



REPORT

Enterprise Hybrid-Cloud Migration

v1.2.0

Author:

Eldon Gabriel

March 18, 2026



TABLE OF CONTENTS

REVISION HISTORY	2
Project Showcase: Enterprise Hybrid-Cloud Migration	3
Executive Summary.....	3
1.0 PHASE 1: NETWORK & ENVIRONMENT SETUP	5
1.1 Build the Domain Controller & NAT Gateway.....	5
1.2 Establish DNS Source of Truth.....	6
1.3 DNS Manager Records (Forward & Reverse Zones).....	7
1.4 ESXi01 VM Deployment.....	8
1.5 ESXi01 Licensing & Resource Validation.....	9
1.6 VCSA01 VM Deployment.....	10
1.7 DC2001 and WS01 Deployment.....	11
1.7.1 DC2001 VM Deployment.....	12
1.7.2 WS01 VM Deployment.....	13
1.7.3 Deployment Verification and Validation of VMs.....	14
1.8 Centralized VCSA Management.....	15
1.8.1 Stage 1: Deployment Configuration.....	15
1.8.2 Stage 1 Configuration and Validation.....	17
1.8.3 Stage 2: Single Sign-On (SSO) Setup.....	18
1.8.3 Deployment Verification and Validation of VCSA.....	19
2.0 PHASE 2: AWS MGN SETUP & MIGRATION	20
2.1 Migration Workflow.....	20
2.2 Migration Test Launch & Visual Validation.....	21
2.3 Launch Settings & Conflict Resolution.....	21
2.4 Migration Test Launch & Visual Validation.....	21
2.5 Target Instance Verification (Screenshot Capture).....	22
2.5.1 Deployment Verification and Validation of DC2001 Instance.....	22
2.5.2 Deployment Verification and Validation of WS01 Instance.....	23
3.0 PHASE 3: FAILBACK & STRESS TEST RCA	24
3.1 Dimensional Analysis.....	24
3.2 Diagnostic Validation and Resolution Steps.....	24
4.0 APPENDIX: LAB QUICK REFERENCE	25
4.1 Lab Architecture Topology.....	25
4.2 Table 1 – Technical Abbreviations & Glossary.....	26
4.3 Table 2 – Lab Inventory & Identity.....	26

Disclaimer: This document records the author’s independent completion of the MCSI laboratory exercise program. This reflects the author’s understanding and work performed in a controlled laboratory environment. No MCSI video content, proprietary laboratory materials, or restricted instructions were included. All the information presented complies with MCSI’s academic integrity and disclosure policies.



Security Systems Specialist

REVISION HISTORY

Version	Date	Author	Description of Changes
1.0.0	03/07/2026	Eldon G.	Initial draft.
1.1.0	03/08/2026	Eldon G.	Updated document hierarchy to standard decimal numbering and added post-migration recovery RCA to the appendices.
1.2.0	03/18/2026	Eldon G.	Refined network hierarchy; updated Lab Gateway logic; and added Root Cause Analysis (RCA) regarding HAL failure and kernel driver remediation.





Security Systems Specialist

Project Showcase: Enterprise Hybrid-Cloud Migration

Author: Eldon Gabriel

Role: Security Systems Specialist

Project Scope: VMware On-Premises to Amazon Web Services (AWS) Migration

Executive Summary

This project details end-to-end migration of Windows Server workloads from a virtualized **on-premises** environment to **Amazon Web Services (AWS)**. Utilizing the **AWS Application Migration Service (MGN)**, the project successfully executed block-level replication of two virtual machines (VMs): a Domain Controller and a Windows Server workstation.

The environment was built under real-world hardware constraints, specifically a 32 GB Random Access Memory (RAM) limit, necessitating a low-overhead architecture using nested virtualization. This phase concluded with a **proof-of-concept (PoC)** validation, in which successful migration was verified via direct instance access rather than a live network traffic cutover. Following verification, AWS replication components and drivers were manually removed to trigger a stress-test failure for Root Cause Analysis (RCA).

Key Technical Achievements

- I. **PowerShell Automation:** Automated the **Domain Name System (DNS)** "Source of Truth" and Active Directory environment using PowerShell scripts to ensure resolution accuracy for vCenter Stage 1 validation.
- II. **Network Engineering:** Configured a Windows Server with NAT (RRAS) to provide outbound connectivity to bridge isolated private network segments with the AWS Public Cloud and managed routing tables and firewall rules.
- III. **Advanced Troubleshooting:** Diagnosed and bypassed agent-level file locks by performing manual ownership takeovers and registry purges in Safe Mode.
- IV. **FinOps and Resource Hygiene:** Successfully identified and reclaimed over 300 orphaned AWS resources following a transformation failure and achieved near zero resource waste during lab cleanup



Security Systems Specialist

This project was originally based on a VMware-to-AWS migration exercise referencing the AWS Server Migration Service (SMS). However, as SMS has been deprecated, this implementation uses the AWS Application Migration Service (MGN), the current AWS-recommended solution for lift-and-shift migrations. The workflow preserves the original lab objectives while aligning with modern cloud migration practices.





Security Systems Specialist

1.0 PHASE 1: NETWORK & ENVIRONMENT SETUP

Goal: Establish the `192.168.10.x` network with DC01 as the primary Gateway (.2).

1.1 Build the Domain Controller & NAT Gateway

Purpose: To deploy infrastructure anchor. DC01 provides Active Directory Domain Services (ADDS), DNS resolution, and NAT routing for all subsequent migration targets.

DC01 Resource Allocation

- **CPU:** 2 vCores
- **RAM:** 1.5 GB (Dynamic Memory enabled)
- **Disk:** 64 GB
- **Static IP:** 192.168.10.2

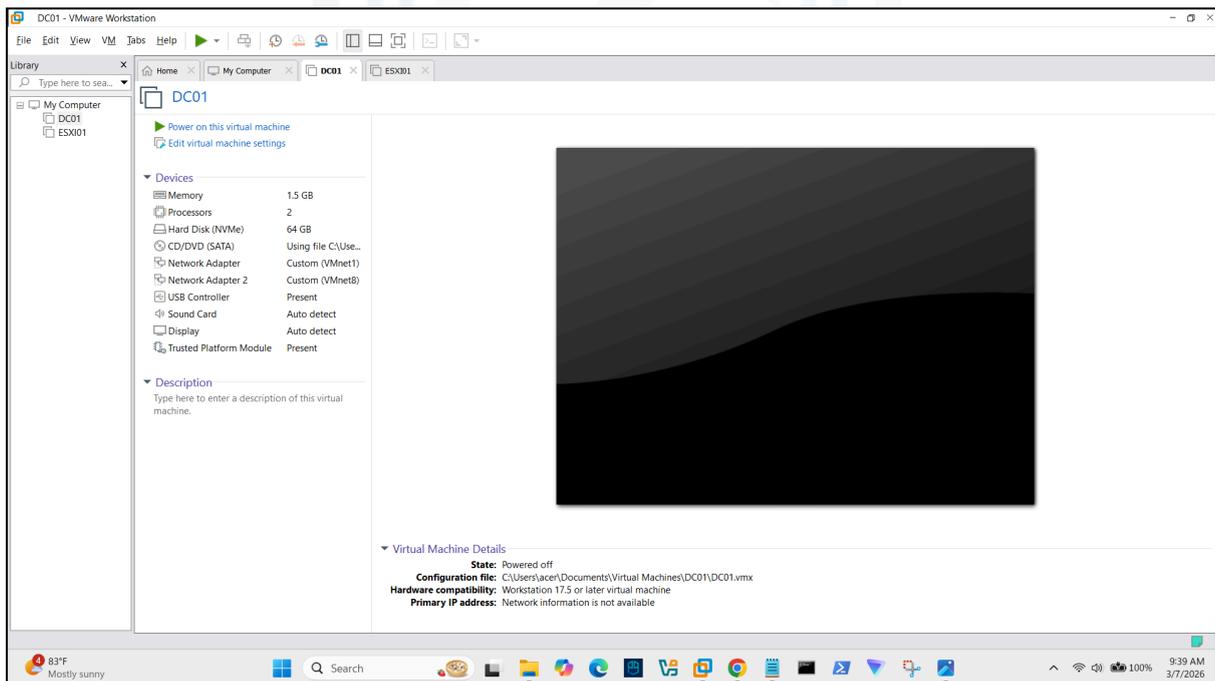


Figure 1: WS 2019 DC01 nested on VMware Workstation. March 7, 2026. Eldon G.



