HashiCorp
an IBM Company

WHITE PAPER

Do cloud right: Image management

Understand the benefits of infrastructure lifecycle management at the image level

Overview

This white paper looks at the implications of **The Infrastructure Cloud** and describes its benefits for standardizing image creation and management. This is part of a series of white papers focused on doing cloud right, exploring topics such as infrastructure as code (IaC) for provisioning, cloud compliance and management, and optimizing cloud spend.

Effective image lifecycle management involves standardizing image creation, tracking all associated builds, automating continuous updates across provisioning pipelines, and simplifying revocation. Implementing these practices lowers the risk of deploying insecure images, reduces the window for vulnerability exploitation, accelerates deployment times, and optimizes cloud spend, all helping organizations better realize value from their cloud investments.

Table of Contents

The move to hybrid cloud

Over the last decade, organizations have been moving their infrastructure from traditional on-premises data centers to the cloud, with **cloud infrastructure spend increasing 66%** in 2024 alone. This move involves a shift from static to dynamic infrastructure, as they move away from manually configuring and managing a fixed set of IT resources to running resources on demand with automated workflows. For most organizations, the goal of this transition is to enable innovation, delivering new business and customer value faster and at a larger scale.

As this movement to the cloud progressed, it soon became clear that the end state for most enterprises is not entirely cloud, but rather a mixture of both cloud and on-premises infrastructure, known as hybrid cloud. This mixed approach enables enterprises to pick and choose the environment that can best support the regulatory and business needs of the organization. Today, we see that an estimated **87% of enterprises** operate within this hybrid infrastructure model.

Despite widespread cloud adoption, many enterprises are still struggling to maximize their returns. In fact, only about **20% have achieved full ROI** due to cost inefficiencies, security risks, and operational complexity.

To address these challenges and realize the expected value, organizations must standardize processes for infrastructure management across cloud and on-prem environments. With this approach, they can establish infrastructure as a central shared service enabled by platform teams to improve speed, increase efficiency, and reduce risk. **HashiCorp Terraform** serves as the industry standard for hybrid-cloud provisioning and enables organizations to utilize shared services at the infrastructure layer, but within this layer sits the building blocks of modern infrastructure and a crucial focus area to achieve hybrid-cloud success: system images.

Image challenges: unlocking full ROI

Images (such as **AMIs** for Amazon EC2, virtual machines, Docker containers, and more) are the building blocks of modern computing infrastructure. While organizations adopting a hybrid cloud model typically start by using Terraform for centralized provisioning, Terraform alone does not handle the details of image creation and management. For that, you can modify infrastructure in place with configuration management tools, or you can take the approach that is considered more stable across the IT world - immutable infrastructure. **Immutable infrastructure** remains untouched following deployment; instead of being modified, it is destroyed and replaced with a fresh version during each infrastructure update. This approach helps ensure consistent, reliable, and secure deployments better suited to support the demands of multi-cloud environments.

As organizations deploy fleets of images to support hybrid services across cloud and private environments, the complexity and scope of these services often involve multiple different teams. Without consistent, central processes and tooling in place, organizations can experience variability in their imaging workflows, creating several challenges:

- **Inconsistencies**: With different image practices, teams are prone to achieve different outcomes with varying levels of infrastructure performance.
- **Risks**: Manual, checklist-driven procedures to apply security standards lead to human error in the form of misconfigured and insecure images that can introduce security threats to the organization and result in outages.
- **Delays**: Teams may duplicate efforts and spend excessive time manually building and updating images for different environments, increasing time to deployment.

