HashiCorp | DATADOG

Monitoring a Cloud Operating Model with Datadog

Accelerating Multi-cloud adoption through observability and the HashiCorp stack

WHITEPAPER

Contents

Executive Summary

The cloud demands a new operating model. Datacenter primitives are changing: static to dynamic infrastructure, security and networking policies based on identity rather than IP addresses, and an automated self-service platform as opposed to manual ticketing systems. While this transformation speeds development and shrinks go-to-market times, it renders much of the previous generation of tools and processes obsolete. To fully realize the benefits of cloud computing, enterprises must transition to scalable dynamic workflows and management at every cloud layer. From this they can deploy shared services enabled by platform teams to improve speed, increase efficiency, and decrease risk. Additionally, they need tools to monitor and audit these new systems and services to ensure they are operating as intended.

For most enterprises, digital transformation means delivering new business and customer value faster, at a very large scale. The implication for a cloud strategy/program office, then, is to balance the need for developer speed with cost optimization and risk mitigation. The cloud is an inevitable part of this shift as it presents the opportunity to rapidly deploy on-demand services with limitless scale. This re-platforming, driven by cloud services, requires new models for architecting applications and completely new approaches to infrastructure provisioning, security, networking, and deployment.

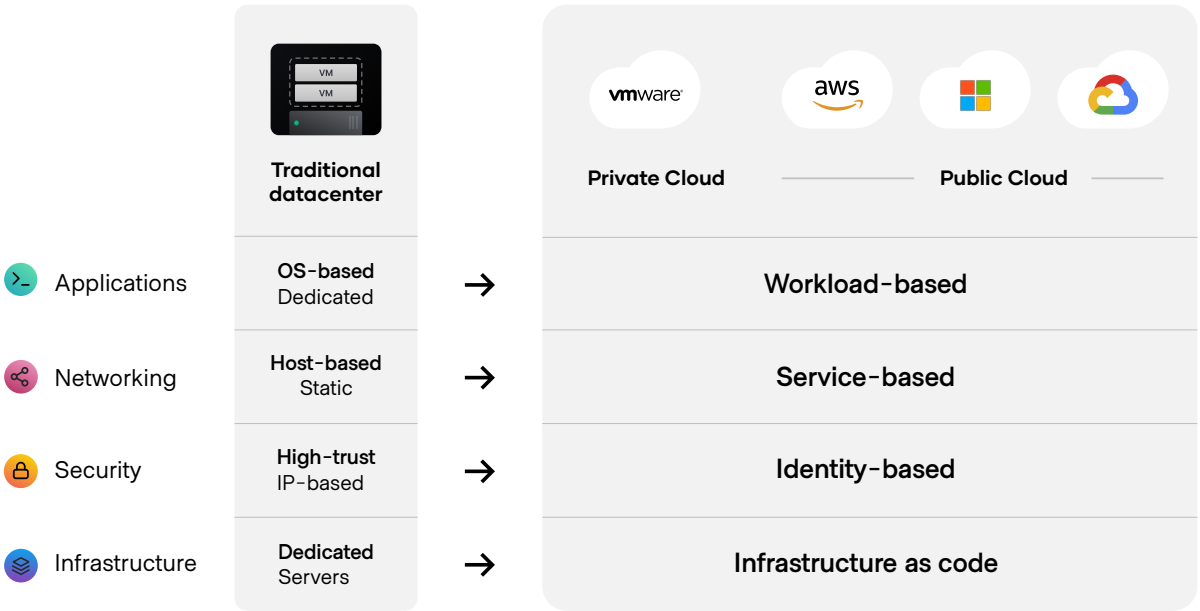
But as enterprises shift to a cloud operating model, they also must consider how to monitor dynamic cloud ecosystems. Datadog helps enterprises add observability to their environments by unifying telemetry data from across their technology stack. This helps IT teams monitor the health and performance of each layer of their infrastructure, get fast feedback on changes, and eliminate performance blind spots as they transition to the cloud.

In this white paper, we look at how Datadog and HashiCorp tools work together to help enterprises align on a clear strategy for not only cloud adoption, implementation, and usage but also observability into their infrastructure, security, networking, and application deployments.

A new cloud operating model

Cloud computing is a generational transition, shifting from largely static, dedicated servers in a private datacenter to a pool of service capacity available on demand from a variety of different providers. Successfully adopting the cloud means enabling a cloud operating model to address the transitional concerns at each operational layer: infrastructure, security, networking, and applications.

- For infrastructure, provisioning and management is done using infrastructure as code
- For security, brokering access to and management of sensitive data is based on identity
- For networking, access and connections are based on service identity
- For applications, deployment and management is workload-based



As infrastructure, security, networking, and applications teams move from traditional datacenters to the cloud, the foundations of each layer change.

For each layer the goal is to build a consistent system of engagement for developers and a system of record for the platform team — the team of cloud engineers responsible for implementing a cloud operating model as a platform of standardized shared tools and services.

Challenges of cloud adoption

With a transition to the cloud, organizations find themselves navigating the complexity of multi-cloud and a variety of different tooling and processes connected to each platform. Organizations bogged down in this tactical approach to their cloud adoption often struggle with inefficiency, security and compliance risk, and runaway costs from isolated teams and disconnected tools.

The answer to these challenges is a cloud operating model that enables standardized shared services at all layers of the cloud. Additionally, teams struggle with how to deliver and monitor these applications in the cloud with consistency while also ensuring the least possible friction across the various development teams. To reduce friction, the transition to the cloud requires facilitating observability in three areas:

1. **Monitoring ephemeral environments at scale:** Teams need to keep pace with the rate of change in a dynamic cloud environment. To accomplish this, they need observability tools that can auto-scale with their environments and provide real time data for monitoring the performance of ephemeral cloud resources as soon as they spin up.

2. **Monitoring complex infrastructure:** Cloud infrastructure can be complex, utilizing resources from various cloud providers, platforms, and technology stacks. Teams need to visualize the connections between all of these resources so they can efficiently diagnose performance problems.

3. **Monitoring for security and compliance:** For most modern applications, teams create security and compliance policies to ensure that sensitive data is safe. Enforcing these policies requires knowing when systems become vulnerable, so teams need to be able to monitor all service activity to detect potential threats and be aware of any compliance issues with new or modified cloud resources.

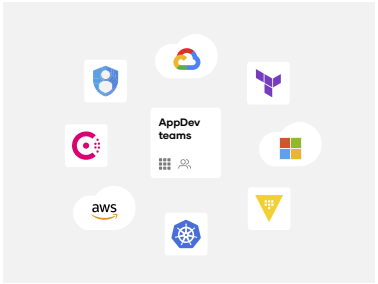
Successfully enabling a cloud operating model

Organizations that successfully enable a cloud operating model follow a typical blueprint called a maturity model and rely on centralized cloud platform teams.

