Zero Trust Scan Report
On Premises EXSi Environment

Scan Date: 2025-07-07
Host: 192.168.0.148

Information

Below are the scan results from the on premises ESXi host(s) analysis. The script performs a number of check to ensure that the infrastructure aligns with the main principle of Zero Trust Architecture. The script verifies the following:

- Network Segmentation
- Encryption of VM's
- SSH and Shell Access
- Lockdown Mode Status
- ESXi Version Complaince
- VM operating System versions
- Firewall ststus
- more

Scan Overview

Resource	Check	Status	Notes
Network Segmentation	Check ESXi VLAN segmentation	Pass	OK
Services Status	SSH & Shell services status	Fail	Needs Review
Lockdown Mode	Host lockdown status	Pass	OK
VM Encryption	VMs encryption check	Fail	Needs Review
ESXi Version	Check ESXi version against latest	Pass	OK
VM OS Info	Unsupported OS versions detection	Pass	OK
ESXi Permissions	Unauthorized full rights check	Pass	OK
Firewall Status	Firewall enabled check	Pass	OK
Log Forwarding	Verify Syslog forwarding	Pass	OK
Check SSH Access Restrictions	Checks if specified users are added to ssh config file to ensure least privilege access	Pass	OK
VM Snapshot Availability	Checks if VM's have snapshots	Pass	OK
SSH Root Login	PermitRootLogin check	Pass	OK
DCUI Shell Access	Verifies if the DCUI account's shell access is disabled	Pass	OK
SSH Banner Content	Verifies a SSH Banner is set to detter attackers	Pass	OK
SSH TCP Forwarding	Checks if SSH TCP forwarding is disabled in the sshd_config file	Pass	OK
ESXI Host Password Complexity Policy	Checks if password complexity polices are set on host.	Pass	OK
ESXI Host Password Expiration Policy	Checks password expiration policy.	Pass	OK

Complaince Percent = 85.0 / 100

Detailed Information

Network Segmentation - Pass

Check: Check ESXi VLAN segmentation

Result: Pass - OK

Details:

Port Group	VLAN ID
Isolation Network	70
ESXi Management	51
Logging	54
File Services	53
Monitoring Services	20
Domain Services	52
Management Network	0

Services Status - Fail

Check: SSH & Shell services status

Result: Fail - Needs Review

Details:

Service	Status
DCUI	True
TSM	False
TSM-SSH	True
attestd	False
dpd	False
kmxd	False
lbtd	True
lwsmd	True
ntpd	True
pcscd	False
ptpd	False
sfcbd-watchdog	False
slpd	False
snmpd	False
vltd	False
vmsyslogd	True
vpxa	False
xorg	False

Lockdown Mode - Pass

Check: Host lockdown status

Result: Pass - OK

Details:

Lockdown Mode	lockdownNormal

VM Encryption - Fail

Check: VMs encryption check

Result: Fail - Needs Review

Details:

Domain Controller 1	Not Encrypted
Ubuntu-Log-Server	Not Encrypted
Wazuh-Siem	Not Encrypted
win-fileserver01	Not Encrypted
VMware vCenter Server	Not Encrypted

ESXi Version - Pass

Check: Check ESXi version against latest

Result: Pass - OK

Details:

ESXi Host Build Number	24585291
Latest ESXI Build	24585291

VM OS Info - Pass

Check: Unsupported OS versions detection

Result: Pass - OK

Details:

Operating System	Supported Status
Microsoft Windows Server 2019 (64-bit)	Supported
Ubuntu Linux (64-bit)	Supported
Other Linux (64-bit)	Supported
Other 3.x or later Linux (64-bit)	Supported

ESXi Permissions - Pass

Check: Unauthorized full rights check

Result: Pass - OK

Details:

User	Access Level
AliceJohnson	Full access rights
dcui	Full access rights
vpxuser	Full access rights

Firewall Status - Pass

Check: Firewall enabled check

Result: Pass - OK

Details:

