Pathways to VMware Cloud Foundation 9.1

VCF Professional Services

At a glance

Get to VCF 9.1 faster with expert assistance for upgrading an existing environment or building a new private cloud.

Key benefits

- Rapidly transition to VCF 9.1.
- Reduce risks from AI-driven security threats.
- Minimize disruption to existing operations.
- Benefit from best practices, proven methodologies, and deep knowledge of VMware technology.
- Keep your IT staff focused on business-critical tasks.

Unlock the full power of VMware Cloud Foundation® 9.1 and defend against sophisticated, AI-driven threats by keeping your environment current. Whether you are converging VMware vSphere® instances to VCF, upgrading VCF, or deploying a new private cloud, competing priorities shouldn't stall your progress. VCF Professional Services provides the expert guidance and proven methodologies needed to bypass complexity and accelerate your transition to VCF 9.1.

Pathways to VCF 9.1

VCF Professional Services can expertly transition your environment to VCF 9.1. Our approach is grounded in best practices and insights gained from our extensive experience working with diverse organizations. There are three pathways to transition your environment to VCF 9.1. For all pathways, we can help you adopt operational processes for frequent patching to keep your environment current and secure.

Converge vSphere to VCF

This recommended pathway is the fastest route to converge vSphere environments to VCF 9.1, specifically to reduce AI security risks. We start by checking and remediating prerequisites, then upgrade vSphere and VMware NSX as required. If there is no pre-existing VCF environment, we deploy a new VCF installer instance and convert vSphere to VCF. We deploy any missing VCF components such as SDDC Manager and VMware Cloud Foundation® Operations which along with vSphere are minimum requirements for basic lifecycle management. If there is an existing VCF instance, we can directly import vSphere into VCF and upgrade the environment. After the upgrade is complete, we validate the environment.

Upgrade an existing VCF environment

If you already have VCF, an in-place upgrade can be performed using the built-in lifecycle management workflows. The effort for this pathway is typically lighter; there is no workload migration required, and workloads remain within the same environment. However, there is still a need to validate the current hardware and configuration requirements to ensure the upgrade goes as smoothly as possible.

Learn more

Visit vmware.com/services.

We begin by checking and remediating the environment. Then we upgrade existing automation and operations components, and upgrade VCF core components (SDDC Manager, NSX, VMware vCenter®, and ESX hosts). We deploy a new VMware Cloud Foundation® Operations instance if not previously installed. Then we perform any required final upgrade activities such as configuring licensing and upgrading VI workload domains. We conclude by validating the environment.

Deploy a new VCF environment

This pathway is ideal if you are doing a hardware refresh, expanding into a new data center or wanting to stand up a new private cloud. If your current environment does not meet upgrade requirements, a new installation provides the most reliable pathway to transition your workloads and decommission legacy hardware.

We design, deploy, integrate, and configure your virtual compute, network, storage, automation and operations platform. Once your new environment is ready, we can migrate your application workloads. We develop a migration strategy, discover and analyze your environment, create a detailed migration plan, and perform and validate the migrations.

Reduce frontier AI-driven security threats

Whether upgrading or building new, it's essential to reduce your private cloud attack surface and accelerate timely release cycles to mitigate AI-driven threats. Our experts implement security standards and hardening across all compute, storage, and network components, including automated installation tools.

We integrate the VMware vDefend Security Services Platform to enable automated virtual patching at the network layer, shielding your workloads against zero-day exploits before vendor patches are committed. To complete the defense-in-depth model, we address edge security by deploying VMware Avi Load Balancer and Avi WAF for centralized L4–L7 ingress protection, SSL offloading, and continuous threat mitigation.

Simultaneously, we can assist with platform lifecycle management processes, removing the friction from maintenance so that your team can apply critical patches when they become available. By implementing these in-depth security capabilities, we can help you reduce frontier AI vulnerabilities to keep your environment resilient against emerging threats.

Benefits

Modernize your infrastructure with confidence. Leverage VCF Professional Services. Our deep expertise and proven methodologies reduce the risk and complexity of upgrading. Get current now. Contact your Broadcom Account Director to learn more about how VCF Professional Services can help your organization.

vmware® by Broadcom

Copyright © 2026 Broadcom. All rights reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.