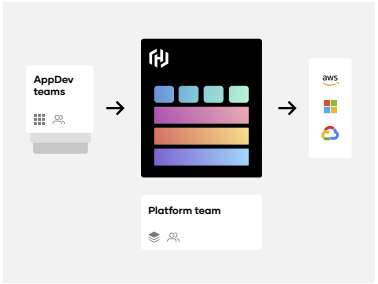
Cloud maturity model

Cloud adoption journeys typically follow an established pattern that flows through three stages:

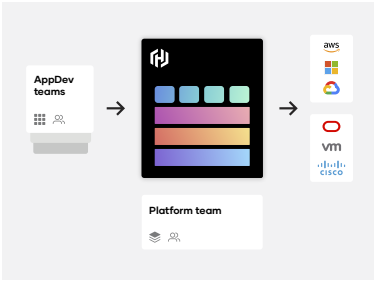
- **Stage 1: Adopting** — This is the beginning of cloud experimentation and usage, defined by individual teams engaging with cloud providers in silos to deliver applications and services. This leads to multiple different workflows, each best suited to a particular team's needs. At this stage there is no platform, limited knowledge share and minimal cloud operating strategy. This is what we refer to as a tactical cloud.
- **Stage 2: Standardizing** — As cloud usage increases, the organization shifts to strategic planning by a platform team to standardize the way developers interface with the cloud. The platform team is tasked with creating central services around provisioning, security, networking, and application deployment. This process accelerates developer productivity by removing the manual tasks associated with deploying cloud resources. At the same time, it reduces risk by providing a centralized way to apply corporate governance and security policies to all cloud-based resources. From here, teams adopt a cloud operating model resulting in the establishment of a cloud program.
- **Stage 3: Scaling** — Once established in a single cloud environment, platform teams can extend these workflows to other cloud vendors and across an organization's private estate, creating a consistent platform and system across all development and deployment areas. The team implements enterprise-scale solutions that can facilitate self-service cloud workflows across dozens or hundreds of teams.



Stage 1: Adopting



Stage 2: Standardizing



Stage 3: Scaling

Platform teams accelerate cloud adoption

The platform team is responsible for delivering each layer of a cloud operating model as a standardized shared service that can be consumed by end-users in the organizations.

In addition to providing standardized shared services, the platform team:

- **Establishes best practices for developers and practitioners** to engage with cloud services. These best practices are then codified directly into workflows and educational programs such as Cloud Centers of Excellence (CCoEs).
- **Serves as a single point of integration for other corporate teams**, including security, compliance, financial controls, etc. to ensure that their best practices are baked into relevant workflows.
- **Provides a central system for tracking, reporting, and auditing** to inform adoption and usage of the cloud operating model. This informs progress of the organization and highlights areas where there may be risk exposure: such as security, compliance, and spending.

Enterprise platform capabilities

The key to implementing a cloud operating model is the creation of consistent workflows and processes. These drive the delivery of core capabilities organizations need for their cloud platform. We have identified six functional areas that need to be built into the cloud platform:

1. **Unified workflow management:** Implement central leadership and processes to unify common workflows across all cloud layers and teams.
2. **Reliability and scale:** Create solutions for the cloud platform that are dependable and perform consistently at scale across all levels of an organization.
3. **Policy and security:** Incorporate tools to enable the integration of policies and guardrails directly into your workflows and cloud platform.
4. **Governance, risk, and compliance:** Establish a consistent philosophy for the integration of security and compliance frameworks directly into all layers of the cloud platform.
5. **Visibility and optimization:** Build tools and dashboards to view and audit all aspects of your cloud platform to ensure consistent performance and drive optimization.
6. **Integration and API-driven workflows:** Create tooling and integrations to ensure the platform has the functionality required and can be easily adopted by the organization.

As organizations mature in the cloud adoption journey, they must create an effective plan for monitoring cloud resources, with the following observability goals:

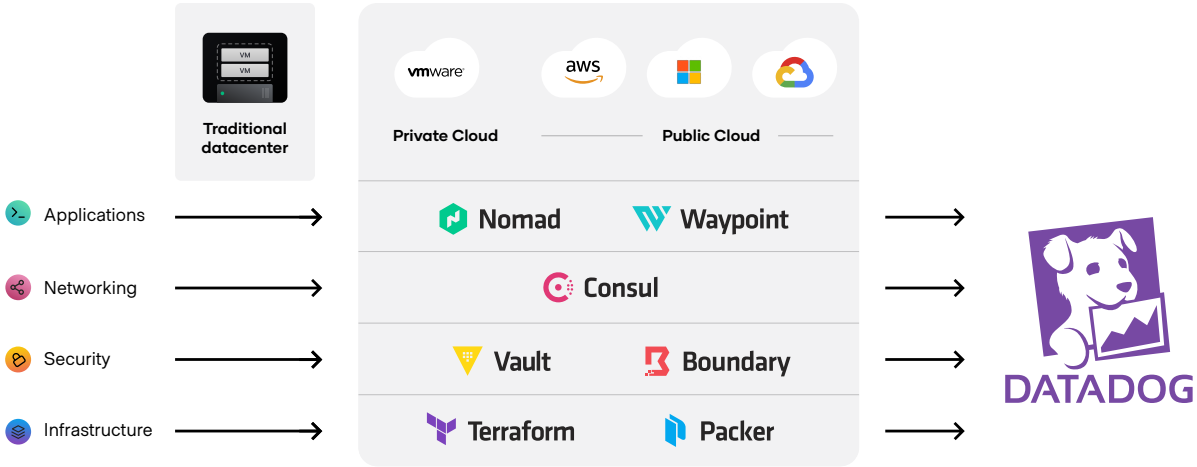
- **Collect the right data:** Cloud resources generate a wealth of data for identifying and investigating problems. Knowing which kinds of data to collect, such as metrics and events, gives teams more complete visibility into their systems. This enables them to create meaningful alerts and quickly investigate performance issues in cloud environments.
- **Alert on what matters:** Automated alerts draw attention to service degradations and disruption, enabling teams to quickly respond to an issue before it becomes more serious. However, not all alerts are useful or carry the same level of urgency. High-severity alerts can be used as direct pages while low-severity ones are better suited as records of activity. Because of this, teams need to look at what types of notifications are most important for their environments.

- **Investigate performance issues:** Once an alert is triggered for an issue that requires attention, teams can use the monitoring data they have collected to swiftly diagnose the root cause. They can start their investigations by first looking at metrics and associated events from their highest-level systems then drilling down to other affected layers of their environments.

By considering these goals, teams can have visibility into the health and performance of their systems at any stage of the transition to a cloud operating model. Datadog brings together all of an environment's metrics, traces, logs, and other telemetry, giving teams a single source of truth for visualizing the connections between services, collaborating on real-time data, and investigating issues across infrastructure, security, networking, and application cloud layers.

Monitoring a Cloud Operating Model with Datadog

HashiCorp provides a platform of products for cloud infrastructure automation to enable a cloud operating model. The implications of this model affect teams across operations, security, networking, and development. To successfully deliver the dynamic infrastructure necessary for each layer, enterprises need a system of shared services for their teams managed centrally by a platform team. This includes leveraging observability platforms like Datadog to consolidate the separate systems teams use to monitor their applications and underlying IT infrastructure.