These challenges may start small, but can quickly become prominent blockers as organizations scale their infrastructure and image estates. **Without intervention, we see bottlenecked developers, lowered productivity, and a lack of realized value from hybrid cloud investments.**

To combat these issues, organizations and their platform teams need to establish a central shared service for image creation and management workflows. These image processes should not be disjointed or unique depending on the environment they are built and deployed to, but rather consistent and repeatable across both cloud and on-premises environments. With this approach, enterprises can unlock the value of their hybrid cloud investments by:

- **Standardizing workflows**: Synchronize tooling and approved templates across teams to minimize edge cases that may undermine the overall health of the final infrastructure delivered.
- **Enforcing security**: Standardize security and compliance testing to confirm adherence to guardrails defined by the organization before images are released for consumption.
- **Optimizing operations**: Deploy faster by automating image provisioning and version updates across downstream provisioning pipelines.

Solution: Infrastructure Lifecycle Management

So how do we actually achieve this image standardization across hybrid environments and realize the value from our cloud investments?

At HashiCorp, we've worked closely with thousands of the world's largest organizations to better understand the infrastructure challenges they are facing. Through this, we have seen two common themes emerge across organizations at all stages of hybrid cloud maturity:

1. Well-architected Infrastructure Lifecycle Management is the foundation for cloud success.
2. To work efficiently across multiple cloud providers and on-premises environments, a successful cloud program uses golden patterns — presented as IaC — to consistently **build, deploy**, and **manage** infrastructure across all teams.

HashiCorp's Infrastructure Lifecycle Management (ILM) portfolio, delivered via the HashiCorp Cloud Platform (HCP), is designed to address the challenges faced in each stage of the infrastructure lifecycle — Day 0 (build), Day 1 (deploy), and Day 2+ (manage). It offers turnkey tools and workflows needed to consistently deliver the infrastructure underpinning cloud applications from initial provisioning to maintenance, and eventual decommissioning. With HCP, platform teams are able to abstract complexities away from core development teams while ensuring they always use the approved approach by baking governance policies into deployment workflows.

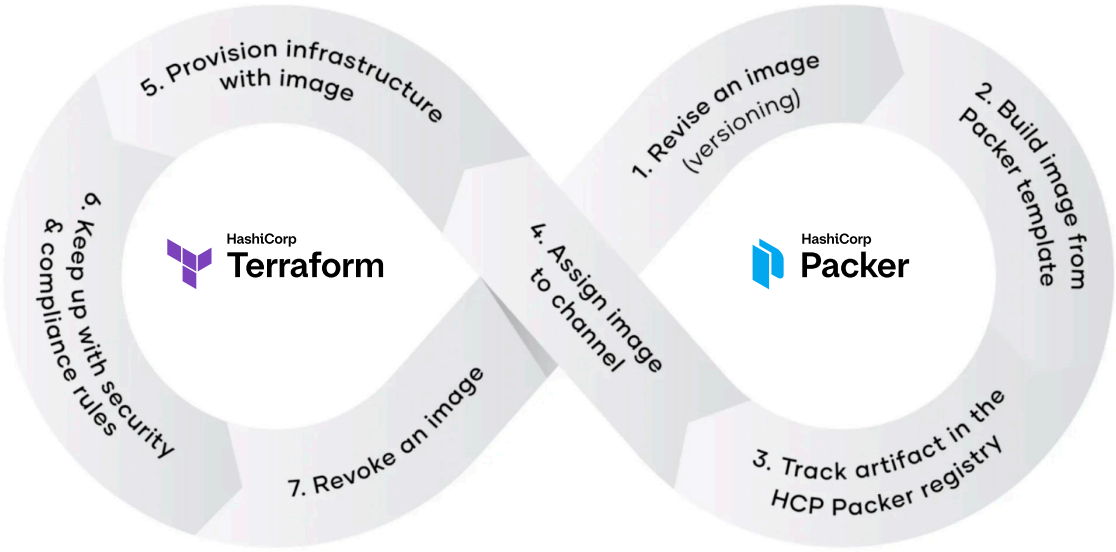
This white paper will focus on HCP Terraform with HCP Packer, two pieces of our ILM portfolio that help platform teams to unify their image management workflows with their provisioning

processes. This integration enables users to shift security and governance left to the image level and create a **golden image pipeline** to automate image management across downstream builds and provisioning pipelines.

