PLATFORM9

What to Expect When You're Exiting

Overview

For more than a decade, VMware has been the cornerstone of the modern data center. Changes in licensing models and rising costs, however, have shifted VMware from a strategic asset into a growing financial and operational burden. For many IT leaders, the challenge is no longer purely technical, it has become a business-critical transition.

The objective of an exit strategy is not simply to leave a platform. It is to migrate an existing application ecosystem to a new home while preserving—or improving—the stability, performance, and security the business depends on.

> The initial goal is to minimize disruption while preserving the functionality, operating expertise, and efficiency your teams rely on today.

Core Philosophy: The "Low-Drama" Approach

A successful migration is one that stakeholders barely notice. The guiding principle is simple: move first, optimize later. The initial goal is to minimize disruption while preserving the functionality, operating expertise, and efficiency your teams rely on today. Replacing a virtualization platform can feel like trying to change a rug without moving the furniture. While that may sound unrealistic, it is achievable with careful planning and a disciplined, risk-aware approach.

Guiding principles for a successful migration:

- Maintain Continuity: Prioritize a like-for-like migration to reduce variables and minimize risk during the initial cutover.
- Boring is Better: Aim for a process that is so well-prepared that the final cutover becomes a predictable, non-event.
- Selective Modernization: Not every workload needs immediate refactoring. Use this transition to decide which applications should remain as VMs and which may be modernized over time.

The five phases of a successful VMware exit

Predictable transitions follow predictable sequences. Teams that skip or compress these steps almost always encounter delays, outages, or stakeholder escalations. If you have not thought through the implications in advance, you will not have a plan when something goes wrong.

Exit phase	The challenge	The risk
1. Assessment	Discovery and Inventory: What you actually run vs. what you think you run.	Operational Impact. Loss of Uptime SLAs due to failure to achieve consistent high availability and resource balancing.
2. Parity and compatibility mapping	Where "VMware equivalent" features do—and do not—line up. What storage, networking, GPUs, tenants, automation, tooling need to be continued, what can be updated or replaced.	Time and Resources. Schedules fall behind, timelines starting impacting both business processes and operational stability. You cannot predict the unknown, but you can plan for it.
3. Provisioning	Ensuring compatibility with existing enterprise SAN/NAS storage and x86 servers.	Stranded Assets. Forcing a multi-million dollar capital expenditure in new HCI hardware.
4. Migration	Moving running VMs and data files across hosts without any service disruption.	Service Interruption. The financial impact of extended downtime or service failures during cutover.
5. Maintenance	Managing ongoing Day-2 operations (upgrades, patching) and ensuring a unified control plane.	Budget Crisis. Unplanned increase in OpEx due to manual toil and required specialized hiring.

Phase 1: Assessment — Discovery beyond the inventory

An automated list of VMs is just the starting point. True readiness requires understanding the connective tissue of your environment. Your virtualization solution is more than just applications running on VMs. It's a complex web of tiered relationships, dependencies like backup and DR, block, object and file storage, security and observability tools, etc. All these dependencies must be understood before you can safely begin migration.

- **Dependency mapping:** Identify multi-tier app relationships to ensure related components migrate together.
- **Dynamic configurations:** Discovery tools often require VMs to be powered on to accurately detect live IP addresses and active network interfaces.
- **Resource sizing:** Migration is an opportunity to right-size workloads; moving over-provisioned VMs as-is simply transfers inefficiency to a new platform.

Phase 2: Parity and compatibility mapping — What works where with who?

Your team has spent years perfecting vSphere operations. Each application relies on the virtualization stack in different ways. Some may be operational; some may be for compliance (or Compliance); some may be for performance. Your new platform must provide equivalent or better capabilities for each application.

- **High Availability (HA)** and live migration (vMotion equivalent).
- **Role-Based Access Control (RBAC)** and auditability for compliance.
- **Storage and data protection:** Integration with existing SAN/NAS hardware and backup vendors.

> Keeping the migration low-drama means finding the best platform for each application and avoiding the inevitable conflicts that arise when multiple applications share an infrastructure.

Phase 3: Provisioning — What goes where?

The phrase 'lift and shift' provokes strong reactions. Some believe it's the easiest, lowest-risk way to migrate an application from one platform to another. Others believe it's a bandage that's as likely to hurt as much going on as it does coming off. Keeping the migration low-drama means finding the best platform for each application and avoiding the inevitable conflicts that arise when multiple applications share an infrastructure. The question becomes "What is the best plan for this application" for each migrating application you

identified in phase 1. This can help minimize risk, reduce the impact of migration, and prioritize workload migration.

- **Maintain:** Stable or legacy workloads nearing retirement that can stay on a reduced VMware footprint.
- **Migrate:** High-priority VMs that need the benefits of a new platform with minimal architectural change.
- **Modernize:** Business-critical apps that will be redesigned for cloud-native or container-based architectures.

Phase 4: Migration — Let's get moving

This is where insufficient planning takes its toll. Service interruption is the most visible risk. The financial impact of extended downtime during a poorly-executed cutover can quickly exceed the savings of reduced licensing fees. Just as damaging, a poorly executed cutover can erode confidence among application owners and business stakeholders. Choose the appropriate migration strategy, have a documented roll-back plan with signposts and timelines, and communicate expectations to all stakeholders.