Infrastructure layer

As organizations move from on-premises infrastructure to cloud infrastructure, operators face new challenges:

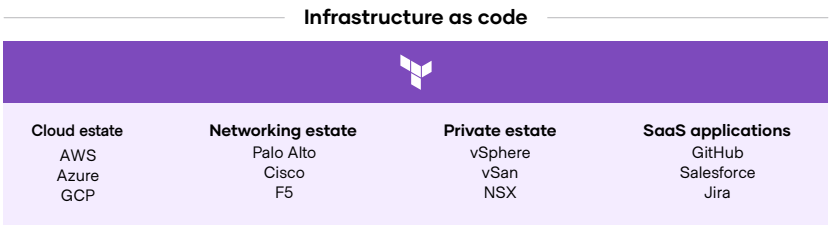
- **Scale:** Teams want to quickly scale their infrastructure usage up and down with no errors despite potentially extensive configuration changes.
- **Variety:** Teams want unified provisioning workflows on a variety of platforms.
- **Dependencies:** Teams want to include and automate existing services and dependencies into configurations as part of this provisioning workflow.

The foundational layer of a cloud operating model is infrastructure provisioning using an infrastructure as code (IaC) approach. Converting infrastructure into code allows teams to declaratively define the

desired end state of their infrastructure, ensuring consistency in every deployment, while also allowing them to track and audit changes to that code.

Infrastructure provisioning with HashiCorp Terraform and Datadog

HashiCorp Terraform enables this IaC provisioning of infrastructure. With a fully extensible engine, it has thousands of pre-built integrations with cloud providers and popular software applications to make it the central tool for all infrastructure provisioning use cases:



By creating a shared service for infrastructure provisioning, Terraform provides product teams a way to plan and provision all of these resource types inside CI/CD workflows using familiar tools. That makes Terraform the lingua franca and common workflow for teams provisioning resources to help their platform scale and extend its capabilities. As organizations mature in their cloud journey, Terraform supports more advanced services that enable it to be run as a shared service to facilitate all infrastructure across an organization's varied hybrid estates.

These shared services allow platform teams to deploy common workflows to fit their core needs. Teams can increase productivity with change tracking and versioning, reusability, and centralized configuration. They can use the same workflow to manage multiple cloud providers and handle cross-cloud dependencies with 2,500+ public providers in the Terraform Registry. And they can extend Terraform's automation with CI/CD integrations, API access, and third-party services with run tasks.

Additionally, Platform teams can reduce the risk of misconfigurations by enforcing guardrails for security, compliance, cost, and organizational best practices before infrastructure is provisioned with a combination of Sentinel (HashiCorp's policy as code framework), other policy frameworks like Open Policy Agent (OPA), and third-party checks integrated through Terraform run tasks. Plus, Drift Detection for Terraform preemptively detects when a resource has changed from the expected state, helping reduce security and operational risks.

Reproducible monitoring as code

HashiCorp and Datadog have partnered to develop the HashiCorp Terraform Verified Provider

for Datadog so teams can leverage Datadog's extensive API library with templates in order to add monitoring as code to their provisioning workflows. Teams can deploy any Datadog resource alongside new or existing infrastructure, which significantly reduces the gaps in visibility between services. With the Datadog provider, teams can use Terraform to:

- Deploy monitors and dashboards for new and existing resources automatically
- Set up integrations for cloud providers like Amazon Web Services, Microsoft Azure, and Google Cloud
- Create new synthetic tests to verify application behavior in new environments
- Create service-level objectives for newly deployed applications

Datadog can also visualize all resources managed by Terraform. Terraform Cloud provides access to an Audit Trails API, which exposes a stream of audit events describing changes to the application entities (workspaces, runs, etc.) within a Terraform Cloud organization. By tying observability to infrastructure, Terraform and Datadog become the standard for provisioning application resources and monitoring their performance. Practitioners can import Terraform Cloud audit logs into Datadog and gain greater visibility into the details of their operation.

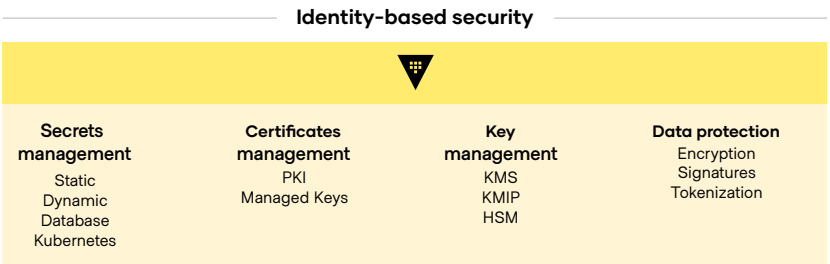
Security layer

On-premises infrastructure environments have traditionally been designed as high-trust networks. Robust firewalls secure the perimeter of the network, and traffic inside is implicitly trusted. In modern cloud environments, this traditional security perimeter no longer exists, so trust must be based on the identity of the requesting entity. IP addresses are no longer a scalable or safe form of identity since they are highly ephemeral in a cloud environment.

As a result, the security layer of a cloud operating model should be built on the principles of zero trust security, which means to trust nothing and authenticate everything. In other words, all traffic inside your network needs to be authenticated (ideally via mTLS) every time someone wants to access infrastructure resources or a service talks to another. Hence, identity becomes the cloud control point for security.

Manage secrets and protect data with HashiCorp Vault and Datadog

HashiCorp Vault provides security automation to manage access to secrets and protect sensitive data. The secrets management layer aims to establish a centralized security automation platform as a shared service to the rest of the organization. This standardizes the workflow to manage the entire lifecycle of secrets management from acquisition to rotation to revocation, while auditing ensures those secrets meet your internal security compliance requirements. Built around identity-based security as the foundation of an organization's zero trust security implementation, Vault covers the core cloud security use cases organizations face:

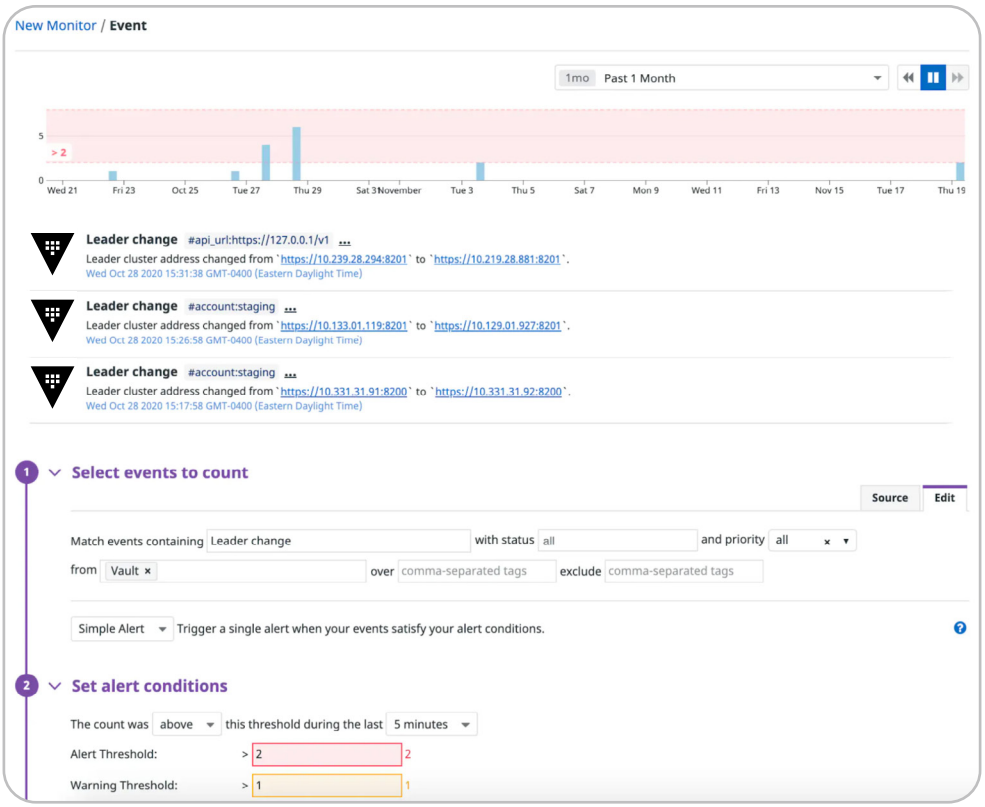


Through all of these use cases, Vault is the identity broker that enables platform teams to securely store and tightly control access to secrets, credentials, tokens, passwords, certificates, encryption keys, and data. First, organizations build out shared services enabled by integrations with more than 100 partners and software tools to enable centralized secrets management services. This is the foundation to deliver more advanced security services. Teams can integrate encryption as a service, automated

secrets rotations, and advanced data protection across their entire hybrid estate. This embeds security considerations within the platform, so product teams need only "plug in" to the provided APIs to ensure their service meets corporate security standards.

Ensure healthy Vault clusters

Using Vault as the basis of secrets management and data protection, requires visibility into the state and performance of Vault clusters. Without this visibility, teams may overlook issues that affect the performance of their clusters and dependent services. For example, teams need to be aware of high leadership turnover in a Vault cluster before any services that leverage secrets to communicate with downstream clients become unstable.



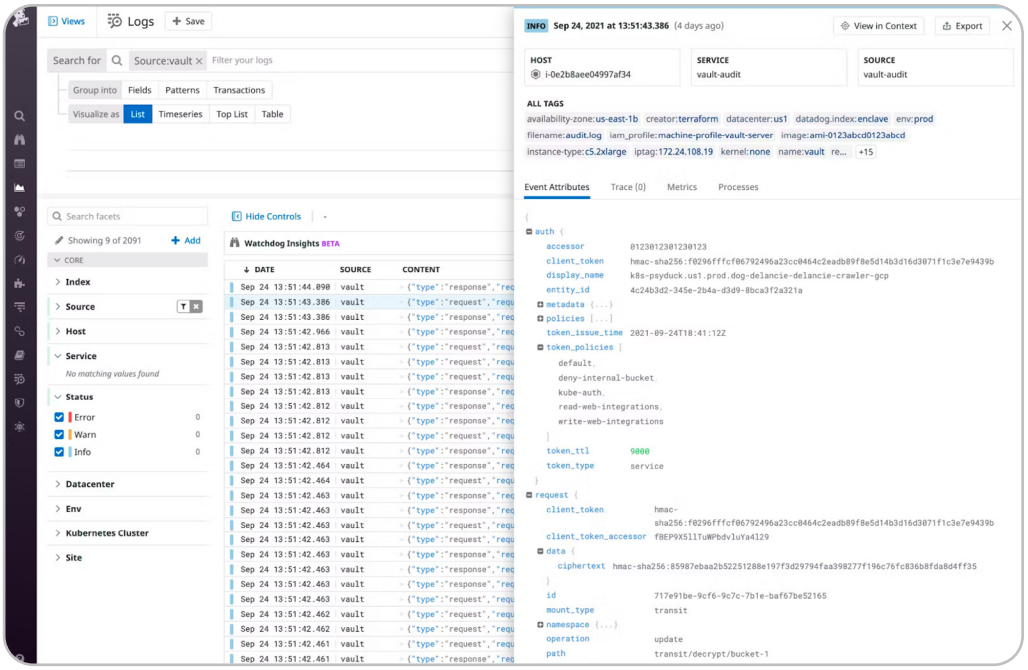
Datadog provides full visibility into Vault cluster health and performance by collecting key metrics and logs from Vault servers. This enables teams to readily detect potential security issues, including high leadership turnover, and to track long-term cluster performance trends. Teams can also use this data to create a variety of automated alerts for cluster performance issues, including forecasting alerts to account for periodic fluctuations in cluster metrics.

Monitor HashiCorp Vault Security with Datadog

To detect potential malicious activity in your Vault installation, Datadog Cloud SIEM automatically analyzes Vault audit logs as they're ingested. You can use Datadog to continuously monitor your Vault audit logs for signs of any of the security threats we looked at in the previous section. Datadog also gives you visibility into your Vault server logs, which can help you understand your server's performance and provide context around the information in the audit logs. In this section, we'll show you how Datadog provides automated threat detection and alerting so you can be sure your secrets are secure.