Firewall Status	Enabled

Log Forwarding - Pass

Check: Verify Syslog forwarding

Result: Pass - OK

Details:

Syslog Forwarding	True
Log Server IP	udp://192.168.0.117:514

Check SSH Access Restrictions - Pass

Check: Checks if specified users are added to ssh config file to ensure least privilege access

Result: Pass - OK

Details:

Username	SSH Status
AliceJohnson	Allowed

VM Snapshot Availability - Pass

Check: Checks if VM's have snapshots

Result: Pass - OK

Details:

VM Name	Snapshot Name
Domain	Snapshots Found
Ubuntu-Log-Server	Snapshots Found
Wazuh-Siem	Snapshots Found
win-fileserver01	Snapshots Found
VMware	Snapshots Found

SSH Root Login - Pass

Check: PermitRootLogin check

Result: Pass - OK

Details:

SSH Root Login	Disabled

DCUI Shell Access - Pass

Check: Verifies if the DCUI account's shell access is disabled

Result: Pass - OK

Details:

dcui_shell	/sbin/nologin
dcui_shell_access	Disabled

SSH Banner Content - Pass

Check: Verifies a SSH Banner is set to detter attackers

Result: Pass - OK

Details:

Enabled	Yes
Banner Content	********** * Unauthorized access to this system is forbidden * * and will be prosecuted. All activity is monitored. * * Zero Trust Policy in Effect. * **********

SSH TCP Forwarding - Pass

Check: Checks if SSH TCP forwarding is disabled in the sshd_config file

Result: Pass - OK

Details:

AllowTcpForwarding	no
Status	Enabled (Non-compliant)

ESXI Host Password Complexity Policy - Pass

Check: Checks if password complexity polices are set on host.

Result: Pass - OK

Details:

Password Complexity Status	Required Password Length
True	12

ESXI Host Password Expiration Policy - Pass

Check: Checks password expiration policy.

Result: Pass - OK

Details:

Username	Password Expires after x days
root	60
dcui	60
vpxuser	60
ciaran	60
AliceJohnson	60
BrandonFoster	60
CharlieDavis	60
CindyMorris	60
FionaMartin	60
IanThompson	60
OscarRamirez	60
PatriciaScott	60
QuintinBrooks	60
StephenHarris	60
TinaEdwards	60

Recommendations

Some areas passed, while others may need attention. Maintaining ESXi security under Zero Trust requires ongoing validation. Based on current scan results, the following improvements are recommended:

- Ensure VM encryption is enabled to protect data at rest.
- Verify ESXi VLAN segmentation to prevent lateral movement between environments.
- Restrict SSH access to authorized users only using the `AllowUsers` directive.
- Ensure SSH banners are configured to display legal warning messages.
- Enable and forward logs to a central syslog server for auditing and incident response.
- Ensure firewall service is running and unnecessary services like SLPD and SSH are disabled when not in use.
- Check that all ESXi hosts are running supported versions with recent security patches.
- Verify strong password complexity policies are in place and account lockout settings are enforced.
- Ensure DCUI and root shell access are properly restricted to reduce local attack surface.

Azure Security Report

Scan Date: 2025-07-07
Azure Subscription: 38915259-0faa-4784-a49a-5b4fcd1ef2b6

Information

Below are the scan results from the Azure Cloud Environment analysis. The script performs a number of check to ensure that the cloud infrastructure aligns with the main principle of Zero Trust Architecture. The script verifies the following:

- Network Segmentation
- Encryption of VM's
- Evaluates Network Security Groups
- Verifies whether Azure Backups are enabled
- Checks for exposed via public IPs
- Reviews deployment of Azure Firewall and Azure Bastion
- Assesses role assignments
- Checks whether VMs have inbound service ports open
- Checks if VNet encryption is enabled
- Analyzes group memberships
- Confirms that the number of subscription owners