- **The strategy:** Utilize "warm migration" techniques where data is synchronized in the background while the VM is live.
- **The goal:** Reduce the "cutover window" to a simple restart, ensuring that the final transition is a scheduled non-event rather than a high-stakes fire drill.

Phase 5: Maintenance — Back to work everyone

The true cost of an exit is revealed after the migration is complete. If the new environment requires manual patching, complex CLI-heavy management, or specialized new hires, operating expenses can spiral. Effective planning ensures that post-migration operations are smoother, more reliable, and more receptive to future modernization.

- **The strategy:** Prioritize a "unified control plane" that mimics the operational ease of vCenter.
- **The goal:** Achieve operational parity — where your existing team can manage the new environment with minimal retraining and no increase in manual toil.

> If the new environment requires manual patching, complex CLI-heavy management, or specialized new hires, operating expenses can spiral.

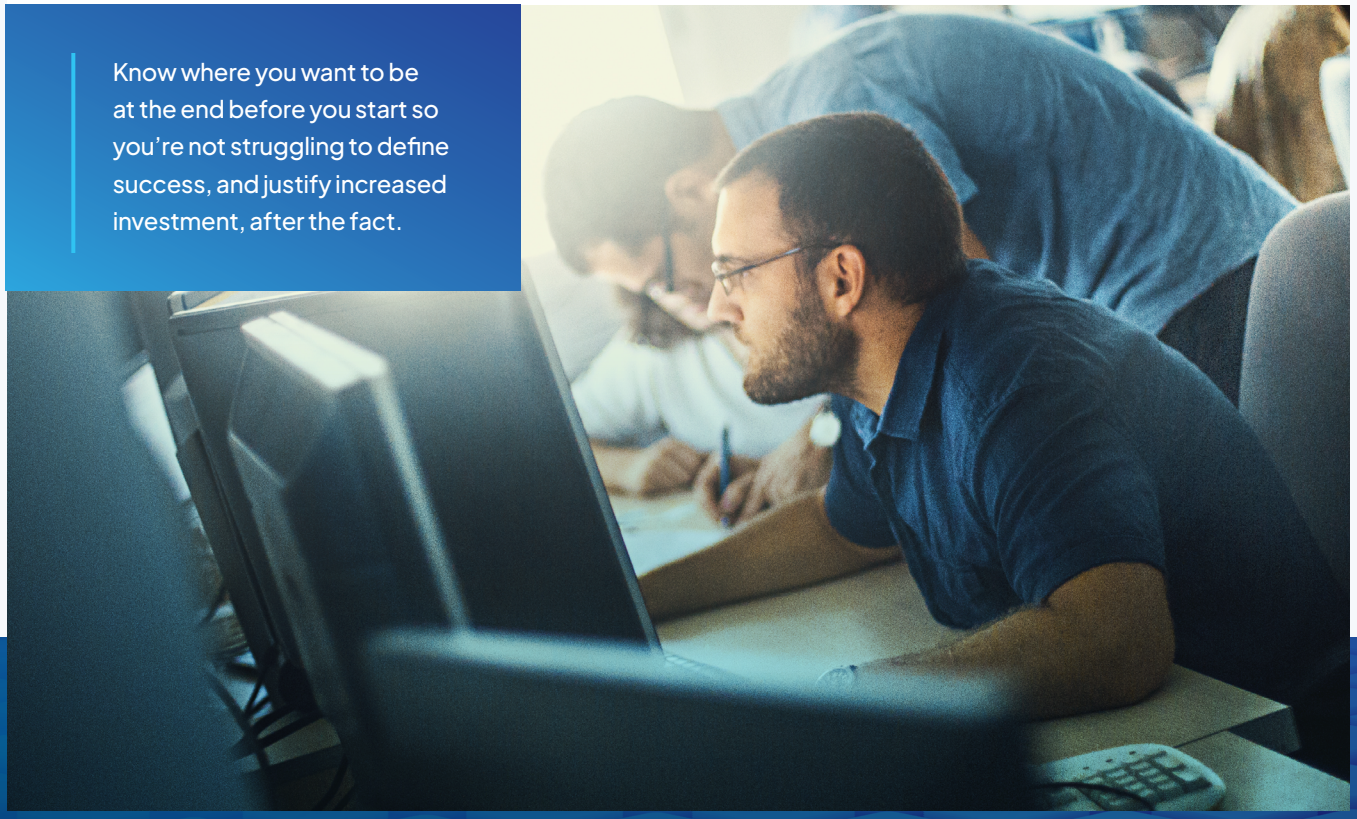
Evaluation: Know before you go

Success isn't just a VM that boots. It is a workload that performs as well — or better — than it did before. While every organization has its own methodology for evaluating success, having specific goals stated before you start helps prove success after you're done. Know where you want to be at the end before you start so you're not struggling to define success, and justify increased investment, after the fact.

Key Performance Indicators (KPIs)

- **Infrastructural integrity:** Do all NICs, storage mounts, and CPU/Memory allocations match the source?
- **Application latency:** Is the response time within the historical baseline?
- **Security posture:** Are the same firewall rules, allowlists, and access controls active and effective?
- **Operational confidence:** Can your team perform "Day-2" tasks (backups, patches, restores) without specialized training?

> Know where you want to be at the end before you start so you're not struggling to define success, and justify increased investment, after the fact.



To learn how Platform9's vJailbreak solution enables enterprises to perform a low-risk migration from VMware please visit our product page.