Security Systems Specialist

1.2 Establish DNS Source of Truth

Purpose: To ensure that the vCenter Server Appliance and ESXi host communicate via a Fully Qualified Domain Name (FQDN), DNS was configured with forward (A) and reverse (PTR) static records.

Hostname	IP Address	Record Type	Function
dc01.corp.internal	192.168.10.2	A / PTR	Primary DNS / Gateway
esxi01.corp.internal	192.168.10.130	A / PTR	Nested Hypervisor
vcsa01.corp.internal	192.168.10.30	A / PTR	Management Appliance
dc2001.corp.internal	192.168.10.10	A / PTR	Migration Workload 1
ws01.corp.internal	192.168.10.51	A / PTR	Migration Workload 2





Security Systems Specialist

1.3 DNS Manager Records (Forward & Reverse Zones)

Purpose: Configure authoritative DNS and PTR records to ensure hostname resolution for all laboratory components. This is required for the VCSA Stage 1 deployment, as missing A and PTR records will cause FQDN validation to fail (see Figures 2-3).

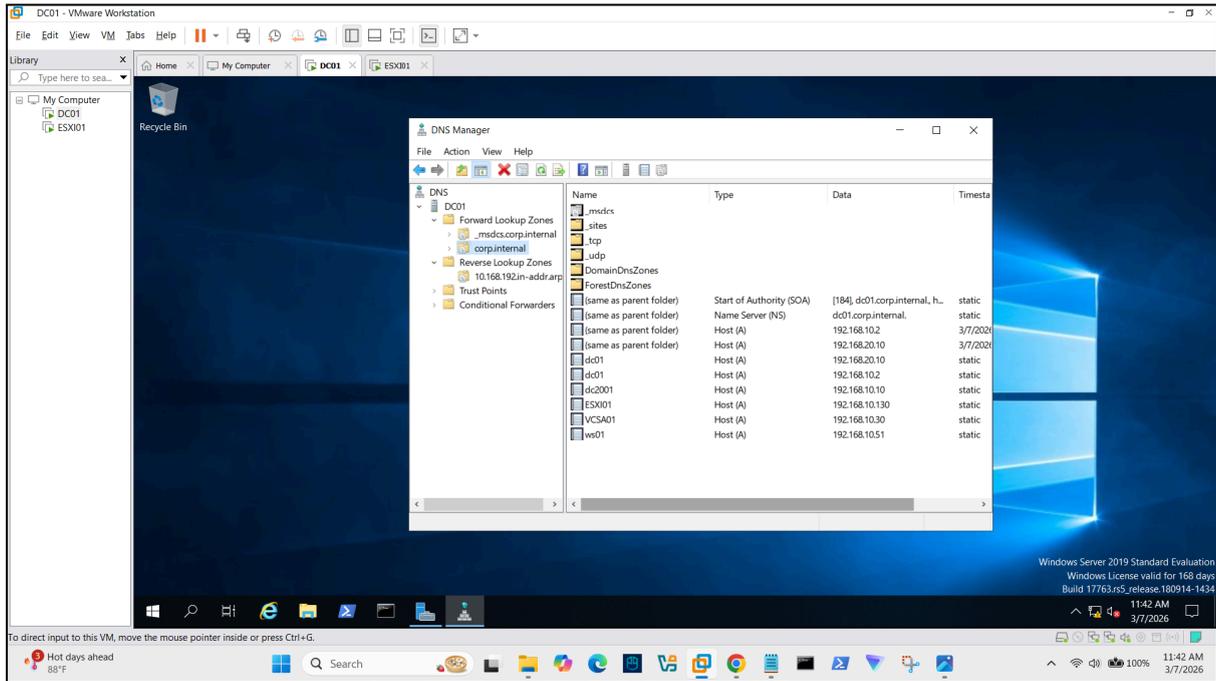


Figure 2: DC01 DNS Manager Forward Lookup Zone. March 7, 2026. Eldon G.

ELDON GABRIEL

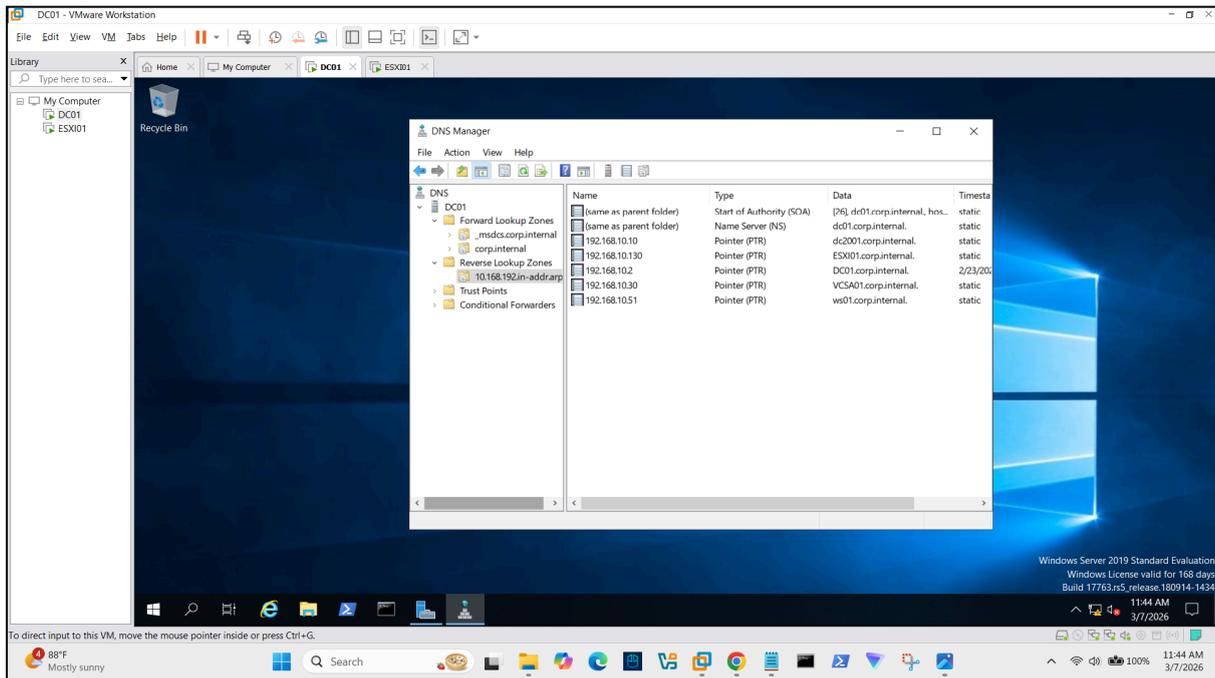


Figure 3: DC01 DNS Manager Reverse Lookup Zone. March 7, 2026. Eldon G.

1.4 ESXi01 VM Deployment

Purpose: To create a nested environment to host VCSA01's Centralized VCSA Management as a virtualized OS. This management plane hosts the DC2001 and WS01 VMs (see Figure 4).

