REPORT
Building a vSphere 8 Nested Lab on AMD Ryzen 6000

v1.0.0

Author:

Eldon Gabriel

February 22, 2026

TABLE OF CONTENTS

Disclaimer: This report documents my independent lab research and configuration work related to enabling nested virtualization on an AMD-based Windows 11 system using VMware Workstation. The VMware ESXi deployment phase was not completed due to licensing restrictions requiring a corporate account for evaluation access.

This documentation reflects my personal testing, troubleshooting, and validation steps performed in a controlled lab environment. No MCSI video content, proprietary lab materials, or protected instructional resources have been shared or distributed. All explanations are written in my own words and follow MCSI's disclosure and academic integrity policies.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/22/2026	Eldon G.	Initial draft.

1.0 AMD NESTED VIRTUALIZATION

1.1 Project Description

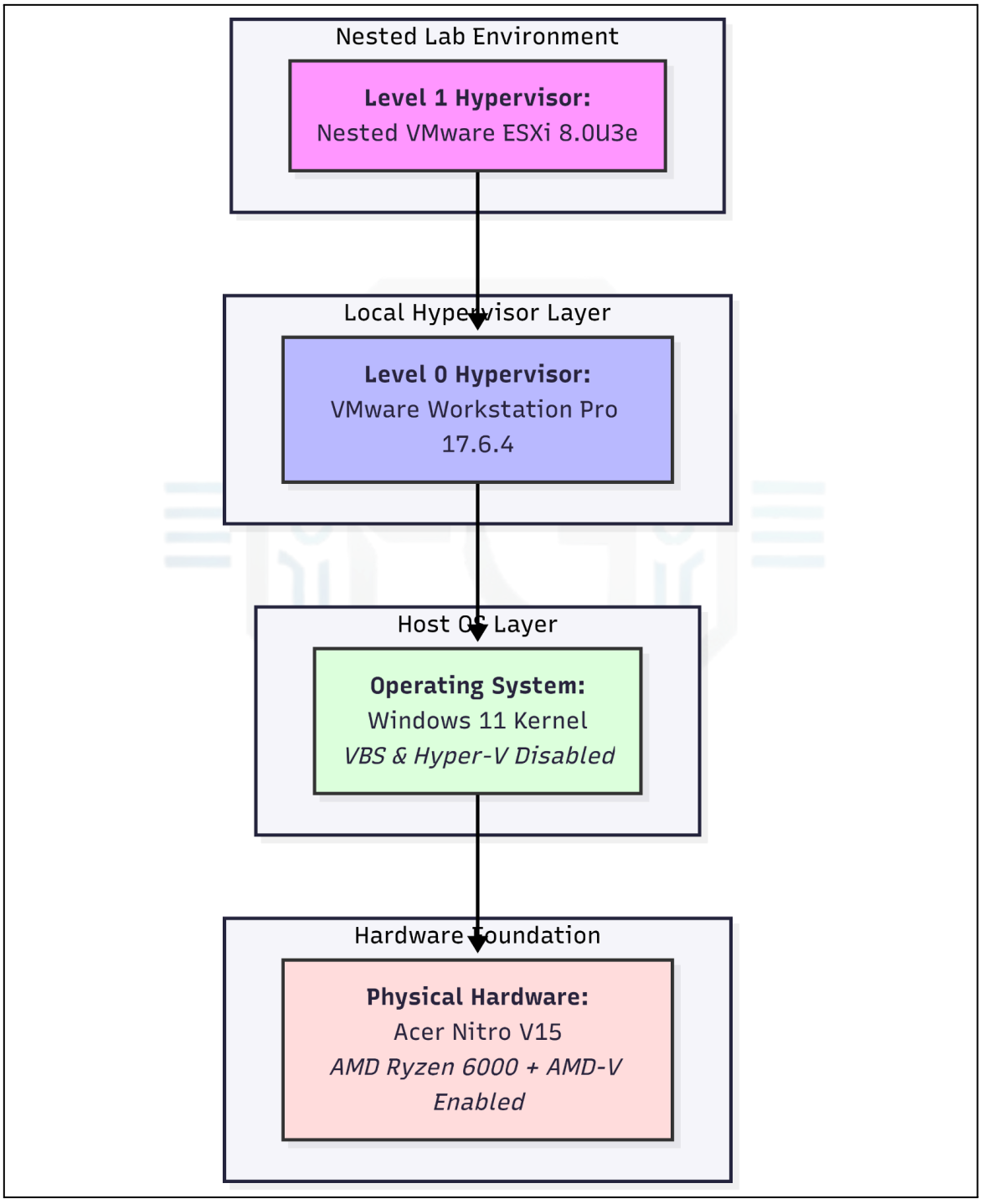

Figure 1: Visualizing the Nested Virtualization Stack on AMD Ryzen 6000. 2026. Eldon G.

This guide explains how nested virtualization was enabled on an AMD Ryzen 6000 laptop. Initially, VMware Workstation could not detect *AMD-V (SVM),* even though the CPU supported it.