Scan Overview

Resource	Check	Status	Notes
Network Segmentation	Check if VNets are segmented	Pass	OK
NSG Rules	Check for overly permissive NSG rules	Pass	OK
Azure Backups	Checks if Azure backups are configured for VM's	Pass	OK
VM Encryption	Check if VMs have encryption at host enabled	Pass	OK
Public IP Exposure	Check for public IPs assigned to resources	Fail	Needs Review
Azure Firewall	Check if Azure Firewall is deployed for perimeter security	Pass	OK
Azure Bastion	Check if Azure Bastion is deployed for secure access	Pass	OK
Over permissive Owne Role	Checks if Owner role is assigned outside the subscription scope	Pass	OK
Key Vault Security	Check Key Vault RBAC, Soft Delete, and Purge Protection	Pass	OK
VM Inbound NSG Rules	Checks if VM's have service ports open for all inbound IP addresses	Pass	OK
Azure Snapshots	Checks if snapshots are taken of VM's	Pass	OK
VNet Encryption	Check if VNets and peerings have encryption enabled	Pass	OK
Subsctiption Owners	Checks the number of owners on the subscription, Microsoft recommends less than 3	Pass	OK
Group Membership	Check if users belong to too many groups	Pass	OK

Azure Complaince Percent = 93.0 / 100

Extra Details

Network Segmentation - Pass

Check: Check if VNets are segmented

Result: Pass - OK

Details:

Name	Address
HubVnet	['10.0.0.0/24']
GatewaySubnet	['10.0.0.0/27']
AzureBastionSubnet	['10.0.0.128/26']
AzureFirewallSubnet	['10.0.0.192/26']
AzureFirewallManagementSubnet	['10.0.0.64/26']
Production-VNET	['10.4.0.0/16']
default	['10.5.0.0/24']
Isolation-Subnet	['10.5.1.0/29']
Testing-VNET	['10.5.0.0/16']

NSG Rules - Pass

Check: Check for overly permissive NSG rules

Result: Pass - OK

Details:

nsg-hub	['Allow-VPN | Src: 192.168.0.0/24 | Dest: * | Proto: Tcp | Access: Allow']
Isolation-NSG	['Allow-SSH-From-Admin | Src: 192.168.0.194 | Dest: * | Proto: Tcp | Access: Allow', 'Deny-All-Inbound | Src: * | Dest: * | Proto: * | Access: Deny', 'Deny-All-Outbound | Src: * | Dest: * | Proto: * | Access: Deny']
nsg-production-server02	['Allow-Bastion-RDP | Src: VirtualNetwork | Dest: * | Proto: Tcp | Access: Allow', 'Allow-Wazuh-1514 | Src: 192.168.0.151 | Dest: * | Proto: Tcp | Access: Allow', 'Allow-Wazuh-1515 | Src: 192.168.0.151 | Dest: * | Proto: Tcp | Access: Allow', 'Deny-All-Inbound | Src: * | Dest: * | Proto: * | Access: Deny']
nsg-testing-kali01	['Allow-Bastion-SSH | Src: VirtualNetwork | Dest: * | Proto: Tcp | Access: Allow', 'Allow-Wazuh-1514 | Src: 192.168.0.151 | Dest: * | Proto: Tcp | Access: Allow', 'Allow-Wazuh-1515 | Src: 192.168.0.151 | Dest: * | Proto: Tcp | Access: Allow', 'Deny-All-Inbound | Src: * | Dest: * | Proto: * | Access: Deny']

Azure Backups - Pass

Check: Checks if Azure backups are configured for VM's

Result: Pass - OK

Details:

VM Name / Resource Group	Backup Vault Name
azure-production-server02 / RG-PROD-VMS	vault114"
azure-testing-kali01 / RG-TEST-VMS	vault114"

VM Encryption - Pass

Check: Check if VMs have encryption at host enabled

Result: Pass - OK

Details:

RG-PROD-VMS/azure-production-server02	Encrypted
RG-TEST-VMS/azure-testing-kali01	Encrypted

