taken before the upgrade will also revert the virtual hardware version. This makes virtual hardware version upgrades less risky and enables easier testing.

In general, VMware guidance is to:

- Run the latest version you are able, ideally the latest version available in the major vSphere version you run.
- Use VM Hardware 14 (vmx-14) or newer. Version 13 introduces important performance and security improvements for CPU vulnerability mitigations, and version 14 introduces support for vTPM.
- Take snapshots of virtual machines prior to upgrading, but do not forget to remove the snapshot later.
- When scheduling virtual hardware compatibility upgrades use the "Only upgrade after normal guest OS shutdown" to help ensure that a compatibility update does not complicate an unplanned incident or HA event.

Use Your Head!

This guide may be updated as necessary to improve clarity, correct problems, and reflect new and changed functionality within the major version of vSphere 8. While many of the general information security principles are timeless, the technical guidance in this guide should not be applied to versions other than the version it was qualified on. **Even within vSphere 8, many security-related changes have serious consequences for performance, functionality, and usability and should be implemented carefully, with thorough testing, and staged rollouts.**

Power Off

All guidance in the Security Configuration Guide is meant to be applied to virtual machines in a powered off state, or hosts which have been placed in maintenance mode and are able to restart. **Changes to vSphere have made it so that most advanced parameters cannot be set with virtual machines powered on**. This ensures that the running configuration of a virtual machine matches the reported configuration, but in practice may require organizational process changes. We encourage organizations to take advantage of product defaults to reduce the scope of work.

Code Examples & Tools

This Guide contains PowerCLI examples that standardize on formatting, such as:

- $VM is a string containing the virtual machine name,
- $ESXi is a string containing the ESXi host name,
- $VDS is a string containing the Distributed Virtual Switch name,
- $VDPG is a string containing the Distributed Virtual Switch port group name,

These code snippets can make changes that deeply affect operations and the responsibility for the impact of these changes is yours. Test these changes in a controlled, non-production environment first, and apply them to production environments using staged rollout techniques. One easy way to build a test environment is to run ESXi inside a VM for non-production testing purposes, just as the VMware Hands-on Labs do.

The vSphere Security Configuration & Hardening Guide includes sample automation scripts for auditing & remediating environments.

We regret that while we are happy to accept constructive feedback about the code examples, we cannot supply scripting support. There are options for scripting and automation support through VMware Professional Services. Please contact your Account Executive for more information. You might also check out the thriving community at developer.vmware.com.

Alternatively, the “Code Capture” and “API Explorer” features inside the vSphere Client’s Developer Center can be used to discover APIs, help script, and automate tasks. It isn’t perfect, but, in general, if you can do it inside the client, it will give you an example script to automate.

Feedback & Support

Please use the issue tracker in our GitHub repository to submit feedback:

https://github.com/vmware/vcf-security-and-compliance-guidelines/issues

For support, review the policy found at:

https://github.com/vmware/vcf-security-and-compliance-guidelines/blob/main/SUPPORT.md

Thank you.

Appendix A: Removed Controls

The following controls have been removed from this guidance due to changes in industry best practice:

esxi-8.ad-enable: Use Active Directory for ESXi user authentication.

Centralized directories have been a popular target for attacks, and a common path for attackers to move laterally into infrastructure. As a result, VMware's guidance for use of those directories has changed. We no longer suggest joining infrastructure to general-purpose Active Directories in organizations, leaving authentication and authorization as a design decision for individual organizations and environments.

vcenter-8.vami-networking-settings: Remove unnecessary NICs.

This configuration is very uncommon and is difficult to check for programmatically in a meaningful manner. Moved the idea to the System Design group.

vcenter-8.vami-access-dcli: Limit access to vCenter Server by restricting DCLI.

