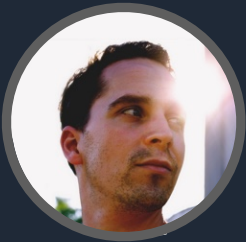




GitOps for MacAdmins Device Management with Terraform

Zentral Pro Services GmbH



Henry Stamerjohann



November 15, 2023



Why GitOps

Save time - automation efficiency, fewer errors

Reliability - stable, predictable operations

Auditability - authoritativeness in change management

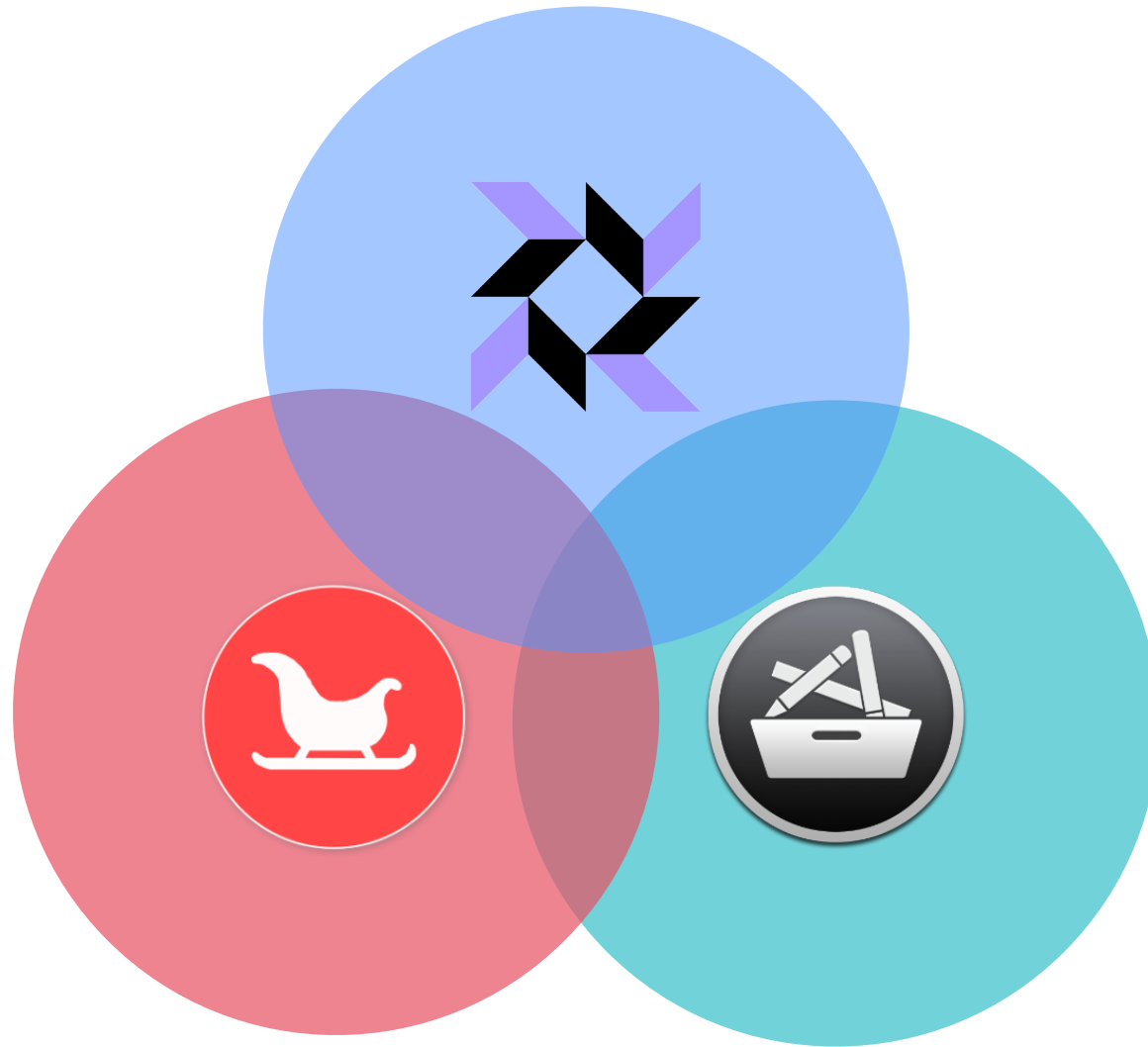


Principles

Git - store config & code in repositories

CI/CD - automation pipelines

Review - merge requests as an agent of change



Device Management with Terraform



Use Case: macOS device management

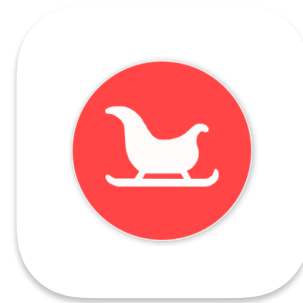
Utilize the best breed of open source tools



