Salem Automation
Systems Integration Specialists

Bare Metal and Security Technical Note

Table of Contents

1. Overview

This document explains the Bare Metal approach for vtAlpha and vtVAX emulators. Traditional emulators that run on Windows or Linux Operating System (OS) have significant hurdles, for which Bare Metal was developed to overcome and become a recommended platform.

2. The Problem with Traditional Virtualization

Many users have experienced frustration with Alpha and VAX emulators running on a Windows or Linux OS. Here's what we hear most often and why:

"We can't afford the downtime"

- Alpha and VAX system historically ran non-stop without interruption.
- Windows and Linux hosts required monthly security patches and reboots.
- Each host reboot means that the production system must be down to install the patch.
- Maintenance of these host system dictates operation schedules rather than your business needs.

"Performance is unpredictable"

- General-purpose OS updates break emulator performance.
- Background processes and features takes resources from your application.
- Storage and network driver changes have caused serious stability issues.

"We have competing IT priorities"

- Your legacy systems team manages Alpha and VAX operations.
- A different team manages the Windows and Linux infrastructures.
- Internal policies conflict and create delays.
- Post-OS update testing to ensure the emulators still work.

3. The vtServer Bare Metal Solution

vtServer is installed directly on your hardware, as a **complete turnkey appliance**, without Windows or Linux running underneath. Think of vtServer like your network or storage arrays: dedicated equipment that is managed as a unit an not a general-purpose computer that must be maintained.

3.1 Real-World Results

Our customers consistently report:

- **Uptime improvements:** Moving from monthly-host reboots to maintenance scheduled around business needs and goals.
- **Performance gains:** 15-30% improvement over traditional virtualization, in many cases.
- **Simplified operations:** Reduced complexity means your team focuses on applications, not infrastructure.
- **Faster problem resolution:** Known configurations that allow for faster troubleshooting.

3.2 What You Get

3.2.1 Purpose-Built Environment

- Based on the standard Linux kernel, which is the same foundation as Red Hat, SUSE, and enterprise appliances.
- Includes only what is needed, without extra features that consume software resources.
- Everything is tested and integrated by us as a single unit.

3.2.2 Simple Management

- vtMonitor web-based GUI for all configuration and monitoring.
- Console interface for system-level settings.
- No separate operating system to patch and maintain.

3.3 Benefits for Your Organization

3.3.1 Maximum Uptime and Stability

Fewer Updates, Fewer Reboots

- Minimal software footprint means fewer security patches apply.
- Updates happen on your schedule, not dictated by Microsoft or Linux vendor cycles.
- Many Salem Automation customers can run non-stop for years at a time.

Tested Reliability

- Every update tested by Salem.
- No surprise compatibility issues from third-party OS changes.
- Your emulators run on a known, stable platform.

3.3.2 Enhanced Security Posture

Secure by Default

- Minimal attack surface with no unnecessary software installed.
- Only 3 network ports enabled initially:
    - 80/443 (HTTP/HTTPS) for management interface.
    - 22350 for license verification.
- Additional services, SSH, SMB, NFS, FTP, are available but disabled by default. For a list of ports, refer to Table 1.
- Opt-in security model allows you to enable only what you need.

Table 1—IP Ports

Service Ports			
Name	**Number**	**Name**	**Number**
FTP	21	vtScan	9456
SSH	22	vtLicense access (Remote)	22350
HTTP	80	RemoteSupport	22, 80, or 443
RPCBIND	111	NFS V4	2049

Table 1—IP Ports			
Service Ports			
Name	**Number**	**Name**	**Number**
Samba SMB	139 and 445	NFS V3	2049 and 111 Port Mapper
SSL	443		
vtAlpha			
Name	**Number**	**Name**	**Number**
OPA0	20000	Com 2	20001
Serial ports, if used.			
vtVAX			
Name	**Number**	**Name**	**Number**
OPA0	10003	TTA1	10001
TTA0	10000	TTA2	10002

Protection Through Isolation

- User data isolated from executable code by design.
- Closed architecture prevents accidental or malicious software installation.
- No risk of misconfigured software creating vulnerabilities.