HCP Packer helps platform teams establish a unified image management system across groups within an organization. This provides embedded policy and governance, organization-wide visibility, ease of integration with peripheral technologies, and overall reliability at scale.

By integrating HCP Packer into their multi-cloud workflows, organizations can:

- Standardize image creation to ensure all builds deployed are secure and compliant.
- Track all image builds and govern usage in a central artifact registry.
- Continuously update images and downstream provisioning pipelines.
- Monitor image health and simplify revocation workflows.



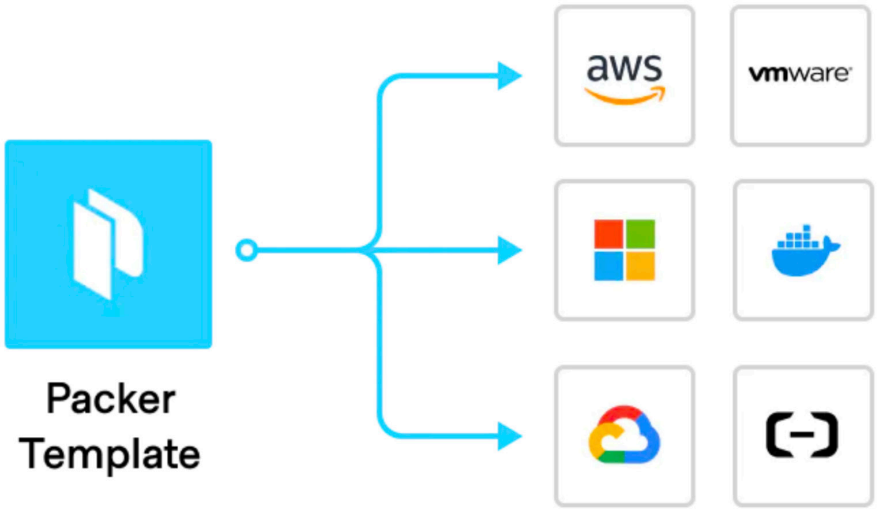
Golden image pipeline with HCP Terraform and HCP Packer

Build

Standardize image creation across clouds and on-prem

TLDR: Packer standardizes how you build images for different environments. By reusing common configurations, you can spin up images faster that always meet your organization's requirements.

HCP Packer is a managed extension of HashiCorp Packer, a free, source-available tool that has become an industry standard for creating identical image builds for multiple cloud and on-premises platforms from a single source configuration file. Packer is lightweight, runs on every major operating system, and is highly performant, enabling multiple image builds to be created in parallel. This standard workflow for generating builds across your multi-cloud environment ensures imaging processes are consistent and repeatable regardless of the type of artifact you are building. Examples include AMIs, Azure VM images, VM templates for VMware vSphere, Docker containers, or Vagrant boxes.



Create identical images for multiple platforms from a single source configuration.

The first step in creating a golden image pipeline is to create a set of golden images with Packer Community Edition. A "golden image" is an approved image that acts as a template on top of which developers can build applications. Quality control teams in an organization will ensure that these images have the most up-to-date common system packages, logging and monitoring tools, security patches, and configuration hardening.

Manual configuration and patching can lead to inconsistent outcomes and increased risk of security breaches and compliance violations due to unsecured or out-of-date base images. Packer helps prevent this by codifying these organizational requirements, ensuring all images are consistent, secure, and compliant before deployment. Golden image versions can then be easily updated and released to react to emerging business, technology, or security conditions.

Packer simplifies golden image creation by enabling organizations to leverage the HashiCorp Configuration Language (HCL). This simple syntax and human-readable language lets users define and describe images using a declarative approach, defining an intended end-state rather than the individual steps to reach the desired outcome. HCL simplifies the process of embedding organizational requirements and also enables collaboration; changes can be reviewed by the appropriate stakeholders using standard version-control workflows before being implemented.