Declarative MDM



Osquery Server



Santa Sync Server

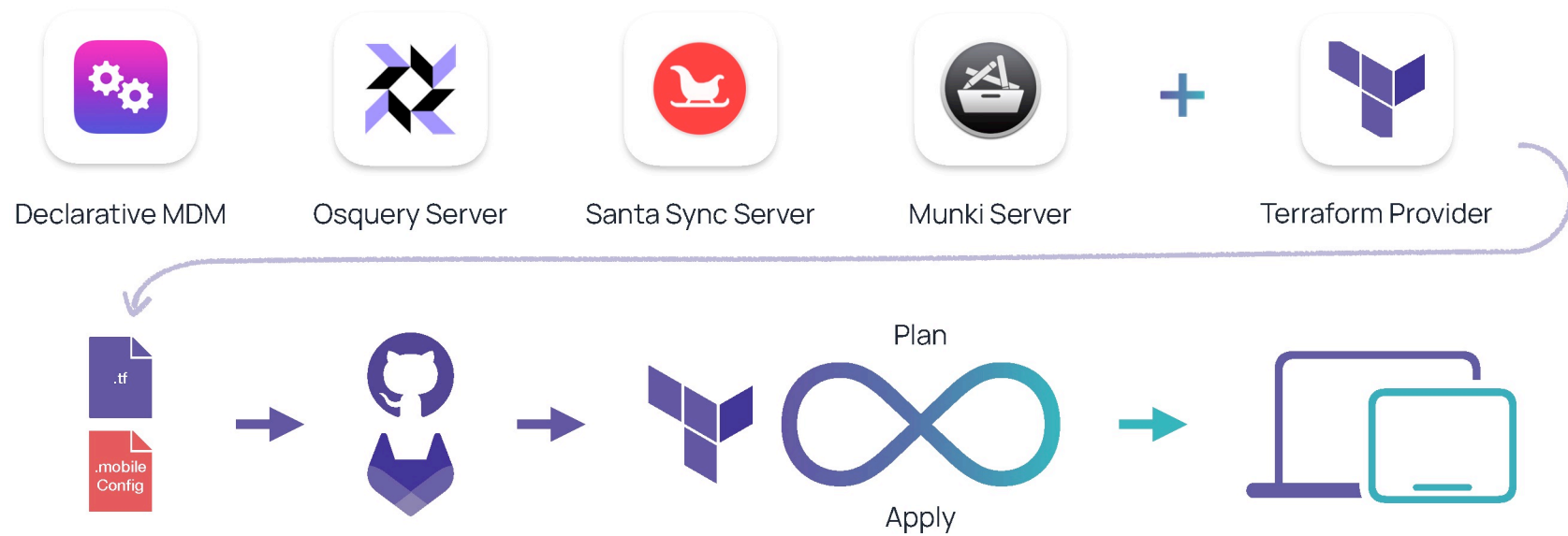


Munki Server

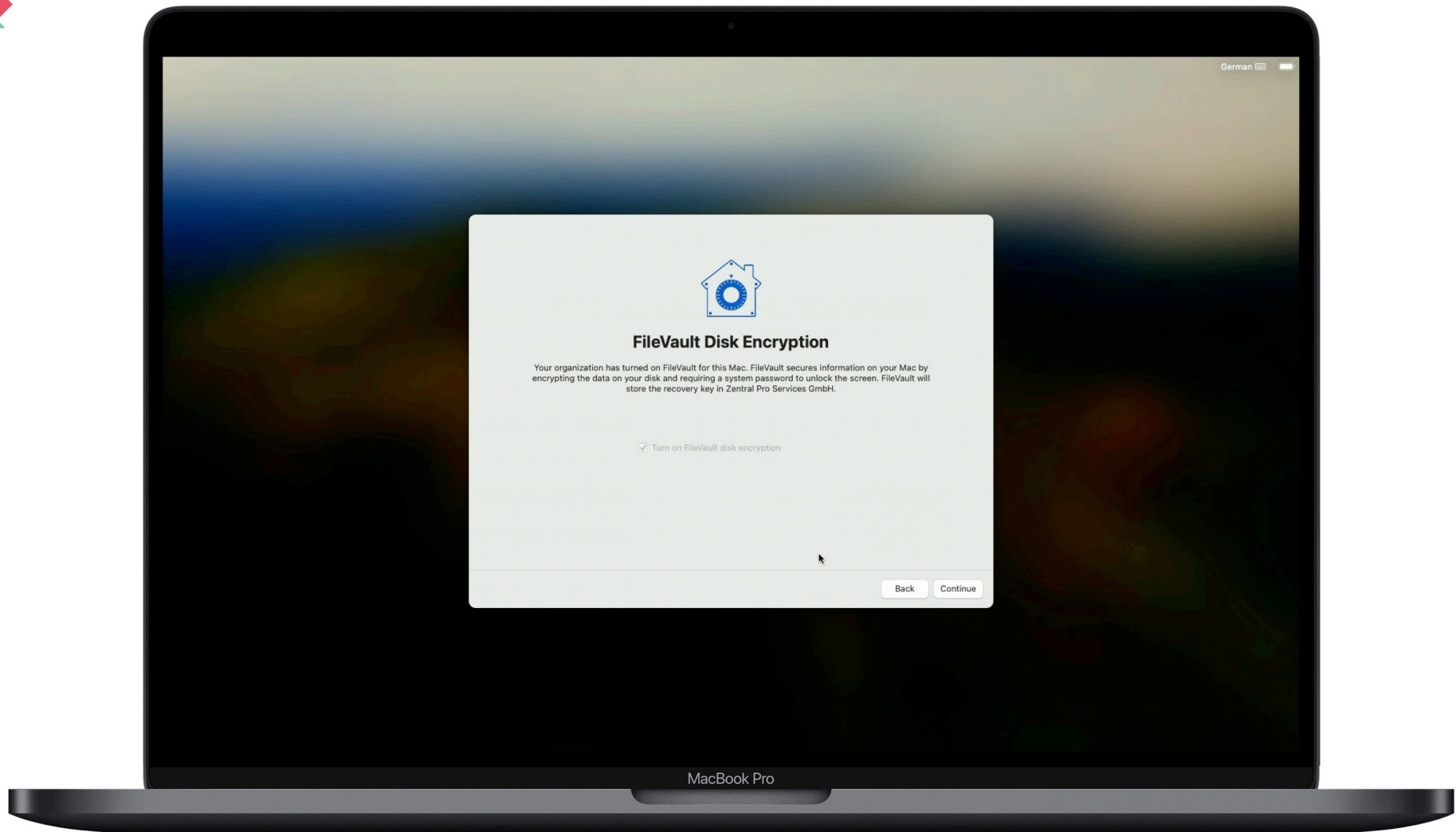


Our scope

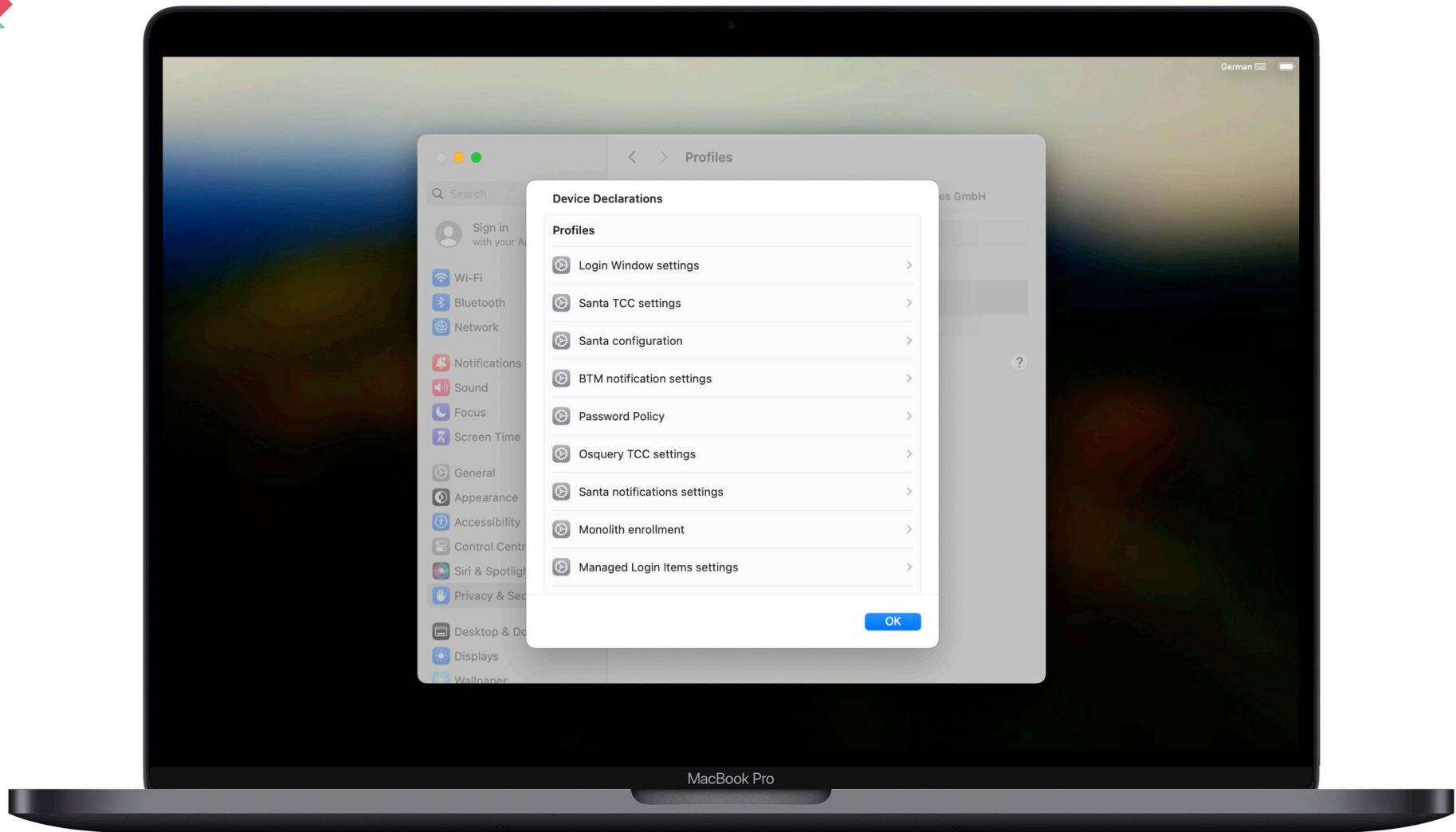
Comprehensive Device Management



Device Management with Terraform



Device Management with Terraform



Device Management with Terraform



Terraform configuration

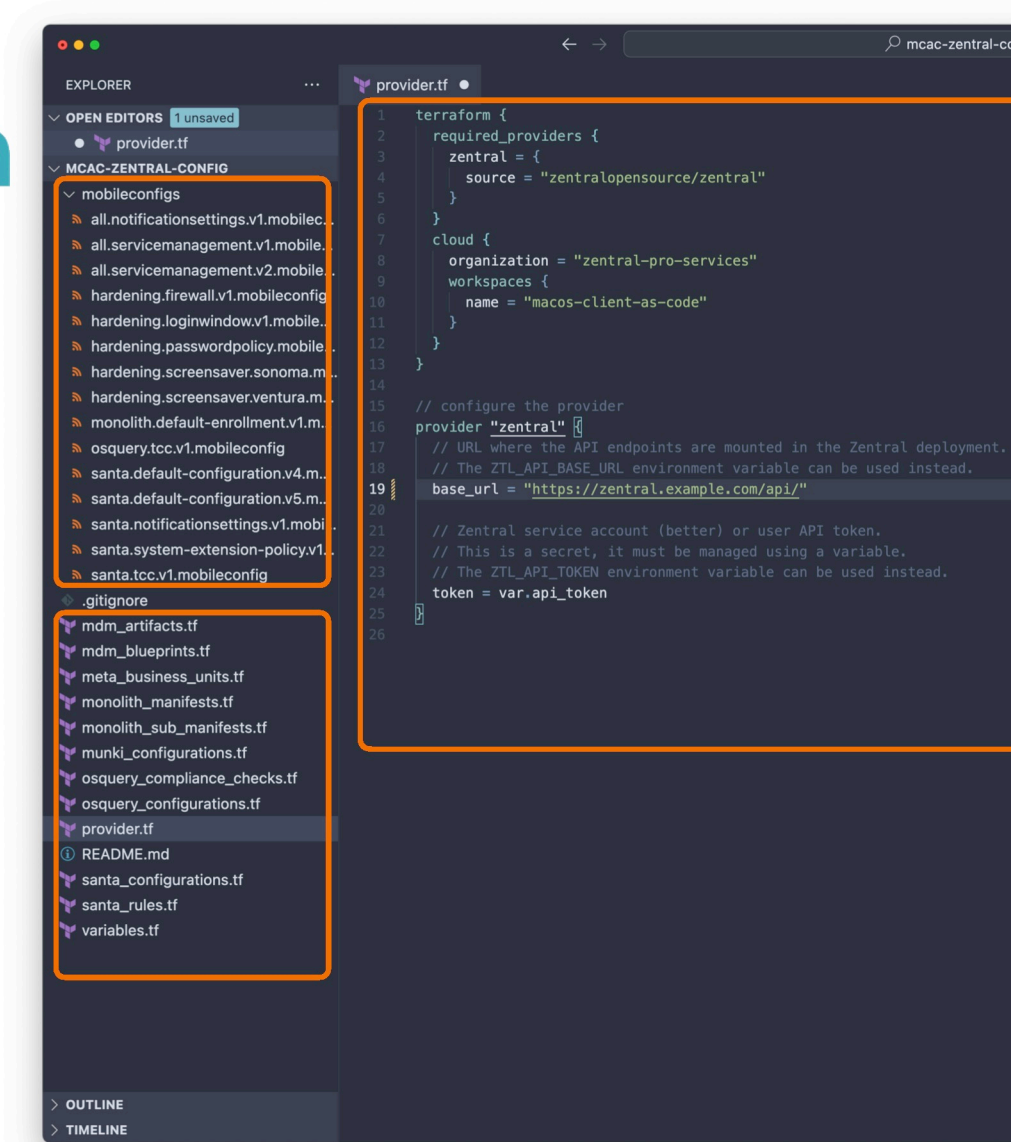
Overview

Official Zentral Terraform provider

Resources described as Terraform HCL files

Standard configuration profiles in separate sub folder

Device Management with Terraform



Terraform Provider

The screenshot shows the Terraform Registry interface for the Zentral Provider. The browser address bar displays `registry.terraform.io`. The navigation bar includes the Terraform logo, the word "Registry", and links for "Browse", "Publish", and "Sign-in". A prominent button encourages users to "Use Terraform Cloud for free". A search bar is positioned below the navigation bar.

The breadcrumb trail indicates the current page: `Providers / zentralopensource / zentral / Version 0.1.42 / Latest Version`. The main header for the provider includes the name "zentral" with a logo, and navigation options for "Overview", "Documentation", and a "USE PROVIDER" button.

The left sidebar, titled "ZENTRAL DOCUMENTATION", features a search filter and a list of resources. The resource `zentral_mdm_profile` is selected and highlighted. Other visible resources include `app`, `zentral_mdm_filevault_config`, `zentral_mdm_recovery_password_config`, `zentral_meta_business_unit`, `zentral_monolith_catalog`, and `zentral_monolith_condition`.

The main content area is titled "Zentral Provider" and contains the following text: "The Terraform Zentral provider is a plugin for Terraform that allows for the management of Zentral resources." Below this, an "Example Usage" section displays a Terraform configuration snippet:

```
terraform {
  required_providers {
    zentral = {
      source = "zentralopensource/zentral"
    }
  }
}
```

On the right side of the page, an "ON THIS PAGE" section lists "Example Usage" and "Schema". A "Report an issue" link is also present.