ESXi01 Resource Allocation:

- **CPU:** 4 vCores
- **RAM:** 10.6 GB (Dynamic Memory enabled)
- **Disk:** 300 GB
- **Static IP:** 192.168.10.130



Security Systems Specialist

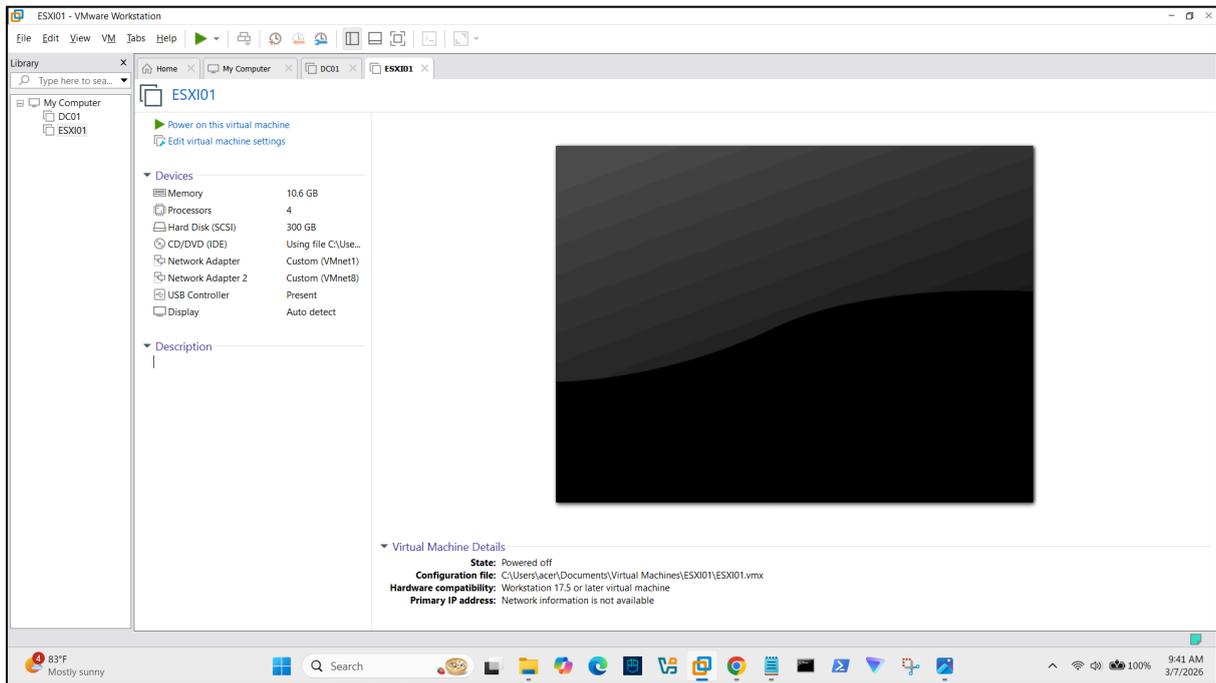


Figure 4: ESXi01 nested in the VMware Workstation. March 7, 2026. Eldon G.





Security Systems Specialist

1.5 ESXi01 Licensing & Resource Validation

Purpose: Activate the ESXi01 hypervisor to unlock the advanced features required for vSphere communication and ensure that the host is ready to receive the VCSA VM (see Figure 5).

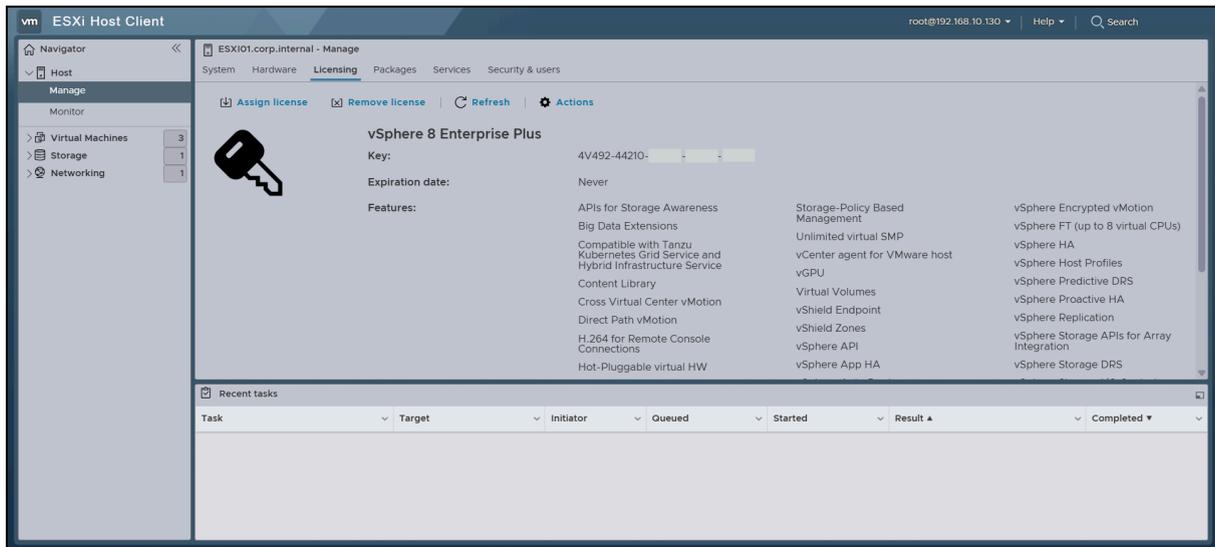


Figure 5: ESXi01.corp.internal > Manage > Licensing UI. March 5, 2026. Eldon G.





Security Systems Specialist

1.6 VCSA01 VM Deployment

Purpose: To deploy the VCSA01 VM to act as the hardware provider for both DC2001 (ADDS) and WS01 (Windows 10 Workstation) (**see Figure 6**).

Resource Allocation:

- **CPU:** 4 vCores
- **RAM:** 10.6 GB (Dynamic Memory enabled)
- **Disk:** 300 GB
- **Static IP:** 192.168.10.130

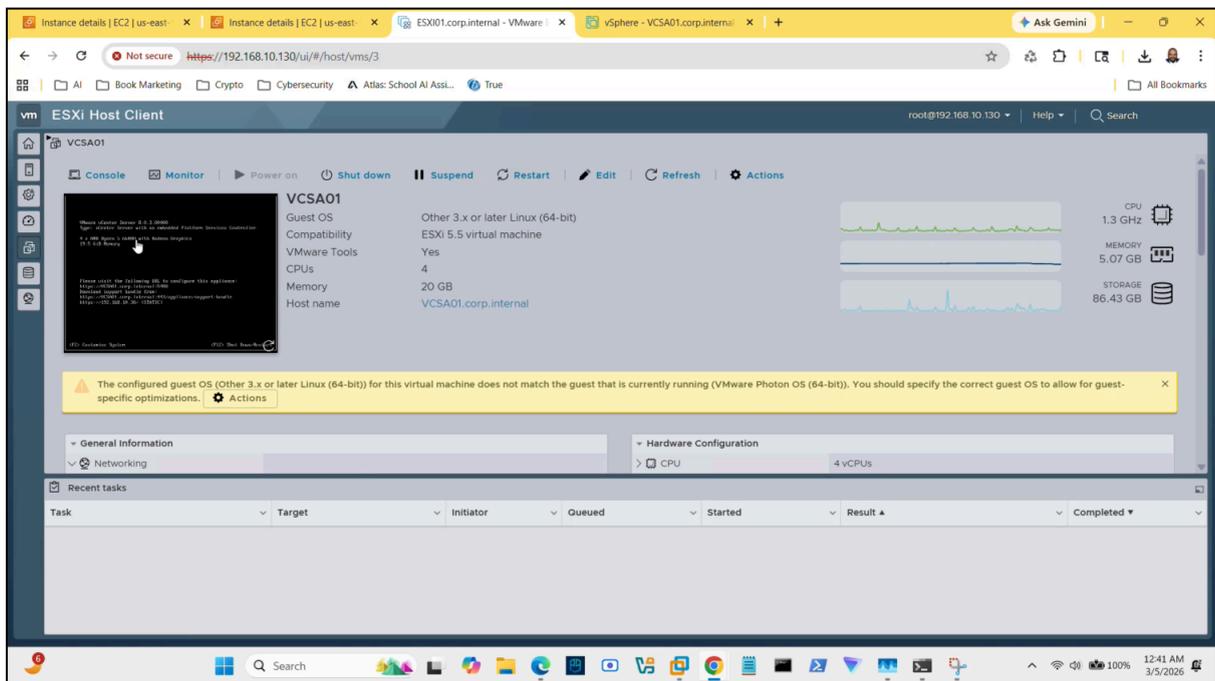


Figure 6: VCSA01 nested on ESXi01.corp.internal UI. March 5, 2026. Eldon G.