Packer also provides an extensive **template library** that enables users to leverage common configurations across multiple image builds. Templates consist of a series of declarations and commands for Packer to follow when generating a new image build. The template specifies what **plugins** (builders, data sources, provisioners, post-processors) to use, how to configure each of those plugins, and in what order to run them.

Deploy

Track and govern images at scale

TLDR: HCP Packer tracks metadata for all your images in a centralized artifact registry, helping you ensure teams across your organization always use the right image.

When a new golden image is created, the metadata for this new version is automatically published to HCP Packer. HCP Packer serves as a managed registry that stores image metadata, including when they were created, the associated cloud provider, and any custom labels specified in your image build. The HCP Packer artifact registry helps you track information about images, clearly designate which versions are approved for consumption, and query the right images to use in both Packer and Terraform configurations. Access to this centralized library helps align the workflows of image creation and deployment, allowing operations and development teams to work together to manage, track, and govern all artifacts across your infrastructure estate.

Image channels is a core feature of HCP Packer that enables collaboration across teams. With channels, you can label image versions, known as versions, to describe the quality and stability of a build. By assigning human-readable names to image versions, downstream consumers can easily reference the images in Packer templates and Terraform configurations.

For example, you can designate a specific channel for testing, allowing users to promote new versions and quickly spin up an instance to validate the image. Once the new version passes the required tests, it can be promoted to the stable channel, alerting downstream consumers that it is approved and ready for deployment. This workflow provides teams with vetted, ready-built artifacts that supply standard services in a plug-and-play fashion. Consumers can tailor versions of artifacts to streamline their efforts in the updating and release stages, and ensure they are referencing the latest version without having to update their code directly.

As new image versions are published, assigned, and revoked, it is important to maintain visibility into their history and downstream dependencies. HCP Packer's image ancestry

tracking gives users visibility into relationships between the new image version (child) and its source version (parent), if any.

Channel assignment history provides a complete record of artifact activity in a channel. You can browse any existing bucket and select a channel to see exactly which versions have been made available to downstream consumers. From there you can view each image verision's channel history, the status of its parent image, and extended metadata. You can also view when the version was assigned and by whom. Image builders need to collaborate with other stakeholders to validate that new image versions meet compliance and functionality requirements before releasing them to downstream consumers. Restricted channels offer control over the release of images by providing a means to limit channel access for other collaborators. This granular permissions control lets you ensure only the necessary users have channel access and enables the least privilege principle. This addition also helps streamline the image-validation process and prevents downstream consumers from using new image versions before they have been validated and approved.

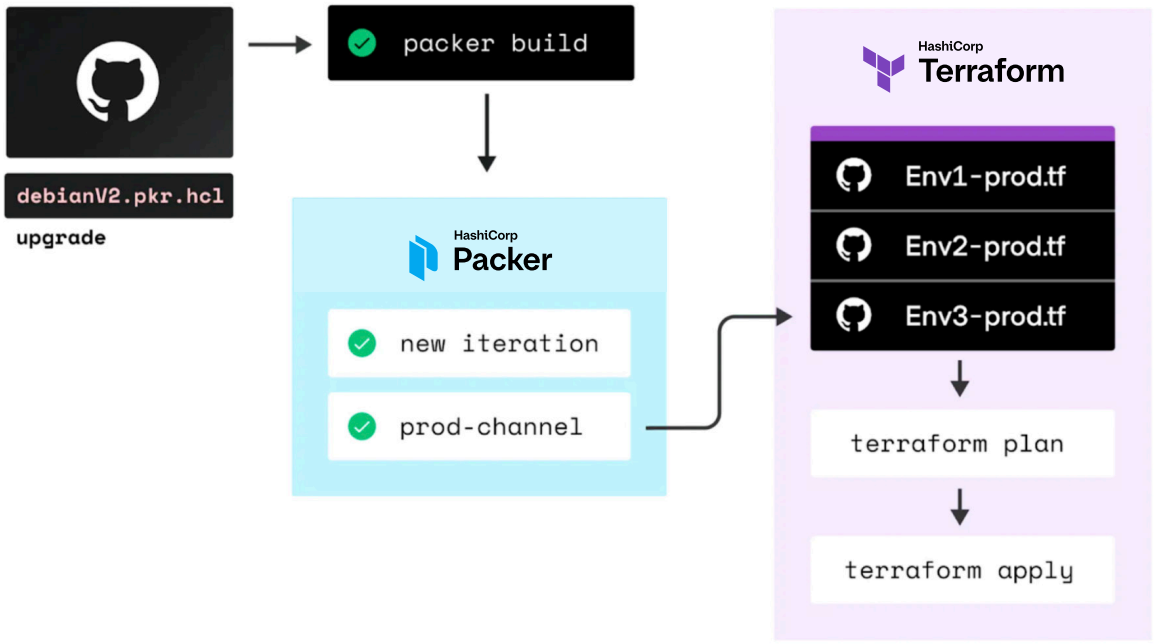
Continuously update images and downstream provisioning pipelines