The goal was to deploy a **vSphere 8.0U3e lab** using VMware Workstation Pro 17.6.4. The lab included:

- **Environment**: Acer Nitro V15 (ANV15-41) | AMD Ryzen 6000 Series
- **Hypervisor**: VMware Workstation Pro 17.6.4
- Nested ESXi hosts
- vCenter Server Appliance (VCSA)

To achieve this, several issues had to be resolved:

- Hidden firmware settings
- Windows 11 Hyper-V and VBS conflicts
- Incorrect chipset drivers from Windows Update
- Security features blocking virtualization

All security settings were restored after testing.

Hardware & Resource Allocation

Component	Specification	Lab Role / Allocation
CPU	AMD Ryzen 5 6600H (6C/12T)	Provides SVM/RVI hardware extensions
RAM	32GB DDR5	Supports Host OS + ESXi + VCSA (Tiny)
Storage	512GB NVMe Gen4	Datastore for vCenter and Nested VMs
Host OS	Windows 11 Home	Management Layer (VBS/Hyper-V Disabled)

1.2 Security and Risk Disclaimer

This process requires changing the firmware settings and disabling Windows security features, including

- *Virtualization-Based Security (VBS)*
- Hyper-V
- *Local Security Authority* (*LSA*) isolation

These changes reduce system security. They were performed only in a controlled laboratory environment.

In production, these settings must follow the company security policy and be restored after testing.

1.3 Chipset and Driver Synchronization (AMD + Windows Alignment)

For nested virtualization to work, Windows must correctly detect the *SVM setting* from the firmware.

During testing, default Windows drivers did not reliably expose virtualization support to VMware. This caused unstable AMD-V detection.

Action

Install the latest **AMD Chipset Software** from AMD.

Objective

Ensure proper communication between the firmware, chipset, and Windows.

Critical Drivers for Virtualization

AMD PSP Driver: Ensures that Windows correctly reads AMD firmware security states.

AMD PMF Driver: Improves stability between the firmware and OS during virtualization workloads

Windows Feature Alignment

After installing the chipset drivers, enable the required Windows virtualization features.

Navigate to:

Control Panel → Programs → Turn Windows features on or off

Enable:

- **Virtual Machine Platform**
- **Windows Hypervisor Platform**

These features allow Windows to properly register virtualization support.

Reboot Required

A full restart was required after these changes.

Note*: In some specific Windows 11 updates, even if you disable VBS in the registry, these two checkboxes can sometimes "re-arm" the Windows Hypervisor.*

1.4 Firmware Initialization: Hidden UEFI Access

Advanced CPU settings are hidden in the BIOS on the Acer Nitro V15.

A special key sequence is required to unlock them.

Startup Holding Method

Stage 1: Fully shut down the laptop.
Stage 2: Press and hold *Fn* + *Tab*.
Stage 3: While holding, press the power button.
Stage 4: Release the keys when the keyboard lights up.
Stage 5: Press F2 repeatedly to enter the BIOS.

Required UEFI Settings

Apply the following:

- **SVM Support → Enabled**
- **SVM Lock → Disabled**
- **SMM Code Lock → Disabled**
- **SMM Isolation → Disabled**

These settings allow VMware to directly control AMD-V.

1.5 OS-Level Configuration: Disabling VBS

Windows 11 uses virtualization to power security features, such as

- VBS
- Credential Guard
- Memory Integrity

When enabled, Windows loads its own hypervisor. This prevents VMware from using AMD-V directly.

To enable nested virtualization, these features must be disabled.

PowerShell Configuration (Run as Administrator)

Reboot required after execution.

Disable Windows hypervisor:

```powershell
bcdedit /set hypervisorlaunchtype off
```

Disable VBS:

```powershell
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "EnableVirtualizationBasedSecurity" /t REG_DWORD /d 0 /f
```

Disable Local Security Authority (LSA) Isolation:

```powershell
reg add "HKLM\SYSTEM\CurrentControlSet\Control\LSA" /v "LsaCfgFlags" /t REG_DWORD /d 0 /f
```

If Credential Guard is UEFI locked:

```powershell
.\DG_Readiness_Tool_v3.6.ps1 -Disable -Execute
```

If this step is skipped, Windows will continue to block nested virtualization.

1.6 Incident Recovery: CMOS / NVRAM Reset

Incorrect firmware settings can cause a *No-POST* condition.

- Black screen
- Fans running
- Keyboard lights on

This usually indicates conflicting firmware settings.

Battery Pin-Hole Reset

Stage 1: Disconnect the power.
Stage 2: Locate the reset pin hole under the laptop.
Stage 3: Press and hold the reset button for 20 s.

This clears temporary firmware states and restores default settings.