1.7 DC2001 and WS01 Deployment

To finalize the local infrastructure setup, existing VMs were created and hosted in the ESXi01's inventory (**See Figure 7, 8 & 9**). This established the centralized management plane required by the AWS MGN replication agent.

Pre-Migration Inventory and Target Mapping

The following table defines the local source workloads and maps them to their designated target identities for the upcoming AWS migration phase.

Source Workload (VMware)	Planned Target (AWS EC2)	Local IP Address	Primary Role
DC2001	DC2001	192.168.10.10	Replicated Active Directory Domain Controller
Workstation-01	WS01	192.168.10.51	Replicated Windows Server Workload

1.7.1 DC2001 VM Deployment

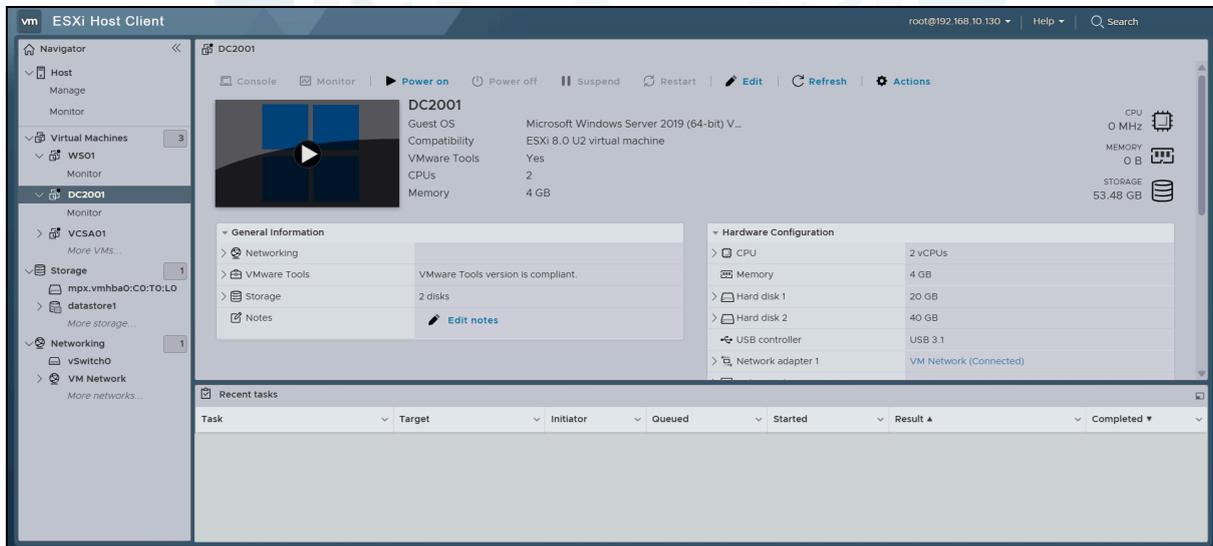


Figure 7: DC2001 nested on ESXi01.corp.internal UI. March 5, 2026. Eldon G.

DC2001 Resource Allocation

- **CPU:** 2 vCores
- **RAM:** 4 GB
- **Disk:** 60 GB
- **Static IP:** 192.168.10.10



Security Systems Specialist

1.7.2 WS01 VM Deployment

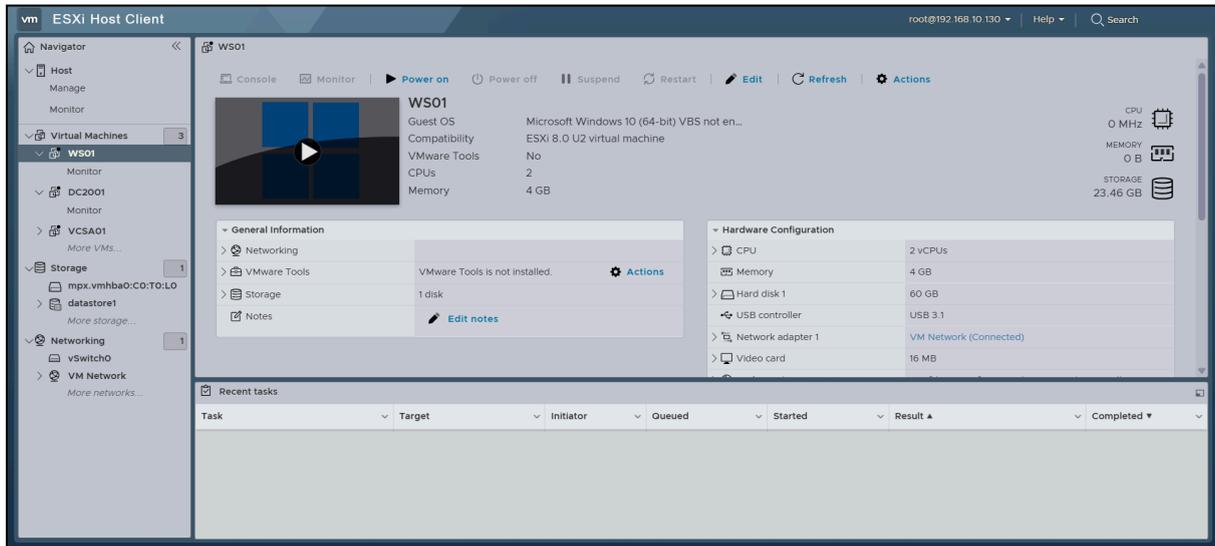


Figure 8: WS01 nested on ESXi01.corp.internal UI. March 5, 2026. Eldon

WS01 Resource Allocation

- **CPU:** 2 vCores
- **RAM:** 4 GB
- **Disk:** 60 GB
- **Static IP:** 192.168.10.51

ELDON GABRIEL



Security Systems Specialist

1.7.3 Deployment Verification and Validation of VMs

Purpose: All vCenter Server components must have proper DNS records before deployment. Both A and PTR records are required for all VMs to enable the system to correctly resolve hostnames and IP addresses. If DNS is not configured properly, the installation may fail, especially during FQDN validation.

