2022

A VMsources Whitepaper

VMware vSphere Best Practices

JOHN BORHEK / VMSOURCES

Contents

Introduction

In this Whitepaper I have created a general-purpose Best Practices guideline for VMware vSphere, including references. I base these Best Practices recommendations on my personal, and VMsources collective experience, in dealing with hundreds (if not thousands, at this point) of unique client environments over the last decade.

My intent is to help VMware users of all skills and experience levels avoid some of the "gotcha's" that I have seen, experienced, or heard about from other users.

If you have a Best Practice you would like to see included in this list, or if you feel any of my Best Practices are mis-stated, I welcome input; please contact me by email or phone.

Sincerely,

John Borhek

John Borhek,
Lead Solutions Architect
Email: john@vmsources.com
Website: https://vmsources.com
Mobile: +1 928.606.0483
Office: +1 215.764.6442 X1001

VMware vSphere Best Practices

The DO's

1. DO use a secure password manager to generate and store strong passwords for all your vSphere and Infrastructure assets

2. DO set strong passwords for all your vSphere and Infrastructure host and device accounts (Such as: root, SSO administrator, etc.)

3. DO set vCenter VCSA root and SSO administrator password expiration policy and update the password as specified in that policy.

4. DO configure vCenter VCSA backups using the VAMI backup utility[i]

5. DO configure forward lookup DNS for ESXi Hosts and forward+reverse lookup DNS for vCenter VCSA[ii]

6. DO use DNS to register/access your VMware vSphere assets such as vCenter and ESXi.

7. DO Enable Lockdown Mode on ESXi Hosts.[iii]

8. DO use the ESXi and VCSA firewall to restrict access to specific hosts/networks.[iv] (See: vSphere Firewalls)

9. DO restrict the vSphere Management Network access, allowing only necessary communications (Such as: NTP, AD, Client) to other networks on the Layer 3 firewall/router.[v]

10. DO disable SSH access for the ESXi Hosts and vCenter VCSA whenever not actively using SSH for administration.

11. DO create specific vCenter Roles per required service (Such as: Veeam Backup and Replication), allowing only the specific privilege(s) required by the service and as published by the OEM of the service.[vi]

12. DO create Service Accounts on your authentication directory or SSO for vSphere associated services

13. DO create vCenter Permission(s) associating the service Role with a Service Account, only for the vSphere assets required (Such as: Datacenter, Cluster, Resource Pool, etc.)[vii]

14. DO minimize use of Virtual Machine Remote Console (VMRC) in all forms (Such as: VMRC extension, Web Console) to ONLY when out-of-band access is required for a VM, using in-band access (Such as: RDP, SSH) for all other administrative access to VMs.[viii]

15. DO Configure vCenter VCSA email settings.[ix]

16. DO configure vCenter VCSA alarms with a recipient email address.[x]

17. DO create Customization Specifications for VM Deployment and system preparation.[xi]

18. DO redirect ESXi logfiles to a persistent disk when logs are stored on non-persistent storage[xii]
19. DO create a persistent scratch location[xiii]
20. DO use vNetwork Distributed Switches for VM and Client Networks if they are a licensed feature.
21. DO use VLANs to separate networking on Virtual Switches.[xiv]
22. DO use a minimum of 2 NICs per Virtual Switch
23. DO set virtual Switch Security Policy to reject for Promiscuous Mode, MAC Address Changes, Forged Transmits.[xv]
24. DO use Beacon Probing as a failover detection method only if there are three or more NICs attached to a Virtual Switch.[xvi]
25. DO use VM Templates to deploy prepared "Golden Imaged" when new VMs are required.
26. DO set MAC addressees manually (only if required) using the Edit Settings property of the VM.[xvii]
27. DO use VMware Paravirtualized adapters/drivers such as pvscsi and vmxnet3 wherever possible on VMs.[xviii]
28. DO configure additional virtual SCSI adapters per additional virtual disk (up to 4 SCSI adapters for 4 disks).
29. DO remove unnecessary hardware (Such as: Floppy, CD/DVD, USB) from VM configuration if those devices are not actively being used.
30. DO provision VM Templates as "thin".[xix]
31. DO provision working VMs as either "thin" or "lazy zeroed thick".[xix]
32. DO provision appropriate use-case disks (Such as: Databases, Transaction Logs and Quorum disks) as "Eager-zeroed".[xix]
33. DO enable DRS to Fully Automated (if licensed and available). If automatic migration is not desirable, set the migration slider all the way to "conservative," as this will only allow affinity rules and ESXi host maintenance to take place.
34. DO configure Affinity Rules to separate Domain Controllers where DRS is enabled.[xx]
35. DO create folders to organize VMs and delegate access using Permissions
36. DO create Resource Pools to reserve or limit Compute availability to VMs
37. DO configure HA advanced options to specify at least two additional Isolation Ping Addresses on your vSphere Management Network.[xxi]