The browser's address bar at the bottom shows the full URL: `https://registry.terraform.io/providers/zentralopensource/zentral/latest/docs/resources/mdm_profile`.



mSCP Demo

Integrating Munki Compliance Checks

1. Transform baseline.yaml into a Terraform .tf File
2. Run Terraform apply in CI/CD Pipeline
3. Employ mSCP Compliance Checks with Zentral

Device Management with Terraform





mSCP Demo

Integrating Munki Compliance Checks

1. Transform baseline.yaml into a Terraform .tf File
2. Run Terraform apply in CI/CD Pipeline
3. Employ mSCP Compliance Checks with Zentral

```
python ./tools/mSCP/build_tf_script_checks.py \  
  --min-os-version 14 \  
  --max-os-version 15 \  
  --custom-dir ./src/mSCP/custom \  
  --default-odv-source recommended \  
  ./src/mSCP/mscp-cis-v1-custom.yaml \  
  PATH_TO/usnistgov/macos_security/ \  
  munki_mscp_script_checks.tf
```

MacBook Pro

Finder File Edit View Go Window Help

Python build_tf_script_checks.py

```
180
181 def main():
182     parser = argparse.ArgumentParser(
183         prog='build_tf_script_checks.py',
184         description='Takes a mSCP guideline YAML file '
185             'and build the Terraform Munki script checks resources.',
186     )
187     parser.add_argument("guidance_file")
188     parser.add_argument("repository")
189     parser.add_argument("ouput_file")
190     parser.add_argument("--min-os-version", default="")
191     parser.add_argument("--max-os-version", default="")
192     parser.add_argument("--default-odv-source", default="recommended")
193     args = parser.parse_args()
194     generate_terraform_resources(
195         args.guidance_file,
```

Filter | All Output | [trash] | [dropdown]

Run Succeeded | Time 175 ms | Peak Memory 15.4M | Symbol | Spaces: 2 | Line 4, Column 1

mSCP

Name	Date Modified	Size	Kind
mcaac-mscp-cis-v1-custom.yaml	Today, 19:20	3 KB	YAML

app.terraform.io

Apply finished 2 hours ago Resources: 64 added, 0 changed, 0 destroyed

Started 2 hours ago > Finished 2 hours ago

+ 64 created

Filter resources by address... Filter by action Terraform 1.5.7 Download raw log

> +	zentral_munki_script_check.mcs-authentication-auth_sma...	✓ Created	name=[mscp] - authentication - allow ...
> +	zentral_munki_script_check.mcs-icloud-icloud_sync_disable	✓ Created	name=[mscp] - icloud - disable icloud...
> +	zentral_munki_script_check.mcs-macos-os_anti_virus_ins...	✓ Created	name=[mscp] - macos - must use an app...
> +	zentral_munki_script_check.mcs-macos-os_authenticated...	✓ Created	name=[mscp] - macos - enable authenti...
> +	zentral_munki_script_check.mcs-macos-os_config_data_i...	✓ Created	name=[mscp] - macos - enforce install...
> +	zentral_munki_script_check.mcs-macos-os_firewall_log_e...	✓ Created	name=[mscp] - macos - enable firewall...
> +	zentral_munki_script_check.mcs-macos-os_gatekeeper_re...	✓ Created	name=[mscp] - macos - enforce gatekee...
> +	zentral_munki_script_check.mcs-macos-os_guest_folder_r...	✓ Created	name=[mscp] - macos - remove guest fo...
> +	zentral_munki_script_check.mcs-macos-os_home_folders...	✓ Created	name=[mscp] - macos - secure user's h...
> +	zentral_munki_script_check.mcs-macos-os_httpd_disable	✓ Created	name=[mscp] - macos - disable the bui...
> +	zentral_munki_script_check.mcs-macos-os_library_validati...	✓ Created	name=[mscp] - macos - enable library ...
> +	zentral_munki_script_check.mcs-macos-os_mdm_require	✓ Created	name=[mscp] - macos - enforce enrollm...
> +	zentral_munki_script_check.mcs-macos-os_mobile_file_int...	✓ Created	name=[mscp] - macos - enable apple mo...
> +	zentral_munki_script_check.mcs-macos-os_nfsd_disable	✓ Created	name=[mscp] - macos - disable network...
> +	zentral_munki_script_check.mcs-macos-os_on_device_dic...	✓ Created	name=[mscp] - macos - enforce on devi...
> +	zentral_munki_script_check.mcs-macos-os_password_hint...	✓ Created	name=[mscp] - macos - remove password...
> +	zentral_munki_script_check.mcs-macos-os_rapid_security...	✓ Created	name=[mscp] - macos - enforce rapid s...
> +	zentral_munki_script_check.mcs-macos-os_recovery_lock...	✓ Created	name=[mscp] - macos - enable recovery...
> +	zentral_munki_script_check.mcs-macos-os_root_disable	✓ Created	name=[mscp] - macos - disable root lo...

zentral-pro-services



GitOps with CI/CD

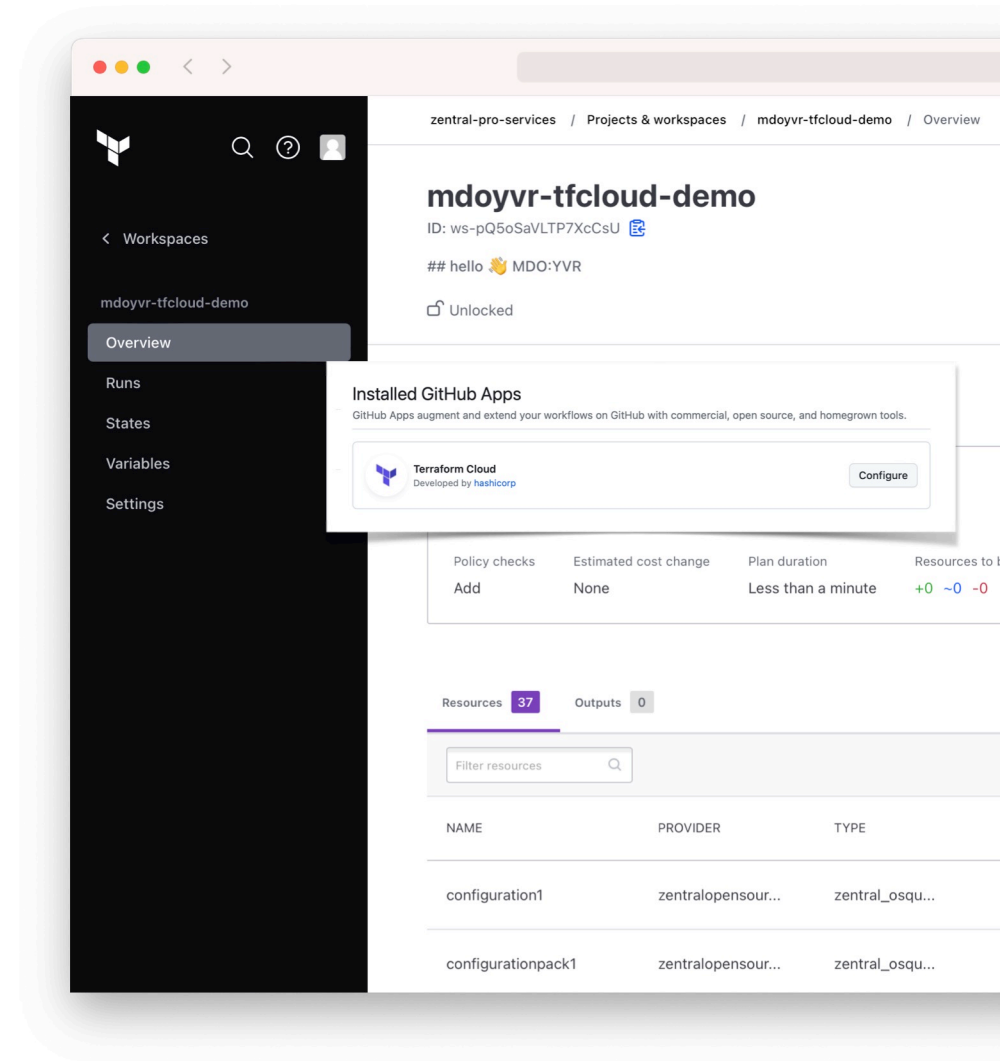
Utilize a Build Pipeline in Terraform Cloud