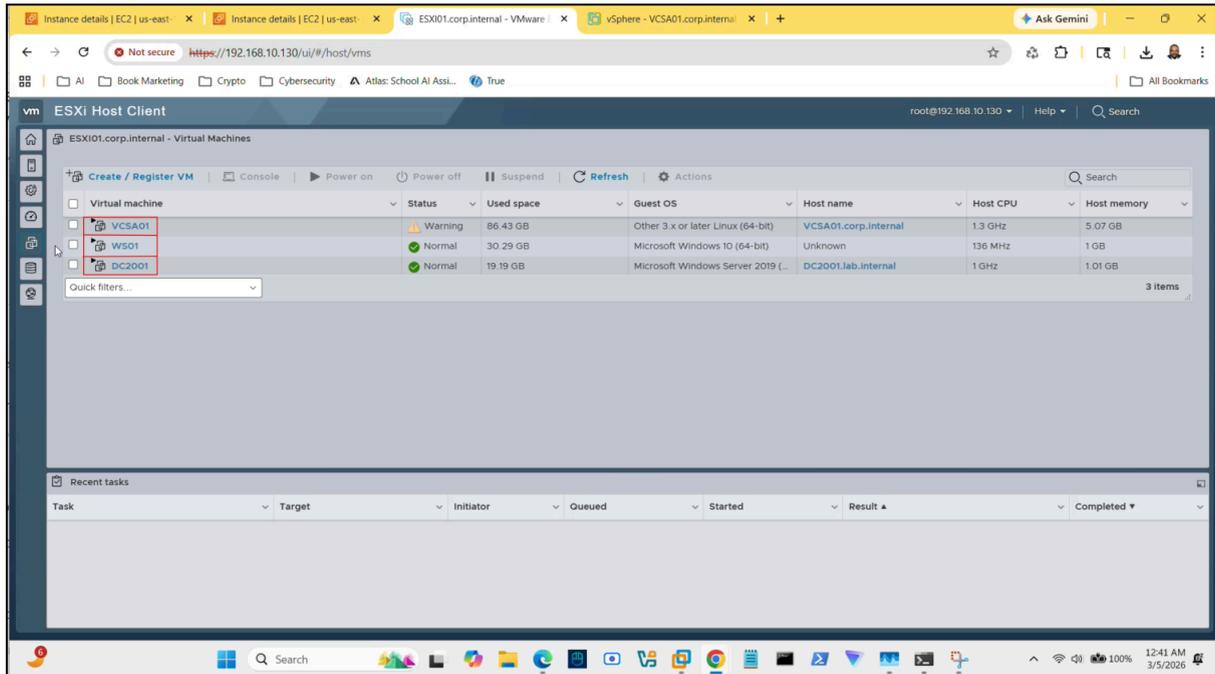


Figure 9: ESXi01.corp.internal–Virtual Machines UI. March 5, 2026. Eldon G.

ELDON GABRIEL



Security Systems Specialist

1.8 Centralized VCSA Management

Purpose: Deploy VCSA01 server to act as a virtualized OS. This appliance orchestrates ESXi01 hosts and provides the necessary Application Programming Interface (API) endpoints for the AWS Replication Agent.

1.8.1 Stage 1: Deployment Configuration

Installer Execution

- I. Mount and a VCSA `.iso` on ESXi01 UI.
- II. Navigate to the drive folder and execute installation.
- III. Click **Install** to begin Stage 1 Deployment.

Appliance Deployment Target:

- I. **ESXi host:** `192.168.10.130`
- II. **User name:** `root`
- III. **Password:** *(Your ESXi01 root password)*
- IV. Acceptance of the certificate thumbprint.

Appliance VM Settings

- I. **VM Name:** `VCSA01`
- II. **Password:** *(Establish VCSA root password for VAMI access)*

Deployment Size:

- I. **Size:** `Tiny`
- II. **Storage size:** `Default`

Datstore:

- I. Select the local ESXi datstore.
- II. Check whether `Enable Thin Disk Mode` is enabled. (saves **NVMe** space).



Security Systems Specialist

Network Settings:

- I. **Network:** VM Network
- II. **IP version:** IPv4
- III. **IP assignment:** Static
- IV. **FQDN:** VCSA01.corp.internal
- V. **IP address:** 192.168.10.30
- VI. **Subnet mask:** 255.255.255.0
- VII. **Default gateway:** 192.168.10.2
- VIII. **DNS servers:** 192.168.10.2

Click **Finish** and wait for Stage 1 to complete.





Security Systems Specialist

1.8.2 Stage 1 Configuration and Validation

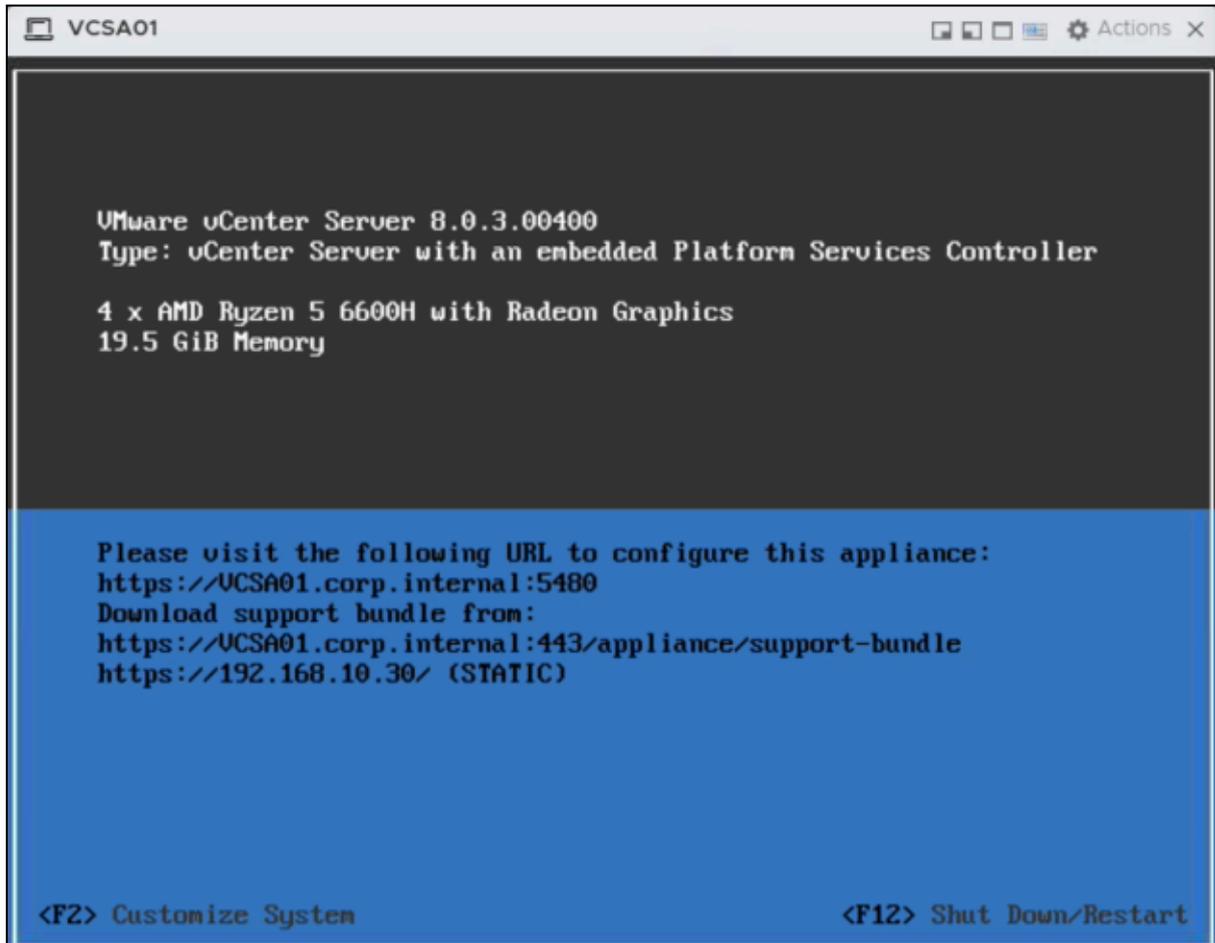


Figure 10: VCSA01.corp.internal - vCenter Server. March 5, 2026. Eldon G.