38. DO set HA to shut-down VMs in case of ESXi Host isolation (only if you have also set additional HA Isolation Ping Addresses)

39. DO set VM Overrides/VM Restart Priority to prioritize specific VMs (Such as: Domain Controllers).[xxii]

40. DO create separate VMkernel(s) for each service (Such as: Management, iSCSI, vMotion, Fault Tolerance, vSAN)

41. DO use the Software iSCSI adapter/HBA in preference to dedicating a physical NIC to iSCSI as this practice allows for maximum management control.

42. DO implement port-binding when using the Software iSCSI adapter/HBA iSCSI.[xxiii]

43. DO use Jumbo Frames for: iSCSI, vSAN, vMotion, and Fault Tolerance networks/VMkernels.

44. DO test Jumbo Frames wherever in use using the command: `vmkping -I vmk`***`X`*** `-d -s 8972 <IP of target>` [xxiv]

45. DO check the VMware hardware compatibility list: https://www.vmware.com/go/hcl to make sure your hardware is compatible with the version of VMware vSphere you are installing or upgrading to.

46. DO use the OEM Customized Installer CDs for the ESXi ISO specific to your server hardware to install or upgrade ESXi. Vendor-customized ISOs are usually available for: Dell, HPE, Cisco, Lenovo, NEC, Fujitsu and more.

The DO NOT's

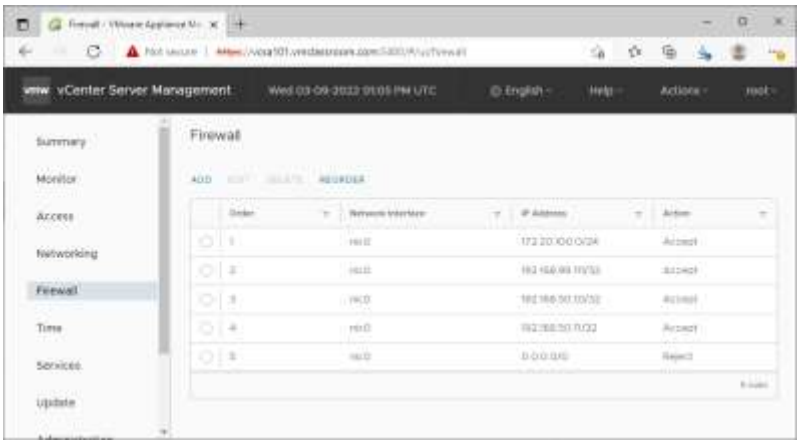
1. DO NOT let root or SSO administrator passwords expire/age out.
2. DO NOT pervasively access vSphere assets using root or SSO administrator accounts.
3. DO NOT use AD or directory access for vSphere assets without multi-factor authentication configured and enforced.
4. DO NOT spoof MAC addresses (if avoidable) using the network driver within the Guest OS of the VM.
5. DO NOT leave removable media devices (Such as: Floppy and CD/DVD) connected to VMs after use.
6. DO NOT place iSCSI or vSAN networks on a vNetwork Distributed Switch if avoidable.
7. DO NOT configure unnecessary CPU or Memory reservations for VMs as that will hinder the ability of other VMs to access resources
8. DO NOT use VM Affinity as a means of load-balancing in a DRS cluster, this defeats the purpose of DRS