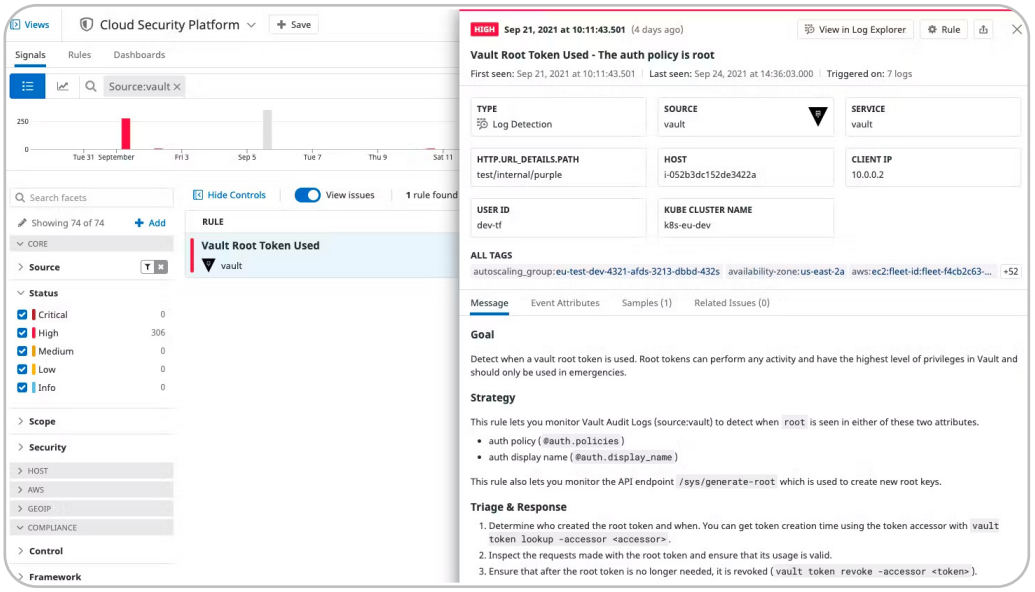
Collect Vault audit logs

Datadog's Vault integration lets you collect Vault metrics so you can understand its performance, as well as Vault audit logs to use as the basis for automated security monitoring. To monitor Vault security with Datadog, you'll need to enable both Vault auditing and the Vault integration. And you'll need to configure the integration to collect your Vault logs. As your Vault audit logs come into Datadog, log pipelines automatically parse and enrich them, so you can easily search for them (example., by source:vault) in the Log Explorer, as shown in the screenshot below. The highlighted log shows the attributes you can use to search, filter, and analyze your Vault audit logs.



Detect threats to Vault with Datadog Cloud SIEM

Datadog Cloud SIEM's out-of-the-box security rules help detect potentially malicious activity in your Vault audit logs. If a log violates a security rule, Datadog automatically generates a security signal that provides information to help you triage the issue. You can use these out-of-the-box security rules to automatically jump-start your Vault monitoring. The screenshot below shows an example of the security signal generated by the root token usage rule, and could indicate that a malicious actor is trying to escalate their privileges.

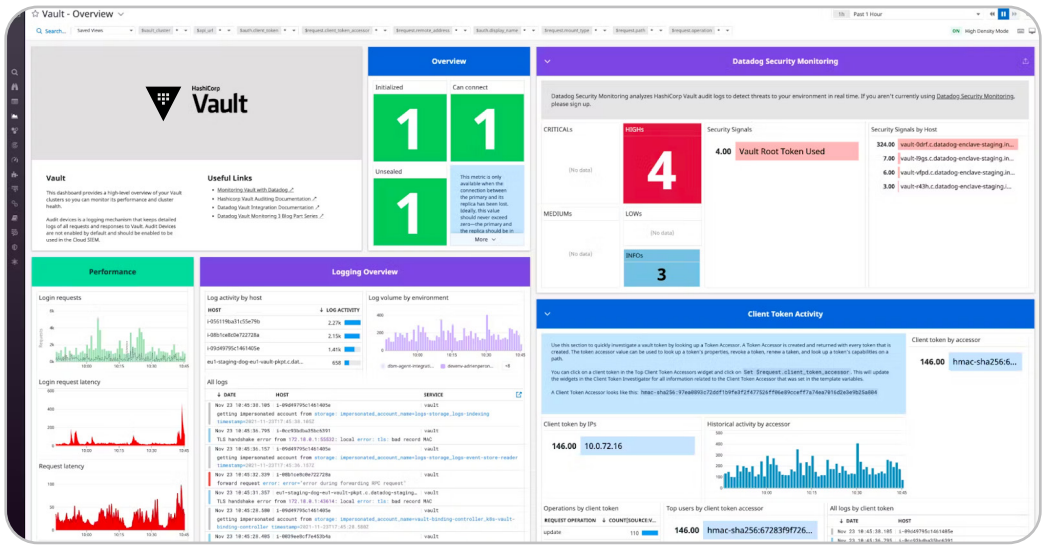


A root token allows an attacker to access Vault secrets and modify Vault policies, so it's important to detect and investigate anytime one is created or used. There are valid reasons for using a root token, but Hashicorp recommends limiting their use, so this rule can also help you ensure that you're following best practices. You can also leverage custom security rules targeted to your specific Vault use case, either by creating a new rule or cloning and modifying a built-in rule. For example, Datadog provides a rule that detects high TTL values on Vault tokens. Excessive TTL values can weaken your security by increasing an attacker's window of elevated privileges. The safest value for a TTL depends on how you use Vault—for instance, you may use a six-hour TTL for user tokens but a one-hour TTL for tokens issued to your cloud provider. You can clone the built-in rule to create one or more custom rules, revising auth.token_ttl to an acceptable value for each use case. Security rules like this use your Vault audit logs as the basis to detect possible attacks, but you can also create rules based on other

logs to gain a broader security perspective. For example, if any of your Vault hosts are accessible from the internet, you can create a rule to detect failed login attempts in your Vault host's authentication log (example /var/log/auth.log).

Visualize and alert on Vault security

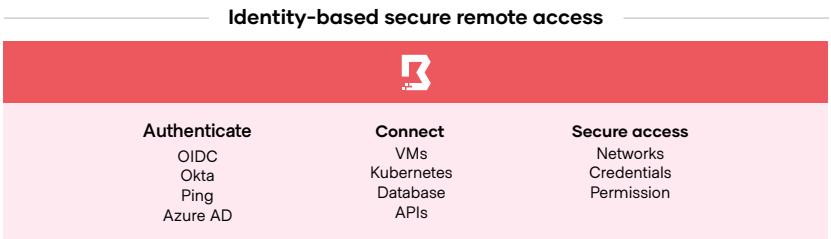
Datadog dashboards give you customizable visualizations of more than 600 technologies. Datadog's out-of-the-box Vault dashboard visualizes activity and performance metrics from your Vault cluster and shows you Vault logs so you can analyze trends in Vault activity and spot changes that could indicate a security concern.



Your Vault Security dashboard will often show typical patterns—such as a high ratio of update and read operations compared to delete and list operations, as seen in the Vault Operations widget. But your use case may generate some unique patterns, too, and the dashboard can help you quickly identify any variations from expected behavior.

Secure, manage, and monitor access with HashiCorp Boundary and Datadog

Secrets management mainly handles the machine-to-machine side of zero trust security. Another solution is required for human-to-machine access. Traditional solutions for safeguarding user access, like distributing and managing SSH keys, VPN credentials, and bastion hosts either don't scale well in the cloud or have significant risks and require substantial manual effort. HashiCorp Boundary is a secure remote-access solution that solves these challenges. Boundary provides an easy way to safeguard access to applications and critical systems with fine-grained authorizations based on trusted identities. Boundary supports organizations' identity-based secure remote-access automation use cases to manage access across any environment:



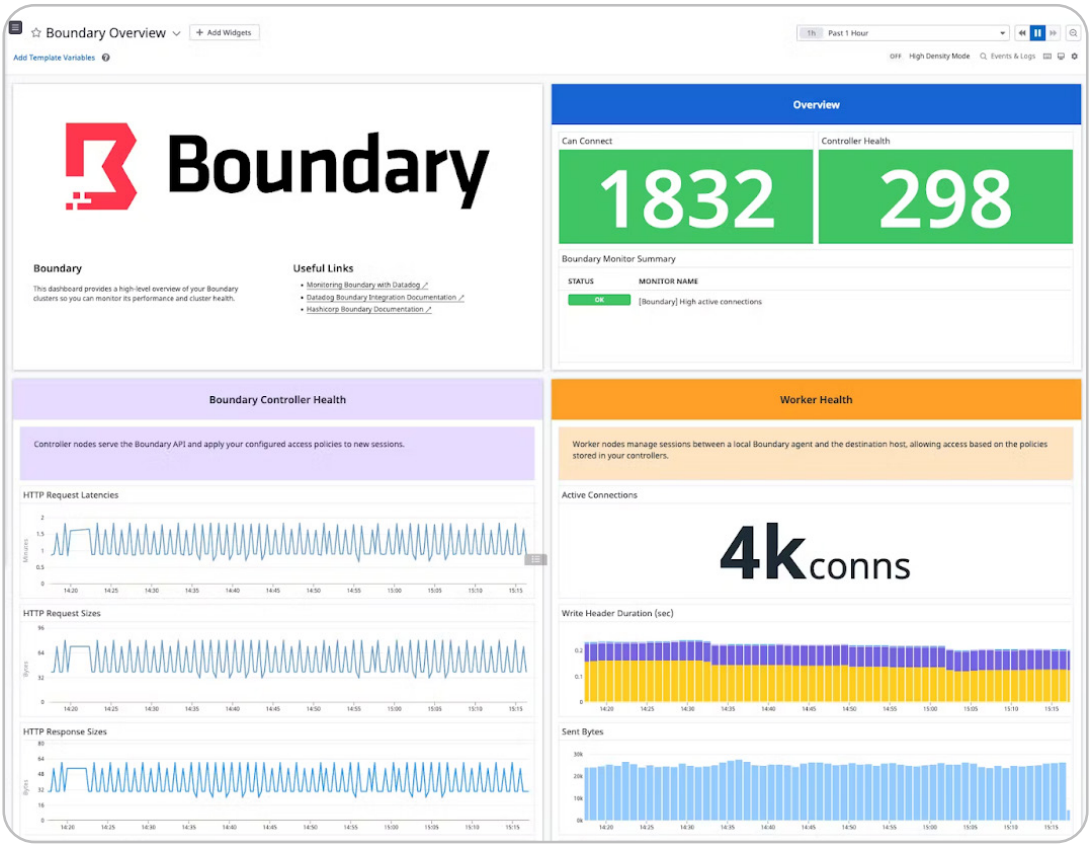
By leveraging Boundary, platform teams can connect users to clouds, local datacenters, and low-trust networks without exposing the underlying network. In a modern secure remote-access session, the user will never be directly on the network, and they'll have precise permissions so they can access only the infrastructure they need, when they need it.

Comprehensive visibility into infrastructure access

Datadog has partnered with HashiCorp to create a turn-key HCP Boundary integration that provides comprehensive visibility into infrastructure access. Teams can leverage real-time audit log streaming and an out-of-the-box dashboard to monitor the health and performance of HCP Boundary instances and track all user sessions within their environment. These integrations allow users to:

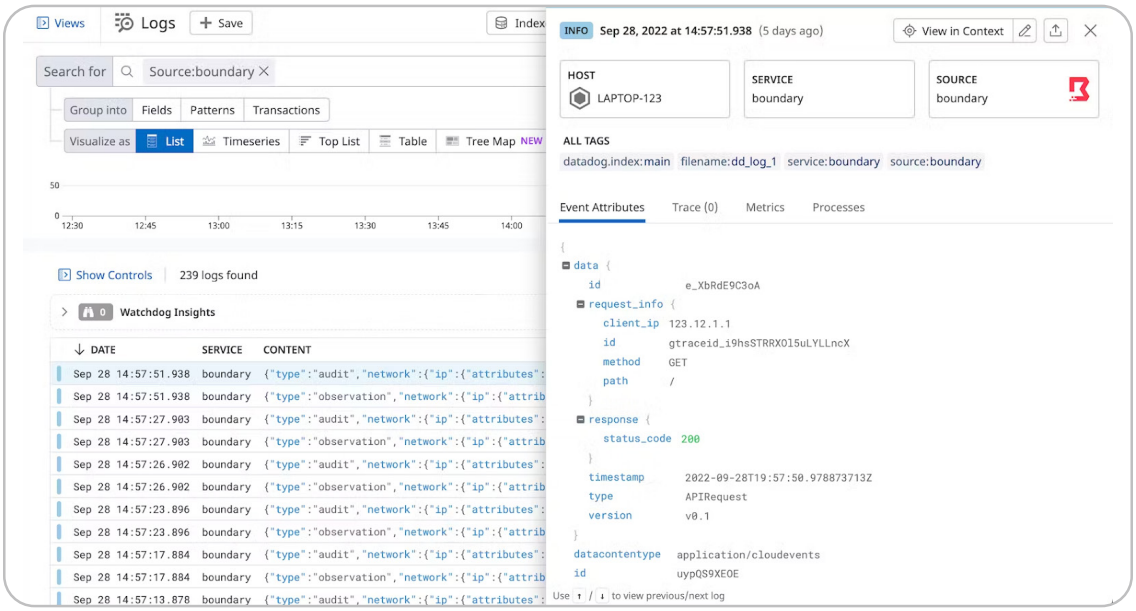
- Track HCP Boundary performance
- Get alerts on the status of HCP Boundary instances
- Monitor event logs for suspicious or unusual activity

A key part of maintaining your HCP Boundary instances is monitoring the performance of their underlying infrastructure, which is made up of controller and worker nodes. Both of these components expose metrics via the OpenMetrics exposition format, which Datadog can automatically collect and display in its out-of-the-box integration dashboard.



The dashboard gives you an overview of key performance metrics for your HCP Boundary instances, such as the number of active connections per worker or request latency for controllers. This visibility is critical for monitoring HCP Boundary performance in large-scale environments, such as those that are deployed across multiple data centers or clouds.

Since HCP Boundary helps organizations manage access to their resources, it's important to ensure that access policies are working as expected. Datadog can do this by monitoring HCP Boundary event logs, which capture details about all user sessions across environments. This data gives complete visibility into who accessed applications, when they accessed them, and what methods they used for authentication.



Datadog automatically collects all event logs from HCP Boundary, enabling teams to review them in the Log Explorer and identify unusual or malicious activity. Additionally, platform teams can leverage HashiCorp's Boundary Terraform provider to automatically provision and manage access controls and ensure that there are no gaps in policies.