Add New Resources for Osquery

Automate Configuration Changes with Git Commits

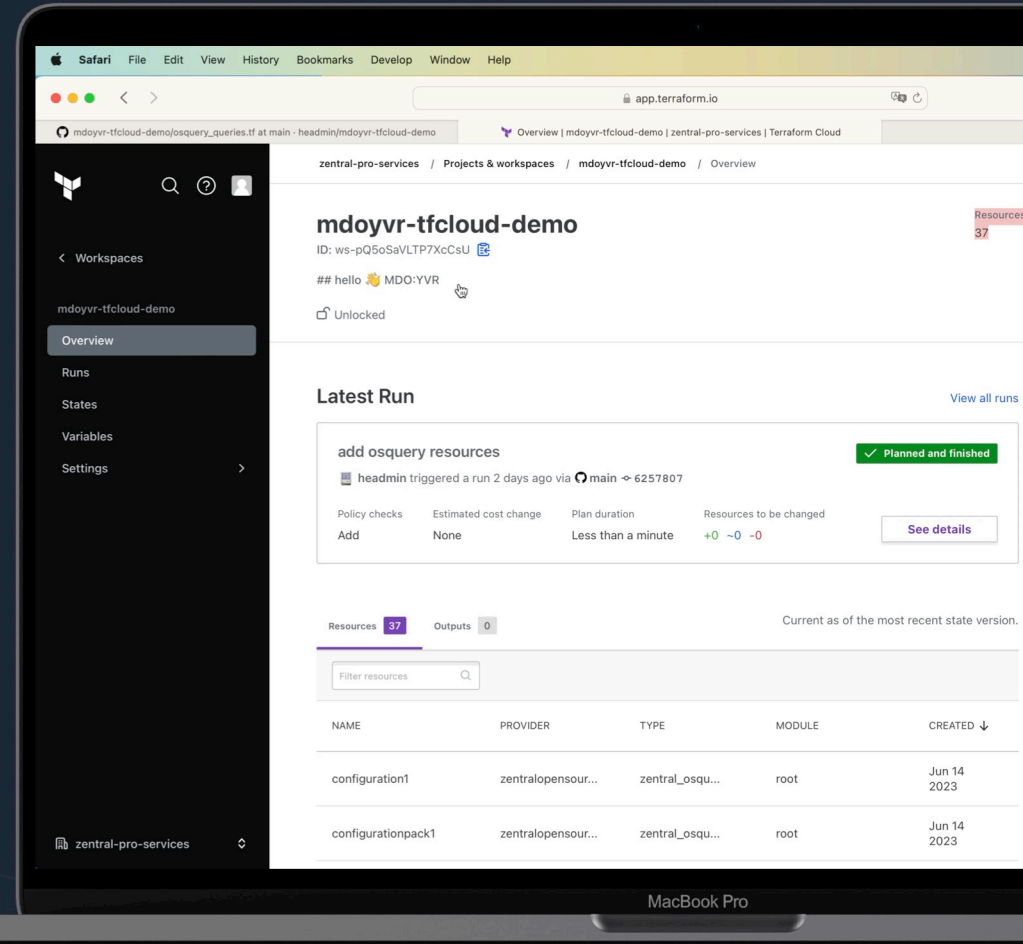
Observe Applied Changes in Zentral

Device Management with Terraform





Terraform Cloud Gitops



Device Management with Terraform

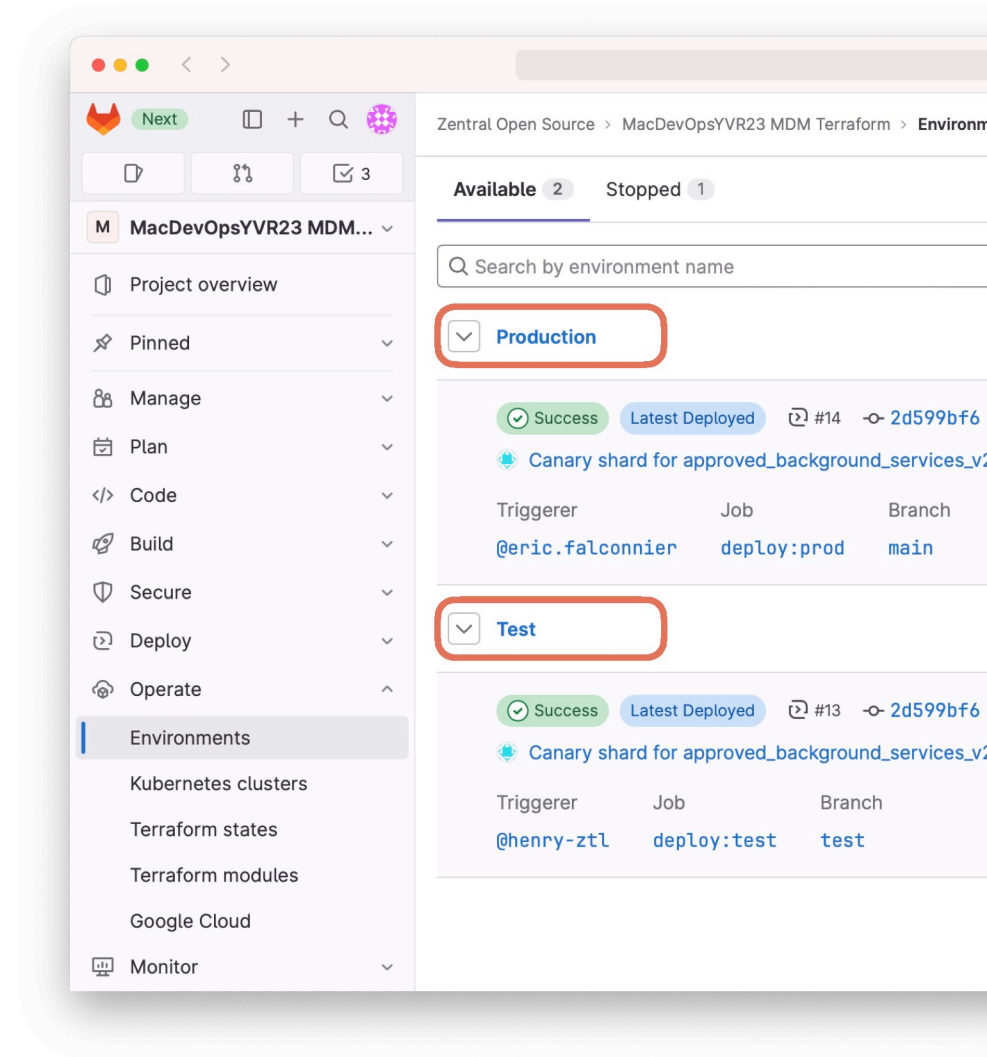


Dual Pipeline Strategy

GitLab-Based Pipelines (2 protected branches)

Utilizing 2 Zentral Environments (Production & Test)

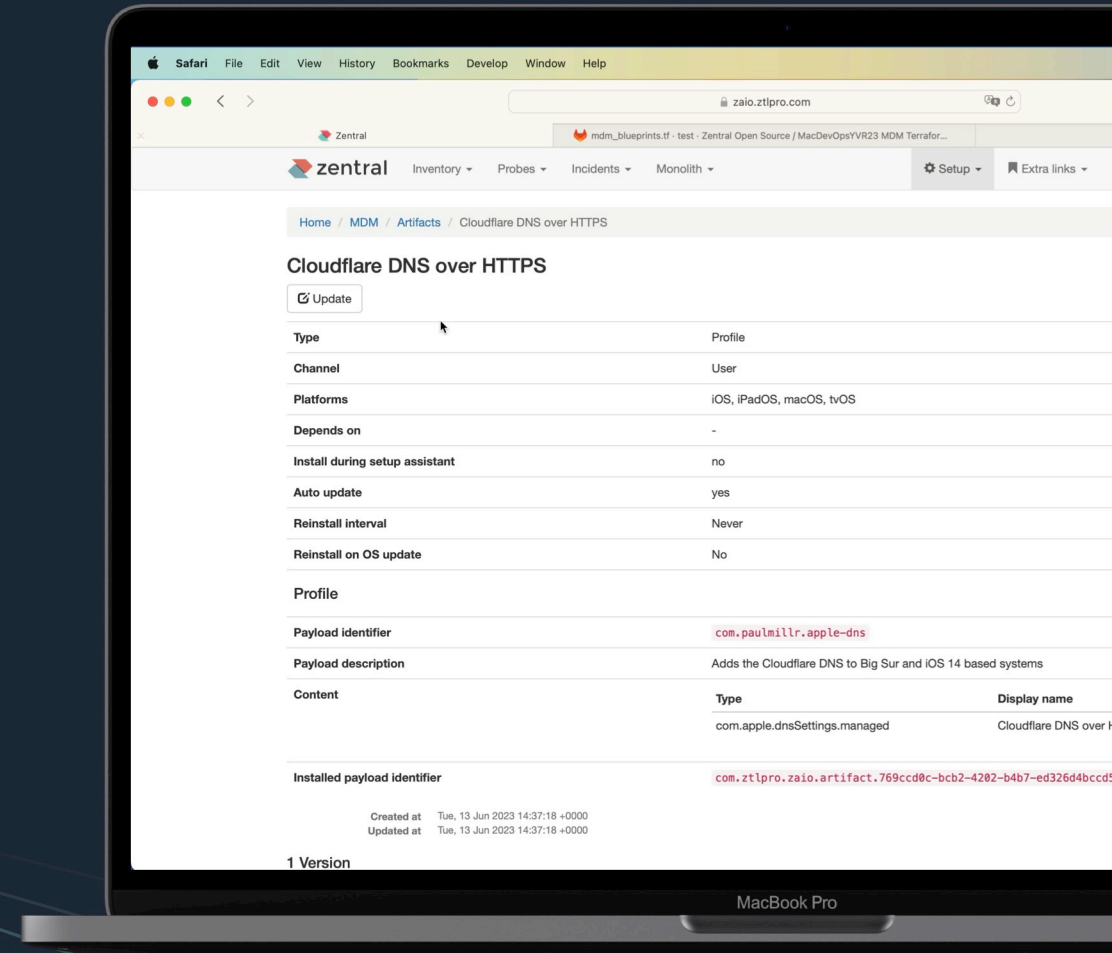
Approval Process Setup (dual control)





