White Paper

# Zscaler and Consul–Terraform–Sync (CTS)

## Achieve Dynamic Zero Trust Services Configuration with Zscaler and Consul–Terraform–Sync

© 2023 Zscaler, Inc. All rights reserved.

## The Challenge

Organizations around the world are looking for greater agility and scale for their application deployments. Application teams are adopting new practices and technologies such as DevOps, Infrastructure–as–Code, and microservices architectures with a focus on enabling self–service and faster application deployment.

With that comes increased complexity in managing the security policies and compliance for those applications. This is exacerbated by the technical difficulties experienced by the security teams who use manual processes for change management, leading to delays in implementation and operations.

Application developers that need to scale their applications are typically required to create new change management tickets that flow through multiple teams in the organization; such as system admins, network admins, and security operations – all of which have their own timelines and requirements to ensure a change can be deployed. Additionally, with developers requiring more autonomy and velocity, there's an increased need to remove silos, eliminate handoffs, and finally accelerate feedback to deliver value to the users faster. All these promises and challenges increase the risk of mistakes, slow the process, prevent a standardized deployment model and affect the user's experience.

An application can be made both continuously secure and reliable with closer collaboration between the DevOps and Security teams, thereby reinforcing security at every stage of the development pipeline. Transparent security promotes expedited application deployment and makes the DevOps team an equal stakeholder in producing highly resilient and secure applications.

### DevOps and Security Challenges

- Prevent resource strain and skill gaps leading to misconfigurations
- Eliminate manual ticketing process and reduce risk through zero touch application delivery with Zscaler Private Access.
- Make applications available to users quickly and securely

© 2023 Zscaler, Inc. All rights reserved.

## Product Integration

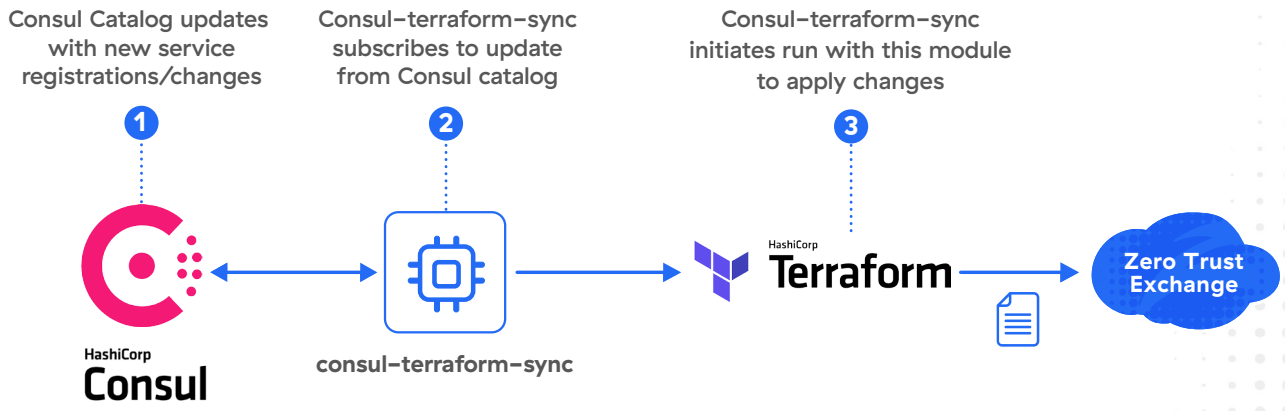
**Zscaler + Consul–Terraform–Sync (CTS)**

The Zscaler Terraform modules for Consul–Terraform–Sync enable network infrastructure automation (NIA) for security and network teams working closely with App and Platform (DevOps) teams to dynamically configure application segments and application servers in the ZPA platform.

As new services are registered in or deregistered from the Consul catalog, Consul–Terraform–Sync updates application segments or application server IP addresses, FQDNs, and TCP/UDP ports for the relevant endpoints in the ZPA platform.

The module is also designed to update Zscaler Internet Access (ZIA) Cloud Firewall module IP Source Groups to ensure only authorized IP addresses monitored by Consul are authorized via predefined Cloud Firewall rules.

Consul–Terraform–Sync improves the application delivery process as it removes the reliance on manual ticket creation for ZPA and ZIA administrators to configure or update application segments, application servers, and cloud firewall IP source groups. Administrators no longer have to rely on tedious and manual processes for analysis and implementation of change management.




© 2023 Zscaler, Inc. All rights reserved.

## How the Integration Works

HashiCorp Consul is a service mesh solution that helps organizations discover and securely connect any service, across any environment. Consul helps customers consolidate all their services in a centralized registry with real-time health checks for availability.

Without Consul, tracking and connecting applications is a manual and intensive process, which makes it prone to mistakes. Using Consul as a source of truth for the location and health of all services, we can automate networking tasks – like changes on Zscaler firewalls – and reduce the burden on network operators.