TLDR: With HCP Terraform and HCP Packer's close integration, you can mitigate risk by preventing the deployment of non-approved versions and continuously updating images.

One reason Terraform has become the industry standard for solving this problem is its environment-agnostic approach to provisioning resources. A unified approach for image deployment across on-premises and different cloud vendors is also crucial. This unification can be achieved by integrating HCP Packer into existing HCP Terraform workflows. Teams that consume images in Terraform can rely on approved, standard subprocesses in the initial provisioning stages, and continue to evaluate whether versions uphold security and compliance standards over time.

With a golden image built, published, validated, and promoted to your organization's stable channel, Terraform runs referencing the updated version can be queued automatically for any workspace using the channel. The image updates across downstream provisioning pipelines can take place autonomously with auto-apply settings or be gated by manual approval processes. The HCP Terraform run task for HCP Packer helps prevent the deployment of non-approved images with:

1. **Data source image validation** to scan your Terraform plan for references to the HCP Packer version and image data sources, warning you or blocking the run if any referenced data is associated with a revoked image version
2. **Resource image validation** to scan your Terraform configuration for resources that use hard-coded machine image IDs and check if the image is tracked by HCP Packer. It also warns users if the image is associated with a revoked version and prompt them to reference the HCP Packer data source instead for better tracking and management capabilities



Reference HCP Packer in your HCP Terraform workflows.

With this automation, teams can integrate images easily onto a larger workflow framework to complement automated delivery pipelines. This automation also makes it easy for platform teams to continuously update their golden images on a regular cadence. Why is this so important? Two words: image vulnerabilities.

We know that identifying and patching vulnerabilities is crucial to the overall infrastructure security strategy, but most would be surprised to hear that upwards of 87% of container images in production **have been found to possess critical** vulnerabilities, with the average age of a vulnerability being **277 days**. Statistics like this show us just how important it is for organizations to modernize their image practices to meet the security demands of hybrid cloud environments.

We have found that one way to address vulnerabilities in infrastructure is to implement an industrialized, **immutable** approach to patching your system images. According to a **recent study**, 32 days is the mean time to exploit a vulnerability. Considering this, we suggest a preventative risk management approach. Our suggested workflow is a continuous 30-day repave cycle for all system images, this allows organizations to:

1. Prevent vulnerabilities from getting out into their infrastructure in the first place
2. Reduce the window for exploitation, continuously updating images before they reach the mean time to exploit

While implementing reactive security methods such as vulnerability scanning tools that check existing infrastructure is an important last line of defense in cloud security, you can think of our approach as proactive, like locking your door before you leave your house. By working to better secure infrastructure before deployment you alleviate the burden on these reactive methods, as there will be fewer vulnerabilities overall for security teams to deal with.