Gitlab pipeline test/prod

with protected branch & approval merge request



Device Management with Terraform



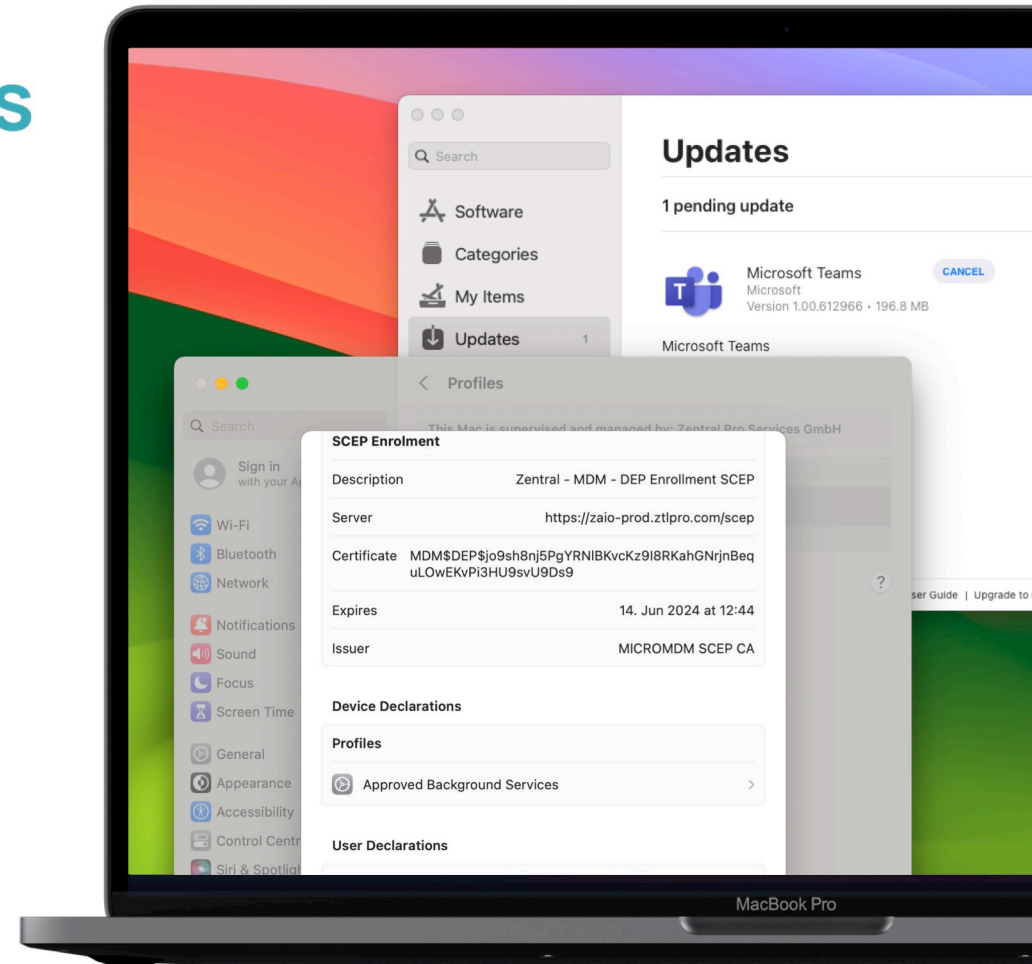
Unlock the Rewards of GitOps

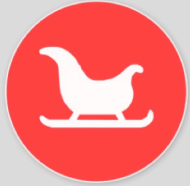
Are toggle switches a thing of the past?

Leaving GUI behind is no walk in the park!