Target: `VCSA01.corp.internal:5480`

Action:

- I. Open a browser and navigate to `https://192.168.10.30:5480`
- II. Log-in as `root`.
- III. Go to **Networking** -> **Edit**.
- IV. Change the Default Gateway to `192.168.10.2`
- V. Save and verify Internet egress.

I verified the following before proceeding to Stage 2:



Security Systems Specialist

- I. **Internet Egress:** Successful `ping` of `google.com` from VAMI SecureShell.
- II. **DNS Resolution:** Successful `nslookup google.com` returned an IP address of `192.168.10.2`.
- III. **Endpoint Reachability:** `Test-NetConnection mgn.us-east-1.amazonaws.com -Port 443` returned `TcpTestSucceeded: True`
- IV. **Time Sync:** Confirmed that all VMs exactly matched the OS real-world time. If the clocks are not in sync, security checks such as SSL certificates and login tokens can fail.

1.8.3 Stage 2: Single Sign-On (SSO) Setup

After Stage 1 is completed, click on **Continue** to start Stage 2.

SSH access: `Enabled`

SSO Configuration:

- I. Create a new SSO domain.
- II. **SSO domain name:** `vsphere.local`
- III. **SSO user name:** `administrator`
- IV. **SSO Password:** *(Establish your SSO password)*

Click **Finish** and wait for services to start.



Security Systems Specialist

1.8.3 Deployment Verification and Validation of VCSA

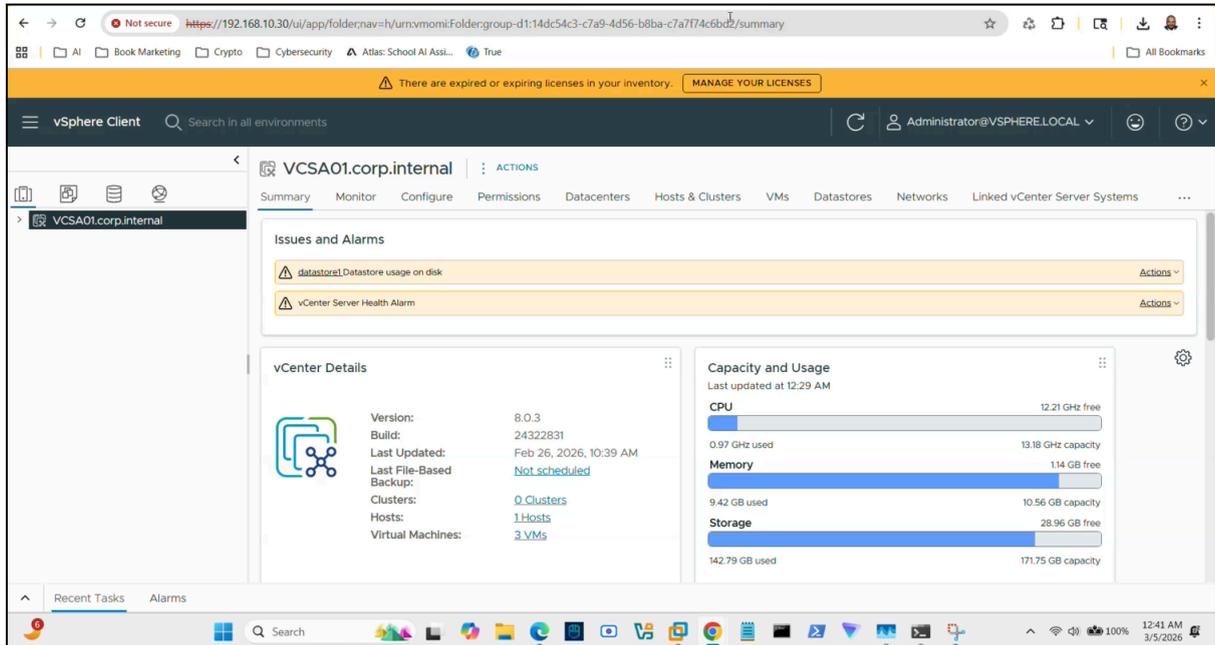
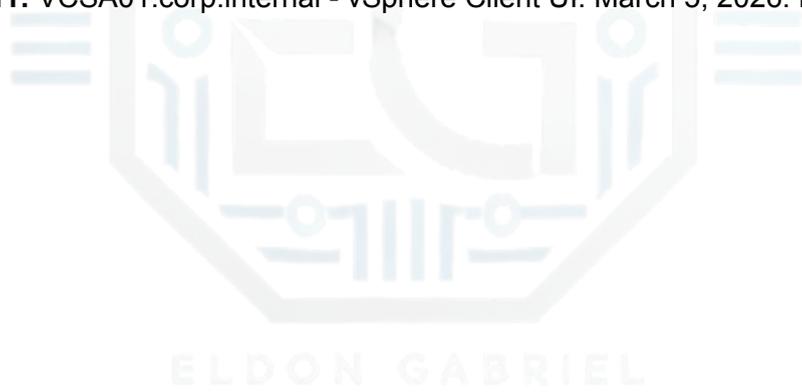


Figure 11: VCSA01.corp.internal - vSphere Client UI. March 5, 2026. Eldon G.





2.0 PHASE 2: AWS MGN SETUP & MIGRATION

Purpose: Execute the replication of migration candidates DC2001 and WS01 to the AWS, configure the target launch templates to prevent conflicts, and perform the final cutover.