1.7 Validation and Verification

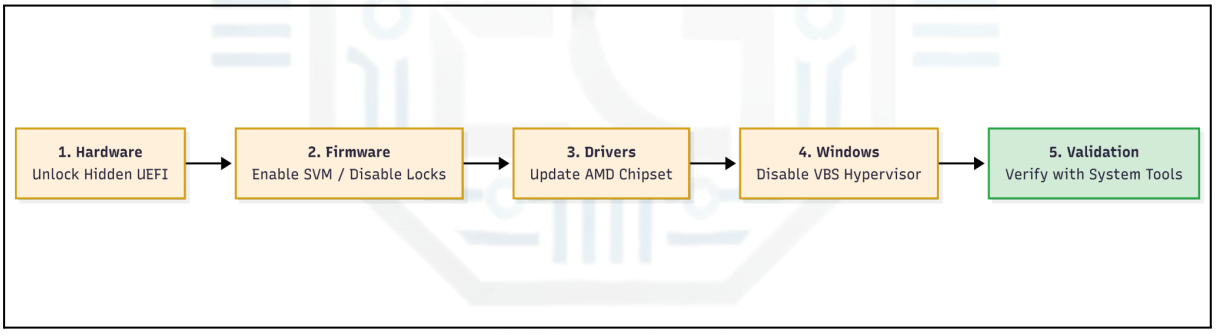

Figure 2: Engineering Workflow for Platform Enablement. 2026. Eldon G.

After configuration, validation was performed.

Step 1: VBS Status

Tool: `msinfo32`

Required value:

Virtualization-based security → **Not enabled**

Step 2: Hypervisor Status

Tool: `systeminfo`

Required results:

- Virtualization Enabled In Firmware → Yes
- Second Level Address Translation → Yes
- VM Monitor Mode Extensions → Yes

The output must not state:

“A hypervisor has been detected.”

If it does, Windows is still blocking VMware.

Step 3: VMware Validation

Open ESXi VM Settings → Processors

Enable:

Virtualize Intel VT-x/EPT or AMD-V/RVI

Expected result:

- ESXi boots without AMD-V errors
- Hardware virtualization is detected
- Nested 64-bit VMs can be created

1.8 Troubleshooting Decision Tree

AMD-V Not Supported

Confirm that VBS is disabled and SVM is enabled in the BIOS.

Black Screen / No-POST

Perform a battery reset. Restore SMM settings to default.

Hyper-V Still Detected

Disable Memory Integrity and all Hyper-V features. Re-run the bcdedit command.

VCSA Stuck at 80%

Verify DNS resolution, time synchronization, and RAM (minimum 12GB for VCSA Tiny).

Engineering Note: Hardware Resource Headroom. *While the standard Acer Nitro V15 ships with 16GB of RAM, this environment was built on a **32GB RAM** configuration. This provides the necessary headroom to run the vCenter Server Appliance (VCSA) "Tiny" deployment (12GB) alongside the Windows 11 Host OS and a nested ESXi host (typically 4GB–8GB) without inducing system-wide memory contention or disk swapping.*

1.9 Security Tradeoff Summary

Security features were temporarily disabled to enable nested virtualization.

Risks Introduced

- Reduced firmware protection
- Reduced kernel memory isolation
- Increased credential exposure risk

Justification

These changes were required to support enterprise-grade nested labs using ESXi and VCSA.

Mitigation

All security settings were restored after lab completion.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- **Hardware Enablement:** The Acer Nitro V15 requires a non-standard startup sequence to unlock hidden CPU virtualization settings.
- **Security Conflicts:** Windows 11 Virtualization-Based Security (VBS) and Hyper-V must be de-provisioned to allow VMware Workstation direct access to AMD-V/SVM extensions.
- **Driver Stability:** Utilizing official AMD Chipset Software (specifically the PSP and PMF drivers) is mandatory for stable firmware-to-OS handoff.
- **Recovery Readiness:** Firmware-level recovery procedures (CMOS/NVRAM reset) are essential when modifying SMM security states.

Conclusion on Capacity: > The selection of the **AMD Ryzen 5 6600H** platform, combined with a **32GB RAM upgrade**, provided the necessary computational density to support the vSphere 8.0 environment. This hardware configuration successfully mitigated common nested performance bottlenecks, such as CPU wait-time and memory ballooning, ensuring a stable foundation for the vCenter Server Appliance (VCSA).

2.2 Security Implications and Recommendations

The steps in this guide reduce standard Windows security protections.

Security Risks

- Disabling VBS increases kernel-level attack exposure
- Disabling LSA isolation increases credential-dumping risk
- Disabling SMM protections weakens firmware security

Technical Recommendations

After lab completion, restore all security settings.

UEFI Settings

- SMM Code Lock → Enabled
- SMM Isolation → Enabled
- SVM Lock → Enabled (if no longer needed, disabled)

Restore Windows Security

```powershell
bcdedit /set hypervisorlaunchtype auto
```

```powershell
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "EnableVirtualizationBasedSecurity" /t REG_DWORD /d 1 /f
```

```powershell
reg add "HKLM\SYSTEM\CurrentControlSet\Control\LSA" /v "LsaCfgFlags" /t REG_DWORD /d 1 /f
```

Procedural Recommendations

- Treat these changes as controlled lab exceptions
- Do not apply to production systems
- Document all firmware and OS modifications

Framework Alignment

NIST SP 800-53 (CM-2, CM-6, SI-2)
Configuration changes must be controlled and reversible.

CIS Benchmarks (Windows 11)
Disabling VBS and LSA protections deviates from the baseline and should be a temporary change.

Least Functionality Principle
Disable only what is required. Restore immediately after testing.