Safety nets are hard work

But we get plenty of rewards





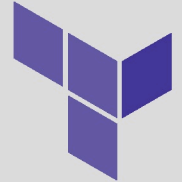
Manage Security Agents



Install Software



MDM with Declarative device management



Automation



Admin GUI



Zentral

www.zentral.com



Git + CI/CD



Data History



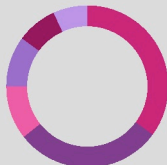
IdP / SCIM



Metrics



Audit Changes



Reports



Approval Process



SW Update



Hardening



Identity



App Provisioning



Open codebase

<https://github.com/zentralopensource/zentral>

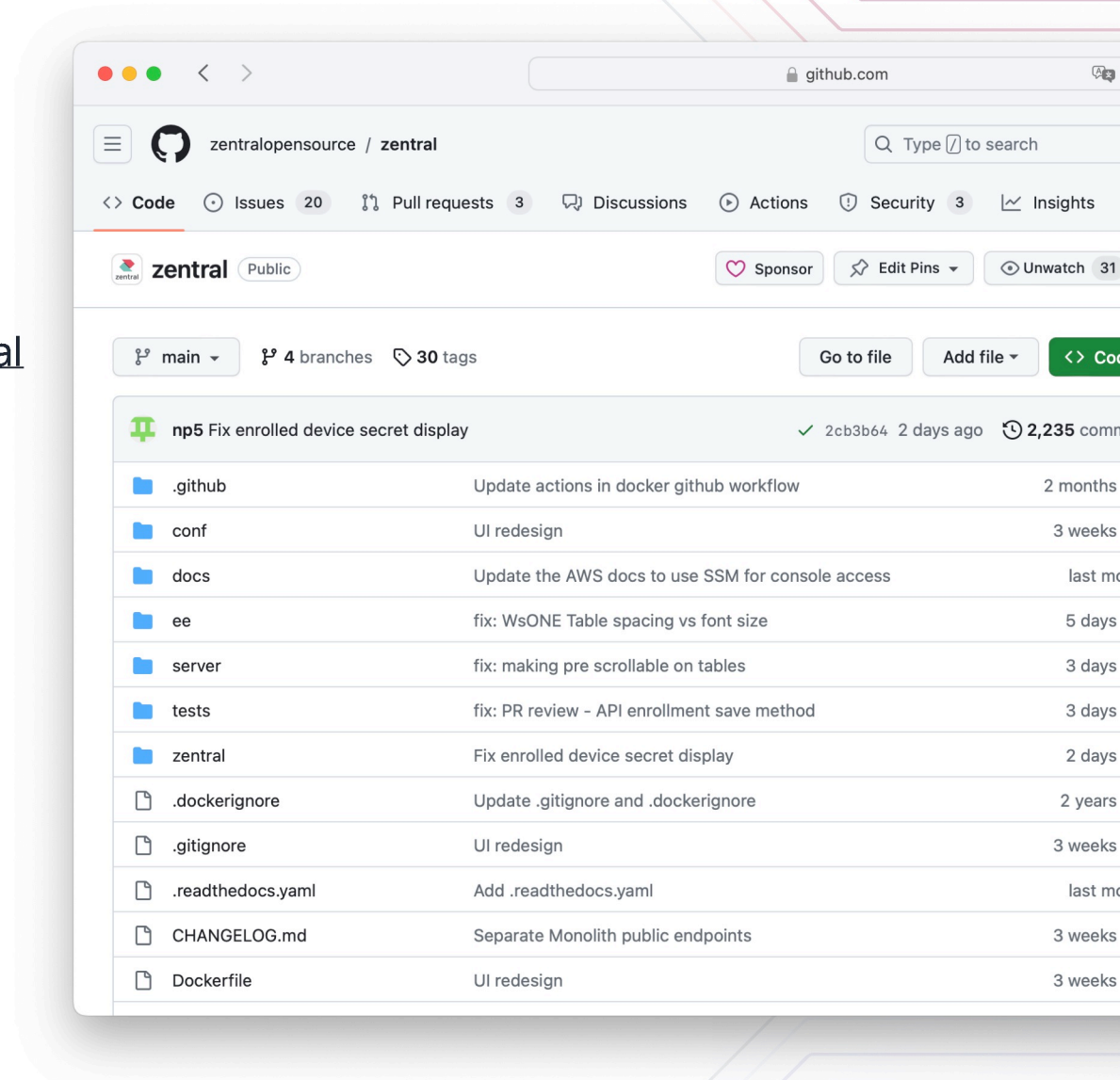
<https://docs.zentral.io>

<https://registry.terraform.io>