2.1 Migration Workflow

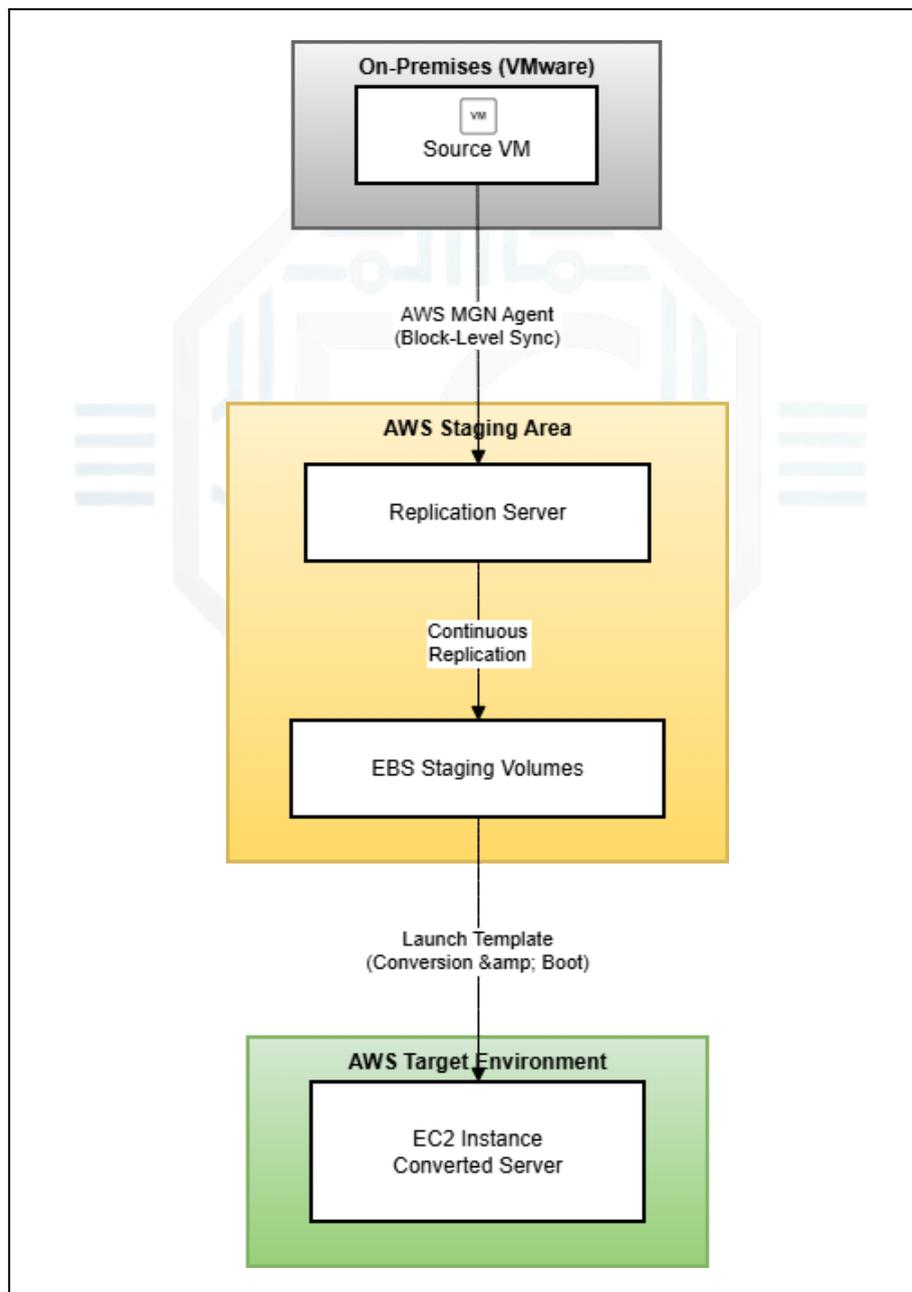


Figure 12: AWS MGN Migration Data Flow. March 6, 2026. Eldon G.



Security Systems Specialist

2.2 Migration Test Launch & Visual Validation

Purpose: To validate the integrity of replicated block data in an isolated AWS environment before severing an on-premise connection. The final cutover should not be executed without a successful test launch.

2.3 Launch Settings & Conflict Resolution

To ensure a successful Test Launch in the **Elastic Compute Cloud (EC2)** environment, the following were implemented:

- **Bring Your Own License (BYOL):** Maintains technical parity with source licensing.
- **Default Host Management Configuration (DHMC):** Centralized management of EC2 instances via AWS Systems Manager (SSM)
- Replication data were staged in an AWS-managed staging area subnet prior to EC2 launch.

2.4 Migration Test Launch & Visual Validation

Expected Result: The instance diagnostics should display the standard Windows Server login prompt, confirming that the OS survived the hypervisor-to-cloud hardware translation without crashing.

Test Launch Validation Parameters

Milestone	Expected Result	Status
Agent Connectivity	Heartbeat detected in AWS Console	VERIFIED
Firewall/Port 1500	Outbound traffic to Replication Server	VERIFIED
Data Consistency	19GB Baseline Sync Complete	VERIFIED



2.5 Target Instance Verification (Screenshot Capture)

Objective Requirement: The final deliverable for the AWS MGN phase is visual verification of the migrated instances. Screenshots of the DC2001 and WS01 EC2 instances at the Windows Server login screen showed that the operating system had survived migration to the cloud. They also confirmed that the AWS Nitro NVMe drivers had started successfully. (See Figures 13 & 14).

2.5.1 Deployment Verification and Validation of DC2001 Instance

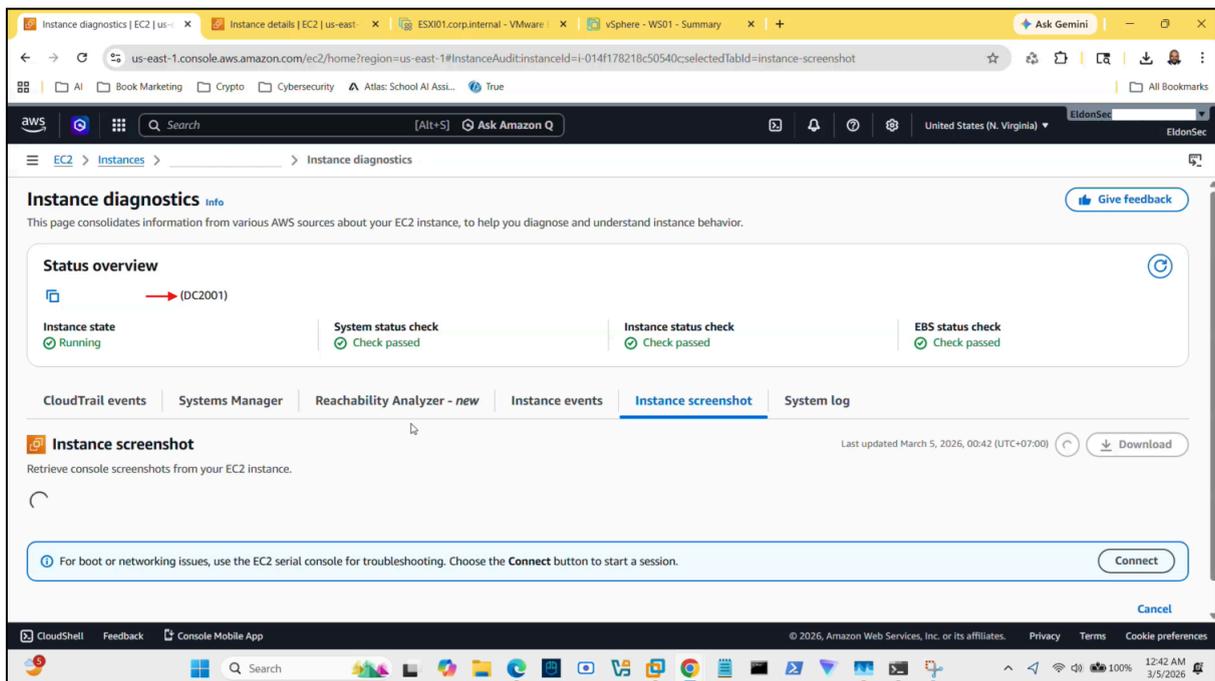


Figure 13: DC2001 EC2 instance diagnostics screenshot. March 5, 2026. Eldon G.