Public IP Exposure - Fail

Check: Check for public IPs assigned to resources

Result: Fail - Needs Review

Details:

Resource Name:	IP address / Resource Group
firewall-ip	74.162.192.248 : HubSpoke-RG
Gub-gateway-publicip	74.243.247.177 : HubSpoke-RG
HubVnet-ip	20.233.231.247 : HubSpoke-RG
managment-ip	40.120.122.21 : HubSpoke-RG

Azure Firewall - Pass

Check: Check if Azure Firewall is deployed for perimeter security

Result: Pass - OK

Details:

Name	Location
Firewall-Hub	uaenorth

Azure Bastion - Pass

Check: Check if Azure Bastion is deployed for secure access

Result: Pass - OK

Details:

Bastion Name	Location
bastionHub	uaenorth

Over permissive Owne Role - Pass

Check: Checks if Owner role is assigned outside the subscription scope

Result: Pass - OK

Details:

obrienciaran4_gmail.com#EXT#@obrienciaran4gmail.onmicrosoft.com	Owner on /subscriptions/38915259-0faa-4784-a49a-5b4fcd1ef2b6
ajohnson@obrienciaran4gmail.onmicrosoft.com	Owner on /subscriptions/38915259-0faa-4784-a49a-5b4fcd1ef2b6

Key Vault Security - Pass

Check: Check Key Vault RBAC, Soft Delete, and Purge Protection

Result: Pass - OK

Details:

Vault name	Key-Vault-VMs-Zero-Trust
RBAC Status	True
Soft Delete name	True
Purge Proetction	True

VM Inbound NSG Rules - Pass

Check: Checks if VM's have service ports open for all inbound IP addresses

Result: Pass - OK

Details:

VM Name / NSG	Open Port / Source
azure-production-server02 / nsg-production-server02	Restricted
azure-testing-kali01 / nsg-testing-kali01	Restricted

Azure Snapshots - Pass

Check: Checks if snapshots are taken of VM's

Result: Pass - OK

Details:

VM Name/Resource Group	Snapshot Ststus / Name
azure-production-server02 : RG-PROD-VMS	True :HealthySnapshot-070725
azure-testing-kali01 : RG-TEST-VMS	True :HealthySnapshot-070725

VNet Encryption - Pass

Check: Check if VNets and peerings have encryption enabled

Result: Pass - OK

Details:

VNET Resource	Encryption Status
HubVnet	Enabled
hub-topro	Enabled
hub-to-test	Enabled
Production-VNET	Enabled
hub-to-prod	Enabled
Testing-VNET	Enabled
hub-totest	Enabled

Subsctiption Owners - Pass

Check: Checks the number of owners on the subscription, Microsoft recommends less than 3

Result: Pass - OK

Details:

Username	Admin Role
obrienciaran4_gmail.com#EXT#@obrienciaran4gmail.onmicrosoft.com	Owner
ajohnson@obrienciaran4gmail.onmicrosoft.com	Owner

Group Membership - Pass

Check: Check if users belong to too many groups

Result: Pass - OK

Details:

Username	Group Memberships
Alice Johnson	['ZTA_IT_Admins']
Bob Smith	['ZTA_Azure_Admins']
Charlie Davis	['ZTA_RemoteDesktopUsers', 'ZTA_Network_Team']
Danielle Williams	['ZTA_ESXi_Admins']
Edward Brown	['ZTA_Security_Team']
Fiona Martin	['ZTA_Systems_Team']
George Lee	['ZTA_DevOps_Team']
Kevin Martinez	['ZTA_App_Developers']

Recommendations

Some areas passed, some could use a bit of fixing.

- Deploy Azure Firewall to enforce perimeter-level traffic control.
- Enable Azure Bastion for secure, browser-based RDP/SSH access to VMs.
- Implement regular snapshot/backup policies for critical virtual machines.
- Enable VM and VNET Encryption
- Limit permissions of users, ensuring principle of least privilege
- Implement Network Segmentation across all resources
- Implement NSG's to further protect resources