Manage

Monitor image health and simplify revocation

TLDR: HCP Terraform and HCP Packer also help ensure your images remain healthy over time and simplify decommissioning when it comes time to retire your infrastructure.

Once the new image version is successfully approved and provisioned, the next step is to perform **health assessments** to make sure this infrastructure doesn't change over time. Even with a standardized initial provisioning process, settings on infrastructure can still be modified or circumvented, opening up your infrastructure to the possibility of configuration drift. Drift is the term for when the real-world state of your infrastructure differs from the state defined in your configuration. Drift occurs when a user modifies resources outside of the Terraform workflow.

For example, a colleague may update resource configurations directly in the cloud provider console to resolve a production incident. HCP Terraform's **drift detection** allows users to actively monitor their infrastructure for these changes and receive alerts when they take place. From the health assessments dashboard they can quickly uncover the root cause for the change, determine if it is necessary, and accept it or automatically remediate if not.

HCP Terraform can also perform health checks for custom conditions and assertions with **continuous validation**. Users can monitor whether the functional validations defined in Terraform code continue to pass over time and receive an alert when an assertion fails. For example, you can monitor whether your website returns an expected status code, whether an API gateway certificate is valid, or whether the image artifact referenced from an HCP Packer channel is too old or has a scheduled revocation. Identifying failed checks helps you proactively resolve failures and prevent errors during your next Terraform operation.

If one of your golden images is outdated or possesses a vulnerability, you may need to revoke it to prevent infrastructure deployments from using it. HCP Packer and HCP Terraform help provide a fast, unified, and simple revocation workflow across downstream builds and

provisioning pipelines. When a golden image version is updated in an HCP Packer channel, any deployments using that image are simply re-run to pick up the new association. The technical effort to support the update is transparent for the practitioner because the Terraform data source integrates directly with HCP Packer to query the channel without hard-coding image identifiers. HCP Packer offers this simplified revocation workflow in three ways:

1. **Scheduled revocation**: Plan a revocation for a future end-of-life (EOL) date or revoke the image version immediately.
2. **Inherited revocation**: Building on HCP Packer's image ancestry tracking and established parent/child relationship to revoke just the base golden image or all associated downstream dependencies.
3. **Channel rollback**: Building on channel assignment history to provide quicker remediation of released artifacts by providing the option to roll back channels to their previously assigned version. This also works with HCP Packer's inherited revocation to automatically roll back the channel assignments of any descendant images when a parent image is revoked.

These two features provide users with flexible options to validate their infrastructure uptime, health, and security — all in one place without requiring additional tools.

Summary and next steps

Integrating HCP Packer's image management capabilities into existing HCP Terraform workflows brings a number of key benefits:

1. **Strengthen security and governance** - Secure images before deployment, continuously update, set EOL dates, and automate revocation.
2. **Accelerate innovation and efficiency** - Decrease time to deployment by reusing standardized golden images. Speed deployment by creating and reusing images from a single-source configuration file, connecting to VCS, and collaborating across teams,
3. **Optimize cloud operations and ROI** - Standardize image versions, change a golden image once, and automatically update across downstream builds.

Do cloud right at the image level to ensure consistent and secure infrastructure workflow across your organization as it grows in scale.

Try HCP Terraform and HCP Packer for free to begin unifying your imaging and provisioning workflows and simplifying infrastructure lifecycle management.

About HashiCorp

HashiCorp is The Infrastructure Cloud Company, helping organizations automate multi-cloud and hybrid environments with Infrastructure Lifecycle Management (ILM) and Security Lifecycle Management (SLM). HashiCorp offers The Infrastructure Cloud on the HashiCorp Cloud Platform (HCP) for managed cloud services, as well as self-hosted enterprise offerings and community source-available products. The company is headquartered in San Francisco, California.

For more information visit hashicorp.com