Easier Compliance

- Single, controlled configuration simplifies security audits.
- Clear documentation of what's running and why.
- Minimal exposed services to document and justify.

3.3.3 Simplified Operations

One Configuration to Manage

- No unique installations with site-specific modifications.
- Consistent user experience across all your vtServer hosts.
- Salem Automation's team know exactly what you're running.

Predictable Support

- Faster troubleshooting with known configurations.
- Updates are tested and proven before deployment.
- Reduced downtime for maintenance activities.

4. Common Comments and Questions from Users

"Our security team requires anti-virus software on all systems."

We understand this requirement, and here's how we address it with your security team:

vtServer's architecture provides protection differently than traditional systems:

- User data is isolated from executable code by design.
- The closed appliance model prevents unauthorized software installation.
- Minimal attack surface reduces threat vectors.

Why traditional AV software creates more risk than it prevents:

- **Performance impact:** Continuous file scanning consumes CPU and I/O resources needed by your emulators, potentially causing instability or crashes.
- **False positive risk:** AV software designed for x86 code misidentifies Alpha and VAX binary code in disk containers as malware, which leads to quarantined files and potential data loss; we've seen it happen.

Salem Automation's recommendation: Treat vtServer as other infrastructure appliances , like firewalls and storage arrays, that don't run AV software. Focus on network segmentation, access controls, and monitoring, which are more effective for appliance-based systems.

We're happy to participate in discussions with your security team to explain the architecture.

"Can we install Tools or monitoring agents?"

We're frequently asked about installing hypervisor integration tools or monitoring software directly on vtServer.

Why this isn't supported:

- Creates unique configurations that complicate support and troubleshooting.
- Introduces untested software that could impact stability.
- May conflict with vtServer's internal operations.

Better alternatives:

- Monitor vtServer at the hypervisor level for virtual deployments.
- Use vtMonitor's built-in monitoring and alerting.
- Monitor your Alpha and VAX guests directly as you always have.
- Contact Salem Automation if you need specific functionality.

"We need command-line access for our administrators."

All configuration and diagnostic capabilities are available through:

- vtMonitor GUI: Web-based interface for day-to-day management.
- Console interface: System-level configuration and troubleshooting.

Why direct shell access isn't provided: The appliance model ensures everyone runs the same tested configuration. This benefits you through:

- Faster support response because we know exactly what you're running.
- Reliable updates without compatibility surprises.
- Consistent security posture across all installations.

If there's functionality you need that isn't available, let Salem Automation know.

"What about running vtServer on VMware, KVM, or Hyper-V?"

vtServer works well on virtualized infrastructure. One consideration:

Nested virtualization creates synchronization challenges:

- Your hypervisor manages vtServer.
- vtServer manages your Alpha and VAX guests.
- Some hypervisor features, like live snapshots, require coordination across all layers.
- OpenVMS and Tru64 weren't designed for this type of coordination.

Practical impact: Certain operations may need to be performed differently. Salem Automation provides best practices for virtualized deployments that help you design the optimal configuration.

NOTE: For more recommendations for vtServer VMware Set Up Requirements, refer to our document here: VMware Setup on a vtServer.

5. Salem Automation's Implementation Approach

When we deploy vtServer for customers, we focus on:

5.1 Initial Setup

- Hardware sizing based on your workload requirements.
- Network architecture for security and performance.
- Integration with your existing backup and monitoring infrastructure.

5.2 Knowledge Transfer

- Training your team on vtMonitor and console interfaces.
- Documentation of your specific configuration.
- Best practices for ongoing operations.

5.3 Ongoing Support

- Salem Automation provides first-line support for all vtServer issues.
- Regular review of your environment to optimize performance.

6. Next Steps

6.1 Evaluating vtServer for your environment?

Salem Automation can help you:

1. Assess your current Alpha and VAX infrastructure.
2. Design the optimal vtServer deployment.
3. Plan migration with minimal disruption.
4. Provide training and ongoing support.

6.2 Have questions about specific requirements?

Whether it's security policies, compliance requirements, or integration with existing infrastructure, we've worked through these scenarios with customers across industries.

Contact Us

Email: info@salemautomation.com

Visit our website: https://www.salemautomation.com/