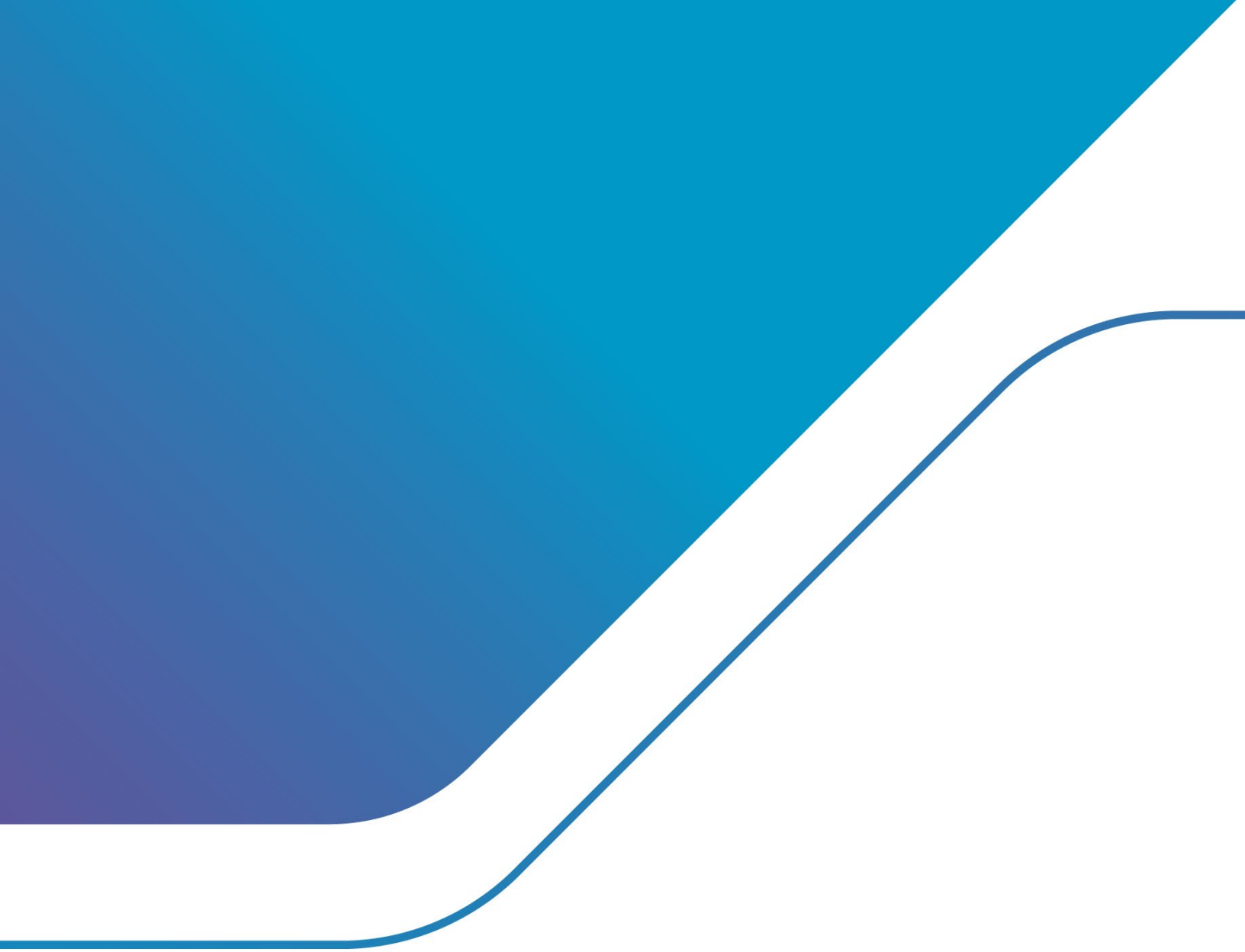
Was a wording error in the VAMI, the control alters the DCUI instead. VAMI was corrected in vSphere 7 Update 3.

vm-8.enable-vga-only-mode: Disable all but VGA mode on specific virtual machines.

Modern guest OSes often use graphics modes beyond VGA in their boot processes. Restricting access to those modes creates unnecessary friction for IT practitioners and limits access to diagnostic information. While there continues to be security merit to disabling 3D functionality when not needed, the return on investment of time and effort for this parameter is very low.

vm-8.isolation-bios-bbs-disable, vm-8.isolation-device-edit-disable, vm-8.isolation-ghi-host-shellAction-disable, vm-8.isolation-tools-dispTopoRequest-disable, vm-8.isolation-tools-getCreds-disable, vm-8.isolation-tools-ghi-autologon-disable, vm-8.isolation-tools-ghi-launchmenu-change, vm-8.isolation-tools-ghi-protocolhandler-info-disable, vm-8.isolation-tools-ghi-trayicon-disable, vm-8.isolation-tools-guestDnDVersionSet-disable, vm-8.isolation-tools-hgfsServerSet-disable, vm-8.isolation-tools-memSchedFakeSampleStats-disable, vm-8.isolation-tools-trashFolderState-disable, vm-8.isolation-tools-unityActive-disable, vm-8.isolation-tools-unity-disable, vm-8.isolation-tools-unityInterlockOperation-disable, vm-8.isolation-tools-unity-push-update-disable,vm-8.isolation-tools-unity-taskbar-disable, vm-8.isolation-tools-unity-windowContents-disable, vm-8.isolation-tools-vixMessage-disable,vm-8.RemoteDisplay-vnc-enabled, vm-8.isolation-tools-setGUIOptions-enable, vm-8.isolation-tools-vmxDnDVersionGet-disable

These parameters are unimplemented in vSphere 7 and newer. VMware does not recommend spending time implementing, maintaining, or auditing guidance that is not applicable to an environment. Some of these parameters do influence operations on VMware Workstation and VMware Fusion, however (such as the “Unity” parameters).



vmware® by Broadcom