Security Systems Specialist

2.5.2 Deployment Verification and Validation of WS01 Instance

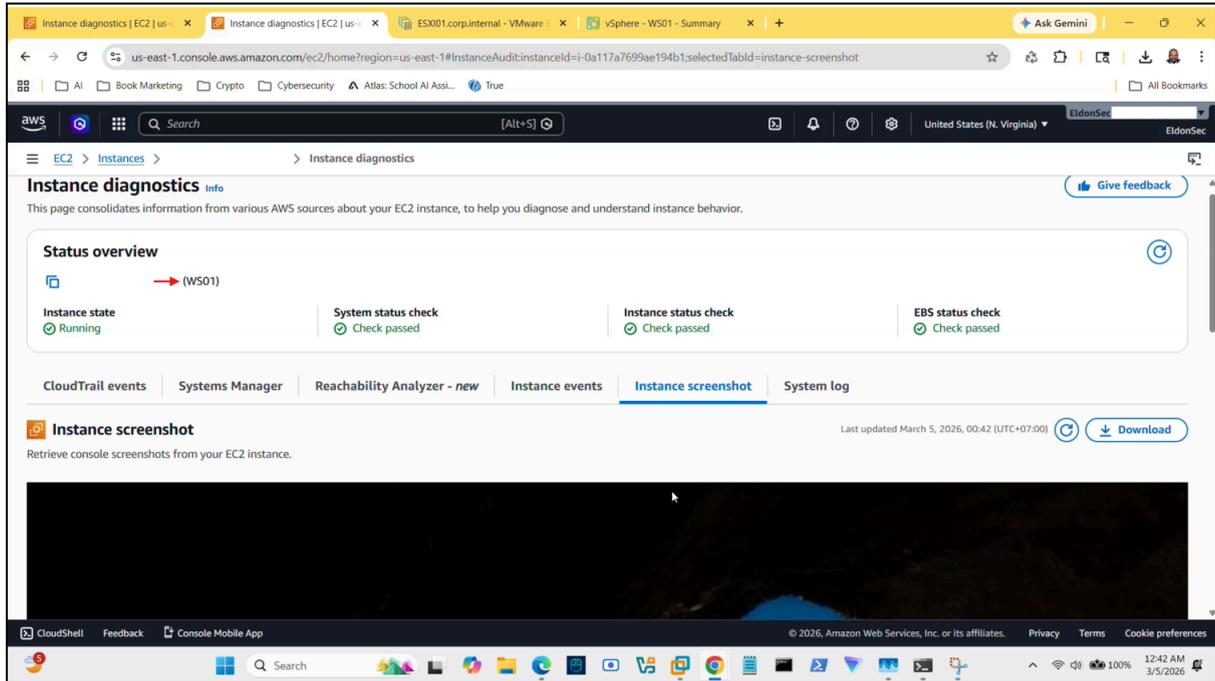


Figure 14: Screenshot of WS01 EC2 instance diagnostics on March 5, 2026. Eldon G.

ELDON GABRIEL



Security Systems Specialist

3.0 PHASE 3: FAILBACK & STRESS TEST RCA

Document ID: RCA-2026-003-DC2001

Subject: Recovery of DC2001 Following Post-Migration Driver Conflict

3.1 Dimensional Analysis

The failure injected during the stress test was analyzed across multiple system layers. The virtual disk used a **GUID Partition Table (GPT)**. The manual removal of the AWS drivers caused a breakdown in the **Hardware Abstraction Layer (HAL)**.

3.2 Diagnostic Validation and Resolution Steps

Step	Action	Outcome	Logic/Validation
1	Firmware Correction	Success	Toggled the VM settings from BIOS to EFI to match the GPT partition requirements.
2	BCD Reconstruction	Success*	Kernel initialization failed due to missing drivers.
3	Parallel Installation	Success	Custom installed the OS via an ISO without formatting to bypass the corrupted System State.
4	Data Verification	Success	The original data in <code>D:\Users</code> remained persistent after OS destruction; C: Drive was mounted as a secondary disk.

ELDON GABRIEL



4.0 APPENDIX: LAB QUICK REFERENCE

4.1 Lab Architecture Topology

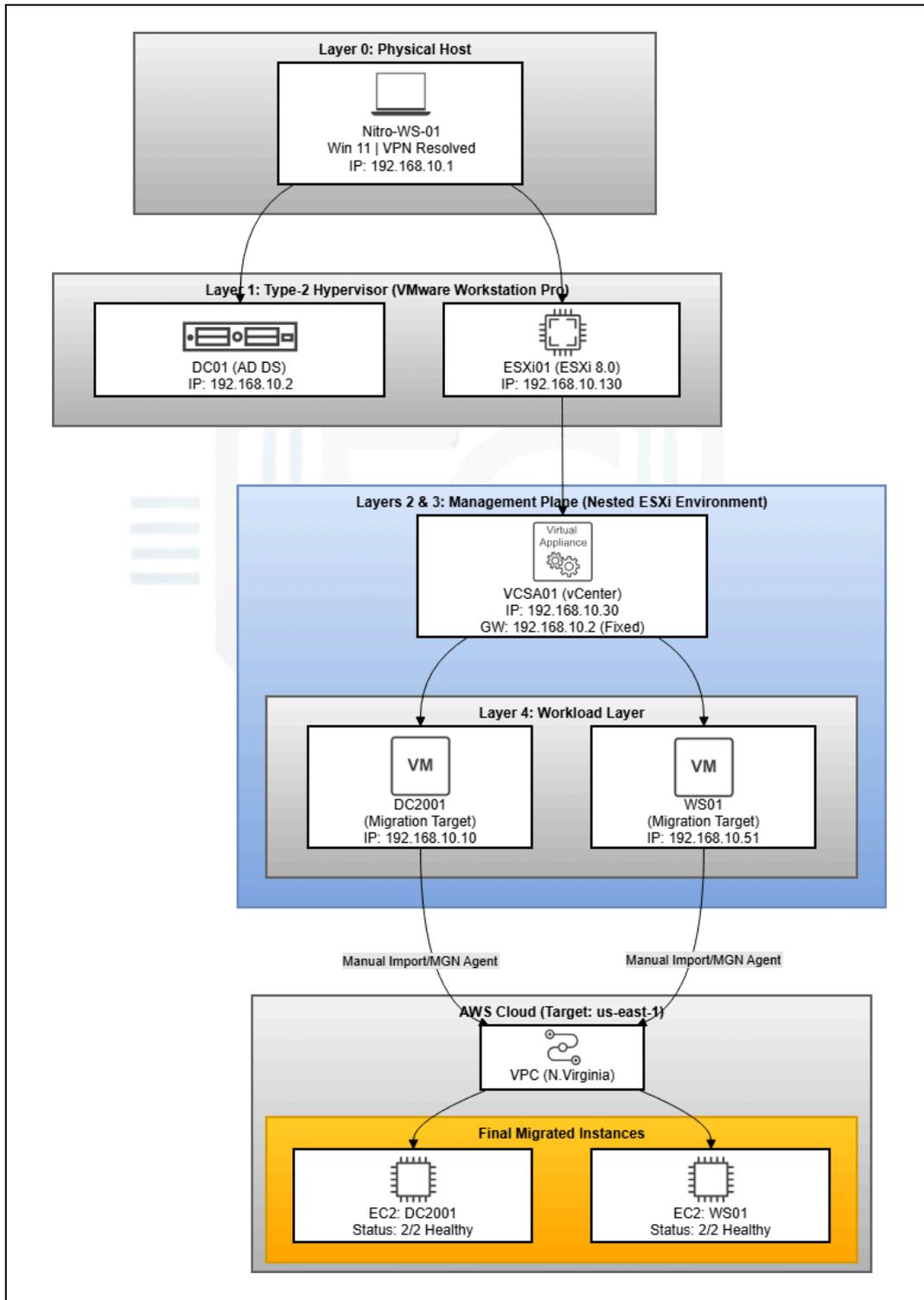


Figure 15: Topology of VMware to the AWS Migration Lab. March 4, 2026. Eldon G.



4.2 Table 1 – Technical Abbreviations & Glossary

Abbreviation	Full Term	Description in Lab Context
ADDS	Active Directory Domain Services	The identity provider was hosted on DC01 for the corp.internal forest.
APIPA	Automatic Private IP Addressing	Default IP allocation (169.254.x.x) when DHCP is unreachable.
DHMC	<i>Default Host Management Configuration</i>	<i>SSM features for automatic agentless EC2 management.</i>
GPT	GUID Partition Table	The modern partitioning standard required for EFI booting.
VCSA	vCenter Server Appliance	Centralized management utility for VMware environments Context:

4.3 Table 2 – Lab Inventory & Identity

Device	Operating System	IP Address	Gateway	Role
Nitro host	Windows 11	192.168.10.1	ISP	Physical Foundation
DC01	Windows Server 2019	192.168.10.2	192.168.10.1	Domain Controller (corp.internal)
ESXi01	ESXi 8.0	192.168.10.130	192.168.10.2	Lab Gateway to VCSA01
VCSA01	Photon OS 4.0	192.168.10.30	192.168.10.2	vCenter Management Plane
DC2001	Windows Server 2019	192.168.10.10	192.168.10.2	Workload (Migration Target)
WS01	Windows 10	192.168.10.51	192.168.10.2	Workload (Migration Target)

ELDON GABRIEL