vSphere Firewalls

Understanding the vCenter VCSA Firewall

The vCenter VCSA Firewall is configured per IP or Network (USING CIDR Notation) to Accept or Reject all connections. Be sure to define your Accepted connections first.

Example VCSA firewall rules:



This example shows:

- 172.20.100.0/24
  - Accept the entire VMware vSphere management LAN (necessary for communication with ESXi Hosts, VMware components, and backup platforms)
- 192.168.99.111/24
  - Accept a single host IP address on a common network (such one workstation on an office LAN)
- 192.168.50.10/32, 192.168.50.11/32
  - Accept two single host IP addresses on a common network (such as company AD Domain Controllers)
- 0.0.0.0/0
  - Reject all IP addresses not explicitly Accepted above

Understanding the ESXi Firewall

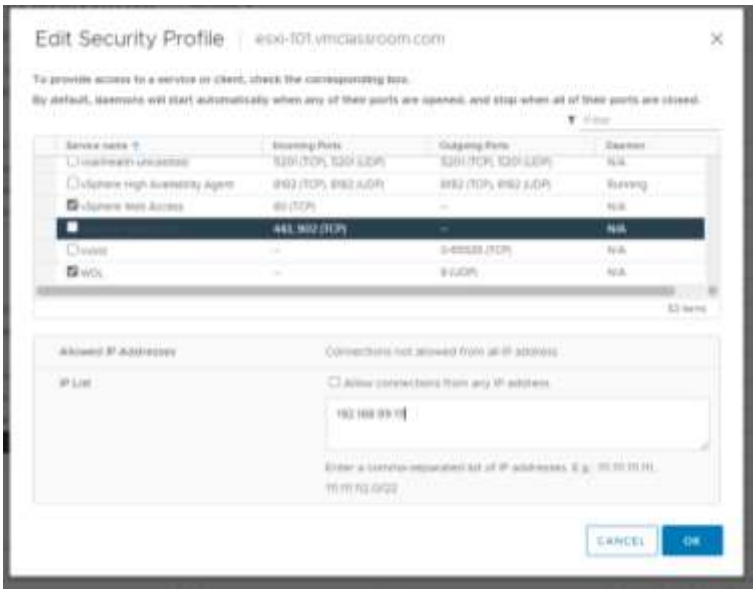
The ESXi Firewall is configured per service. The reality is that, even if your primary connection to vSphere is through vCenter, you still need to enable a couple of rules on the ESXi Firewall because the VMware Remote Console (VMRC) passes directly from the ESXi Host to the **client**.

Services necessary for client communication are: **vSphere Web Client (443,902)** and **SSH (22)** access (only if you plan on enabling SSH from time to time for administrative or support purposes).

You should allow only services necessary for **client** communication to pass from the ESXi Host to authorized administrators.