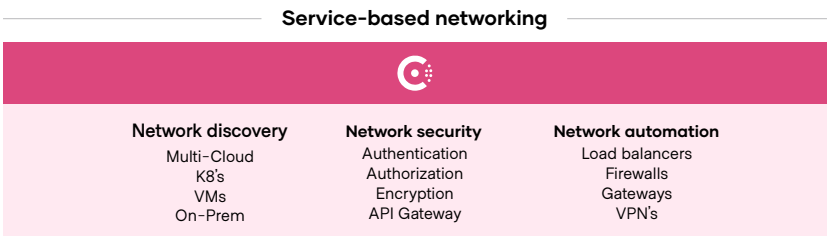
Networking layer

Networking in the cloud is one of the most difficult challenges for organizations. Engineers must navigate dynamic IP addresses, manage a significant growth in east-west traffic for microservice implementations, and adjust to the lack of a clear network perimeter. With the volume and variety of networking requirements in cloud environments, legacy ticket-driven workflows should be replaced by automated processes to unlock the speed and scaling promises of cloud-native applications.

The first step in adopting a cloud operating model at the networking layer is to find a solution that drives the discovery, registering, and connection of your services, applications, and environments. Organizations can then use this foundation to facilitate proper identity-based zero trust networking policies and advanced networking systems, such as a service mesh.

Securely connect and monitor apps with HashiCorp Consul and Datadog

HashiCorp Consul enables platform teams to overcome these networking challenges by automating service networking across their entire cloud estate. Consul covers the core networking use cases that organizations must adopt as part of a cloud operating model:



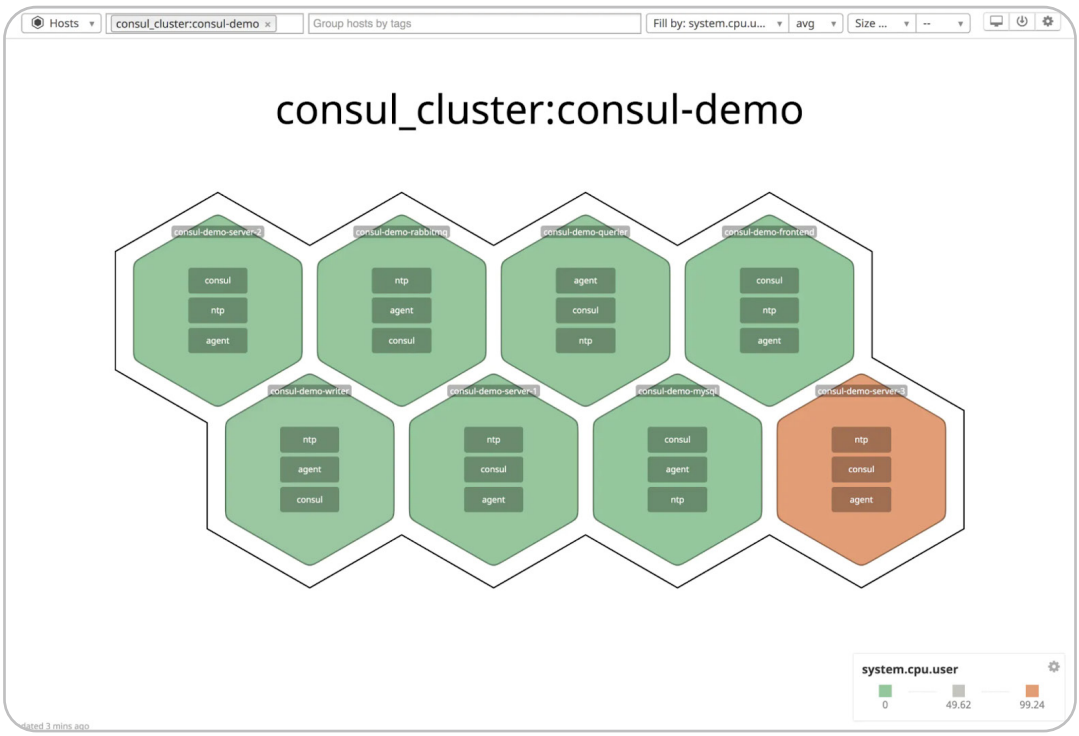
To start, Consul facilitates the discovery, registration, and connection of all services in your application environment. This registry provides a "map" of what services are running, where they are, and their current health. Next, these connections can be secured based on service identities (not IP addresses), a key component in a zero trust architecture. This enables proper authorization and access to only required services as opposed to full network access. From there, platform teams can reduce the operational complexity of existing networking infrastructure through automation.

As network scale expands, network complexity grows exponentially. To cope with this complexity, Consul can provide a service mesh as a central networking control plane. This service mesh contains all necessary networking services including service discovery, secured service-to-service communication, and traffic management — all bundled in one interface. This enables a networking

platform that developers can use to leverage the secure network layer without needing to manually deploy or understand all of the underlying technology.

Maintain stable Consul clusters

Because Consul manages the network and configuration details that distributed services rely on for communication, monitoring the health of Consul clusters is key to ensuring those services continue performing as expected. Datadog's built-in Consul integration collects Consul-generated metrics and logs, giving teams greater visibility into cluster health so that they can prevent outages before they occur.



Datadog provides a real-time view of the state of a Consul cluster with host maps. Teams can group hosts by tags so they can determine if a performance issue is affecting individual nodes or an entire cluster. Teams can also monitor key cluster metrics and create alerts for critical issues that can affect Consul's overall stability, such as frequent leadership transitions.

Monitor service performance

Implementing a service discovery solution creates the foundation for improved analytics and performance monitoring. Beyond tracking the health of Consul clusters, Consul and Datadog can integrate to collect service level data such as error rates, request per second, total connections, and more. Using this data, teams can gain greater insights into how their services are running and identify specific areas of improvement.

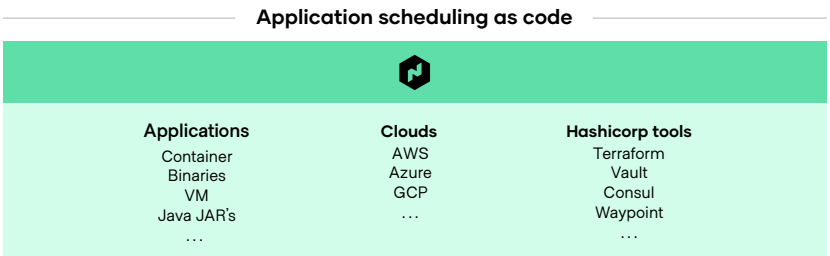
As organizations move towards a service mesh architecture, teams can implement distributed tracing within their applications to monitor the path of requests as they cross service and process boundaries. In distributed systems, individual requests may travel through multiple services (e.g., sidecar proxies, APIs, etc.) before resolving. Capturing performance data at each service endpoint enables organizations to identify bottlenecks so they can reroute traffic to healthy endpoints. Consul and Datadog make it possible to both capture and visualize this information, enabling greater observability into network performance.

Application layer

Application teams strive to deliver code and software updates faster as organizations start building in the cloud. Traditional IT practices can hold them back, however, requiring developers to go through complex ticket-driven workflows that take days, weeks, or months to deploy new applications. On top of this, even as new cloud-native applications are built, legacy application deployments still need to be managed in parallel, ideally through one workflow and interface. New tools are required to facilitate the needs of building, deploying, and running multiple applications in the cloud.