Consul-Terraform-Sync runs a daemon that watches Consul state changes at the application layer (based on service health changes, new instances deployed, etc.) and forwards the data to the Zscaler Terraform modules that are automatically triggered.

Zscaler integration with Consul-Terraform-Sync (CTS) provides three different modules for complete Network Infrastructure Automation (NIA).

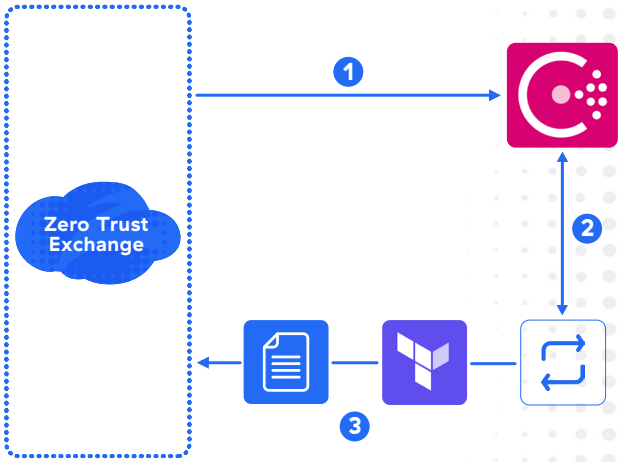
- **ZPA Application Segments:** Add, update, and delete IP addresses, FQDNs, TCP/UDP Ports
- **ZPA Application Servers:** Add, update, and delete application server objects
- **ZIA Cloud Firewall IP Source Groups:** Add, update, and delete IP address entries in a Source Group object and automatically update existing firewall policies.

Using this Terraform module in conjunction with Consul-Terraform-Sync enables teams to reduce manual ticketing processes and automate Day-N operations to be constantly aligned with your application state, while 100% of the process is encapsulated into a declarative model.

**Eliminate manual ticketing process and reduce risk**

1. Consul sends updated service-level information
2. Consul-Terraform-Sync receives updated data
3. The configured Terraform module is triggered

In addition to the benefits mentioned so far, the integration with Consul-Terraform-Sync guarantees that your automation process is easily repeatable, consistent, and secure.



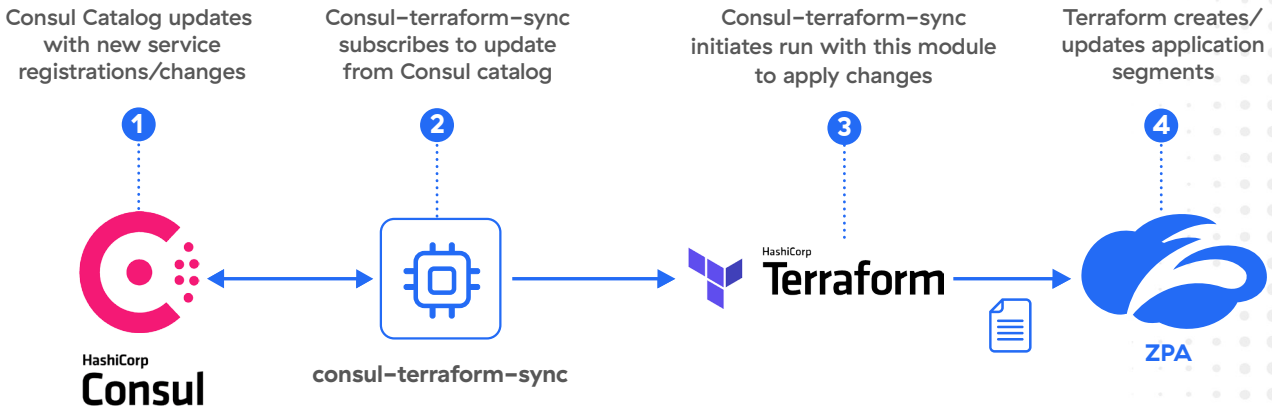

© 2023 Zscaler, Inc. All rights reserved.

## Use Case 1: Agility of Application Updates

Most enterprises are constantly refreshing their application environment. However, the actual time to add or update new entries in a Zscaler Private Access application segment can be cumbersome due to the many approval and change management processes that are sometimes required. The result is that multiple development and operations teams must work in parallel.