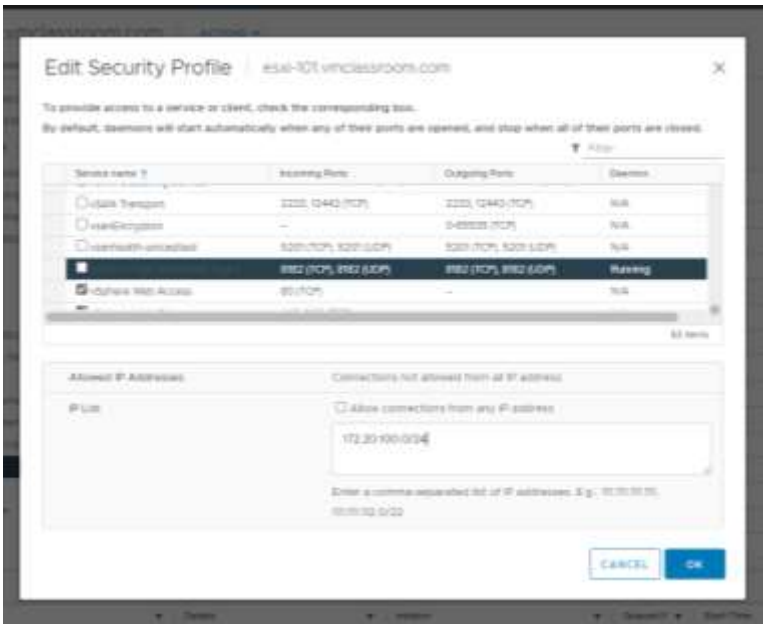
All other enabled services (has a checkbox to the left of the ESXi Firewall rule) should be allowed to the vSphere Management Network, and/or other specific network/Host IP as required by the specific service/group, such as AD or NTP on a per-service/group basis.

Example ESXi Firewall rule for client communication:



Example ESXi Firewall Rule for AD

Example ESXi Firewall rule for vSphere Management Network:



These examples show:

- 192.168.50.10, 192.168.50.11
  - Allow communication with AD Domain Controllers which may not be on the vSphere management network
- 192.168.99.111
  - Allow communication with a single host IP address on a common network (such one workstation on an office LAN)
- 172.20.100.0/24
  - Allow the entire VMware vSphere management LAN (necessary for communication with ESXi Hosts, VMware components, and backup platforms)

Endnotes and References

[i] Back up and restore vCenter Server Appliance/vCenter Server 6.x vPostgres database (vmware.com)

[ii] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-24D34C53-B00E-47B7-92A7-6B0155DF6889.html

[iii] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html

[iv] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9C6D29E6-C58D-4102-9FBA-DC1723E18FE9.html

[v] https://kb.vmware.com/sfc/servlet.shepherd/version/download/068f4000009EghBAAS

[vi] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-93B962A7-93FA-4E96-B68F-AE66D3D6C663.html

[vii] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-5372F580-5C23-4E9C-8A4E-EF1B4DD9033E.html

[viii] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-1D0C095D-0552-42B5-8F01-60ECFFF15833.html

[ix] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenter.configuration.doc/GUID-467DA288-7844-48F5-BB44-99DE6F6160A4.html

[x] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-82933270-1D72-4CF3-A1AF-E5A1343F62DE.html

[xi] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-EB5F090E-723C-4470-B640-50B35D1EC016.html

[xii] System logs are stored on non-persistent storage (2032823) (vmware.com)

[xiii] Creating a persistent scratch location for ESXi 7.x/6.x/5.x/4.x (1033696) (vmware.com)

[xiv] VLAN configuration on virtual switches, physical switches, and virtual machines (1003806) (vmware.com)

[xv] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-62914CF2-A6A8-4DCC-90A9-8CD4BBF50017.html

[xvi] What is beacon probing? (1005577) (vmware.com)

[xvii] Setting a static MAC address for a virtual NIC (219) (vmware.com)

[xviii] Configuring disks to use VMware Paravirtual SCSI (PVSCSI) controllers (1010398)

[xix] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4C0F4D73-82F2-4B81-8AA7-1DD752A8A5AC.html

[xx] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-FF28F29C-8B67-4EFF-A2EF-63B3537E6934.html#:~:text=An affinity rule specifies that,a specific host DRS group.

[xxi] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-E0161CB5-BD3F-425F-A7E0-BF83B005FECA.html

[xxii] Customize an Individual Virtual Machine (vmware.com)

[xxiii] Considerations for using software iSCSI port binding in ESX/ESXi (2038869) (vmware.com)

[xxiv] Testing VMkernel network connectivity with the vmkping command (1003728) (vmware.com)