Standardize application scheduling with HashiCorp Nomad and Datadog

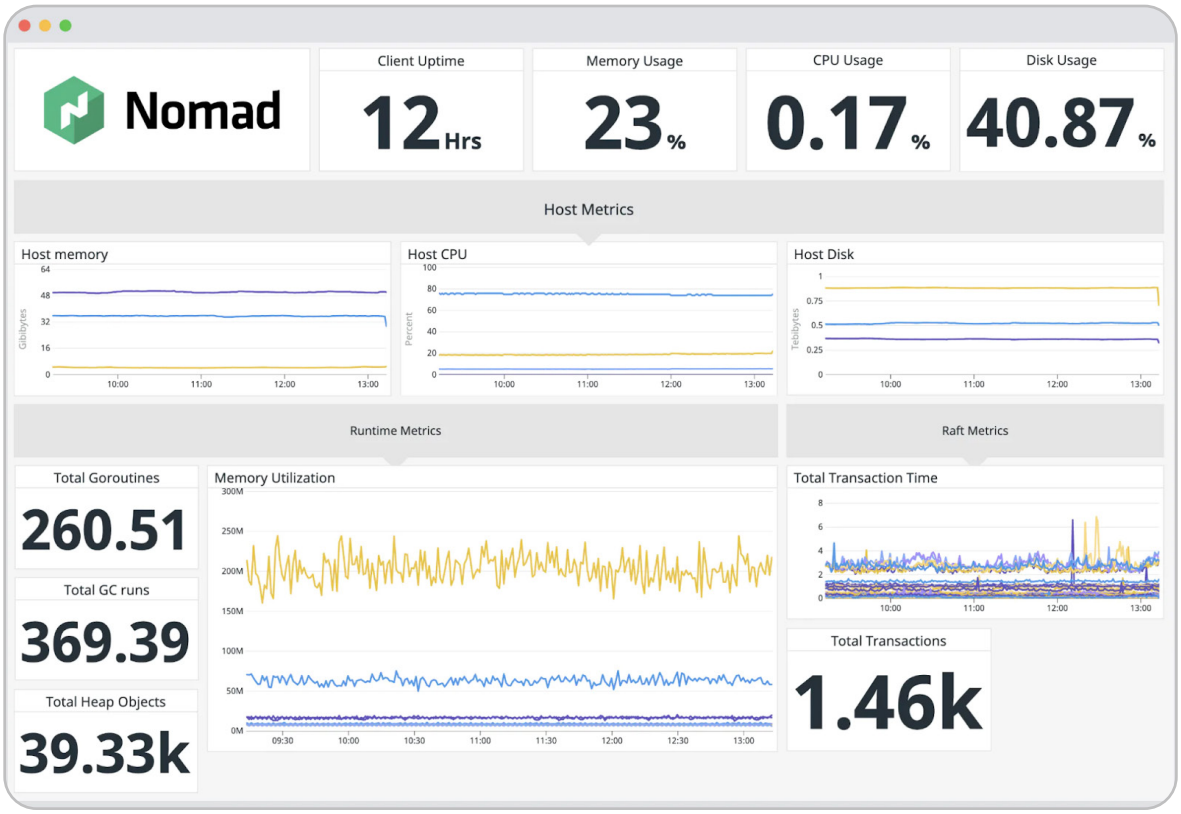
HashiCorp Nomad is a flexible application scheduler that can deploy and manage both traditional and modern applications for all types of workloads. It serves as a coordination layer between developers and operators, providing automated deployment (no more tickets), efficient server utilization (cost reduction), and easy workload management. It helps with the common use cases organization experience as they schedule their applications across multiple formats, operating systems, and environments:



Nomad is flexible enough for all major cloud environments, operating systems, and workload types, with functionality to support new workload types in the future. Plus, Nomad's integrations with Terraform, Vault, Consul, and Waypoint enable consistent delivery of applications, while meeting necessary compliance, security, and networking requirements.

Monitor Nomad cluster performance and availability

Teams can use Datadog's Nomad integration to capture key metrics from Nomad clusters, so they can monitor performance indicators such as cluster capacity, job status, and memory pressure. Since Nomad clusters share resources to run a variety of workloads, monitoring capacity and other performance indicators helps ensure that clusters have enough resources to run all of them optimally.



Teams can also leverage tags to track the performance of specific workloads, such as those that execute long-running processes. And with Datadog's alerting capabilities, teams can be automatically notified as soon as key cluster metrics, such as CPU utilization or memory usage, reach specified thresholds. This enables teams to address performance issues for critical workloads and maintain cluster stability.

Autoscale Nomad workloads and clusters to meet real-time demands

Nomad provides an autoscaler for scaling workloads and clusters horizontally in order to meet real time demand. Teams can leverage the autoscaler's Datadog APM plugin in their autoscaling policies to schedule when to modify resources based on specific metrics captured by Datadog, such as an underlying host's CPU and memory utilization. By using Datadog to help make scaling decisions, teams can ensure they always have sufficient resources to support their applications.

Conclusion

The cloud is the most fundamental shift in computing over the last 20 years. But while it promises dramatic advances in how organizations innovate, respond to market trends, and connect with their customers and employees, it also requires significant changes in how applications are built, deployed, and managed.

Coping with those changes requires core shifts in 3 key areas to promote greater efficiency through unified workflows:

- **People:** Shift to platform engineering practices to enable cloud and platform engineers to automate with code and treat operations as a software problem.
- **Processes:** Establish centers of excellence for infrastructure, security, networking, and other functional areas for self-service delivery of capabilities.
- **Tools:** Switch to dynamic environments that use tools that support the increasing ephemerality and distribution of infrastructure and applications to power critical workflows rather than being tied to specific technologies.

Adopting a cloud operating model is a critical step for enterprises aiming to maximize their digital transformation efforts. The cloud strategy/program office is evolving away from ITIL-based control points — focused on cost — toward becoming self-service enablers focused on speed. They enable product teams to deliver new business and customer value efficiently, at speed, and with reduced risk.

Observability is an essential shared service across infrastructure, security, networking, and application cloud layers. Datadog and HashiCorp are working together to promote a smooth transition to the cloud by equipping platform teams with the appropriate suite of tools for deploying to, securing, and monitoring in the cloud.

Datadog supports this transition by establishing an enterprise-wide monitoring standard, delivering end-to-end visibility across each layer of cloud applications by unifying telemetry data from HashiCorp Terraform, Vault, Consul, and Nomad. This enables enterprises to collaborate around a single source of truth, using real-time data to visualize the connections between services and components in the cloud and identify the source of performance issues before they significantly affect users.

With HashiCorp and Datadog's suite of products, platform teams are empowered to successfully lead this shift to a cloud operating model with solutions for each layer of their cloud infrastructure.

Learn more about how HashiCorp and Datadog can make the cloud operating model a reality for you at www.hashicorp.com and www.datadoghq.com

HashiCorp