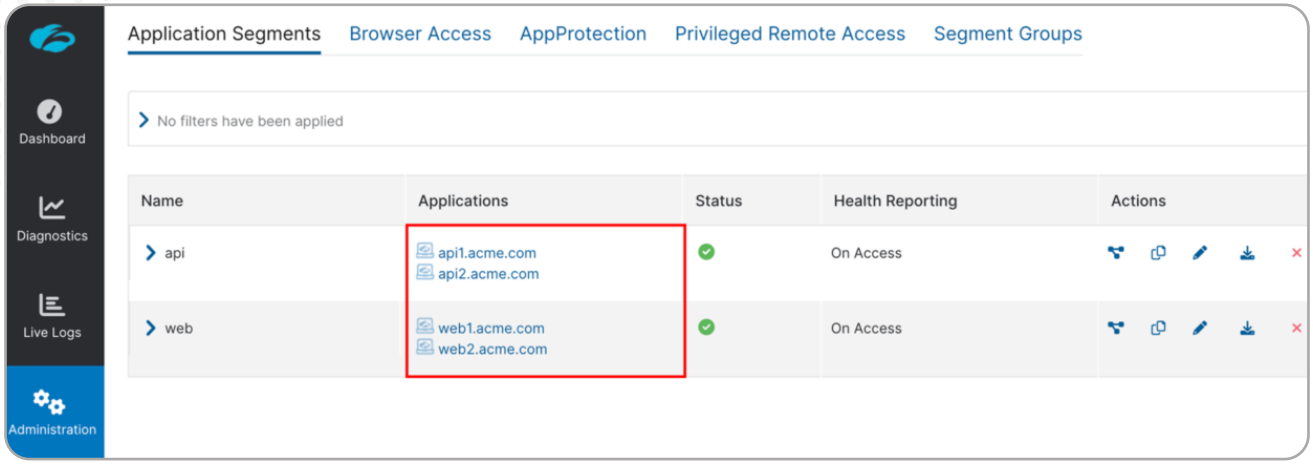
With ZPA and HashiCorp Consul–Terraform–Sync and Terraform, enterprises can update application segments in minutes with high confidence that the best experience is being delivered securely.

1. Application teams add, update, or delete new application segment FQDNs or IP address entries by avoiding multiple manual tickets.
2. Consul dynamically discovers the changes required by application teams as it is continuously monitoring the application environment.
3. Security teams can predefine access policies once and tailor the CTS configuration module provided by Zscaler to suit their needs.
4. Consul–Terraform–Sync reuses the module and auto–generates a new ZPA application segment or application server configuration as a Terraform resource.
5. Terraform configures the production–ready application segment in the ZPA platform by making those applications available to users in near real–time.
6. The platform team reviews and approves the automated configurations and workflows.



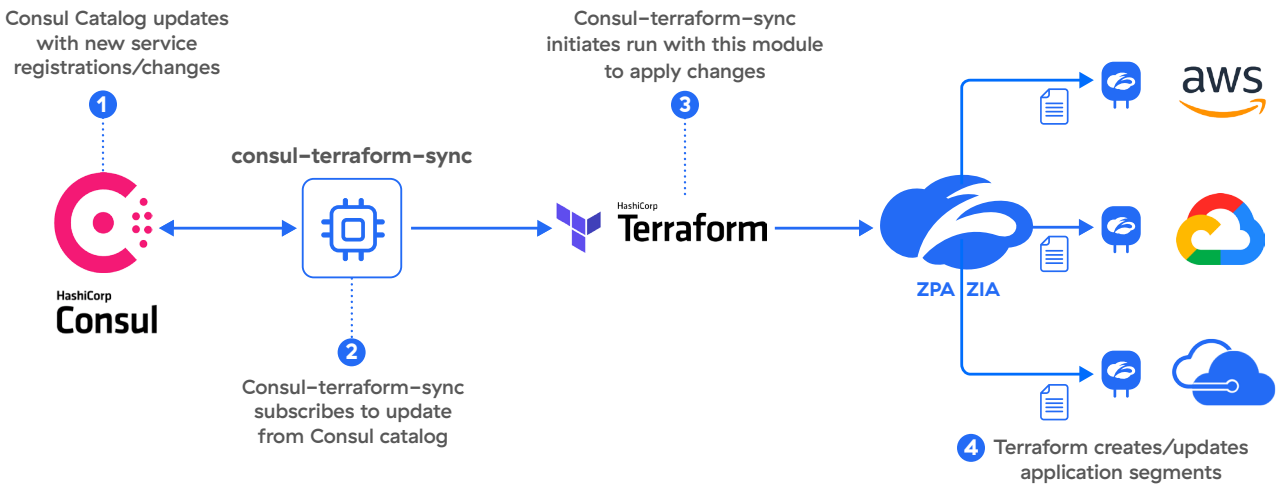

© 2023 Zscaler, Inc. All rights reserved.

## Terraform creates/updates application segments




Migrating a major enterprise application to hybrid cloud or multicloud can reduce capital expenditures, increase operating efficiency, improve user experience, and provide backup to improve up-time. But the project is error-prone because of the need to preserve and validate different security policies. Additionally, operating on multicloud requires IT teams to maintain consistency across different cloud providers, manually.

The CTS modules for ZPA and ZIA can facilitate the Day-N operations of a multicloud environment by reducing the time taken to make an application instance available across multiple cloud providers.




zscaler™ | Experience your world, secured.™

**About Zscaler**

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

©2023 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com