★ Starred 702

Device Management with Terraform





Open codebase

<https://github.com/zentralopensource/zentral>

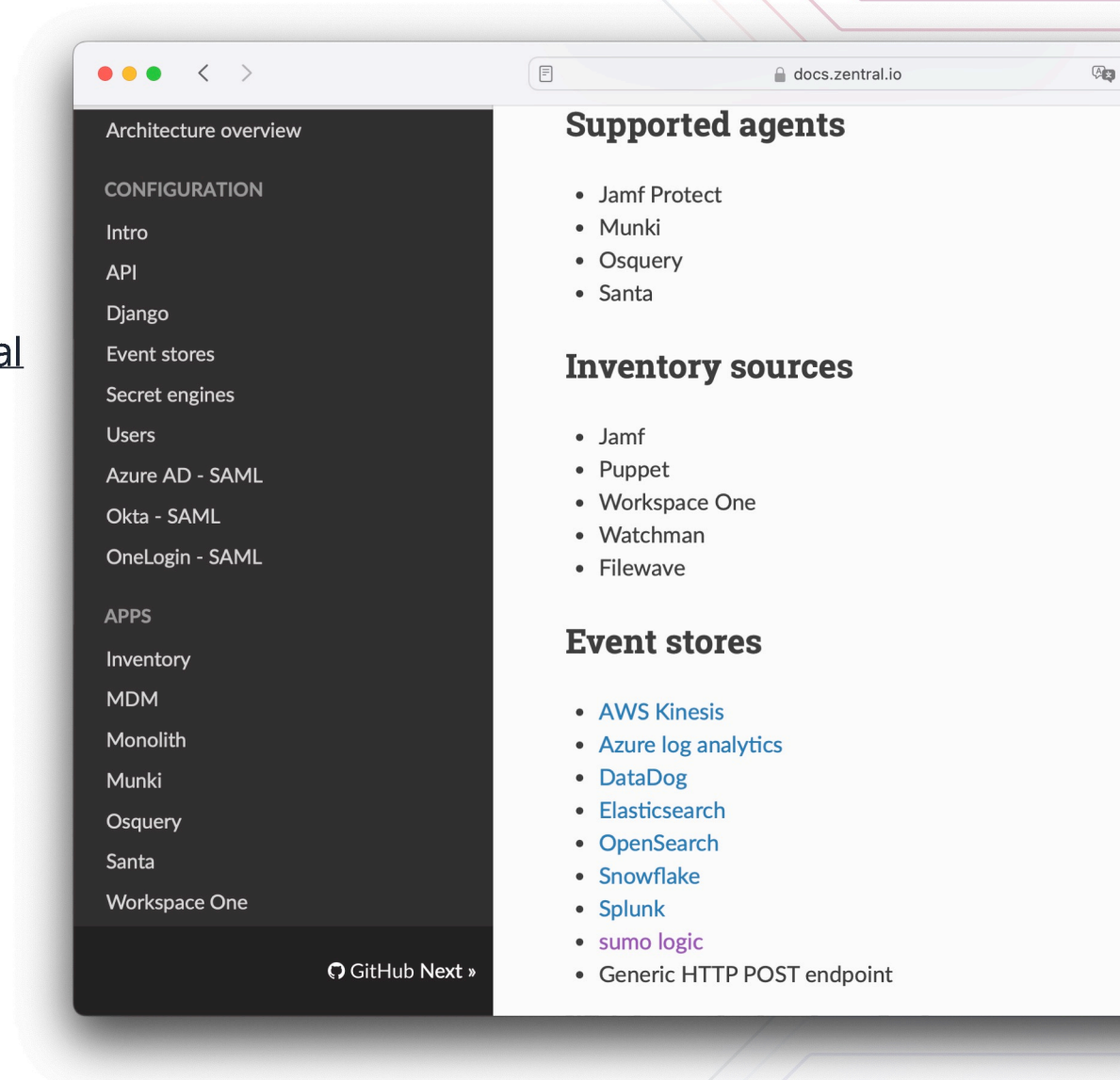
<https://docs.zentral.io>

<https://registry.terraform.io>



★ Starred 702

Device Management with Terraform





Vendor Support with SLA

Leverage Best-In-Class Open Source Agents

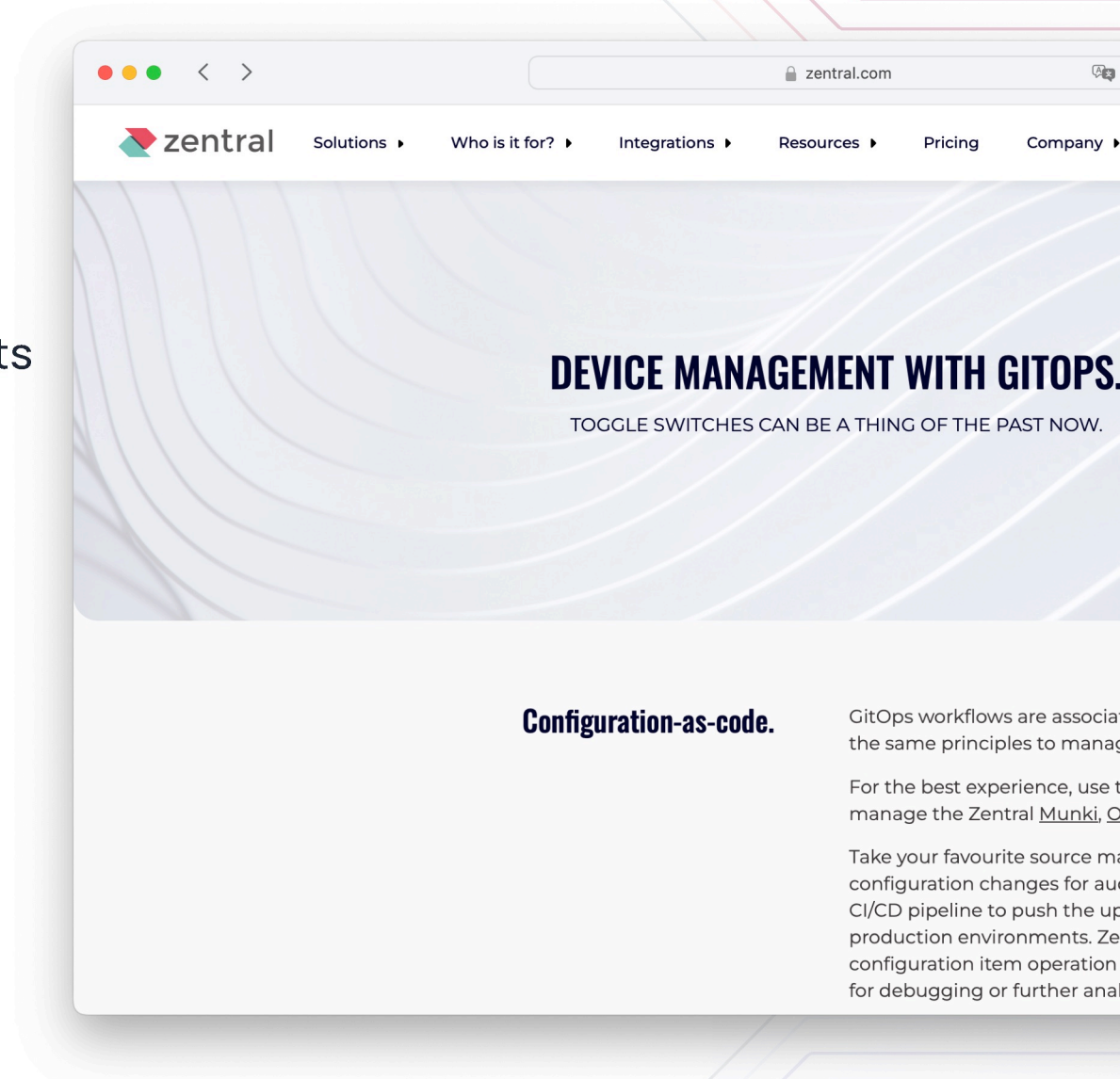
Terraform-Powered Device Management

Pioneering GitOps Declarative MDM

www.zentral.com

[#zentral](#) - Macadmins Slack

Device Management with Terraform





Vendor Support with SLA

Leverage Best-In-Class Open Source Agents

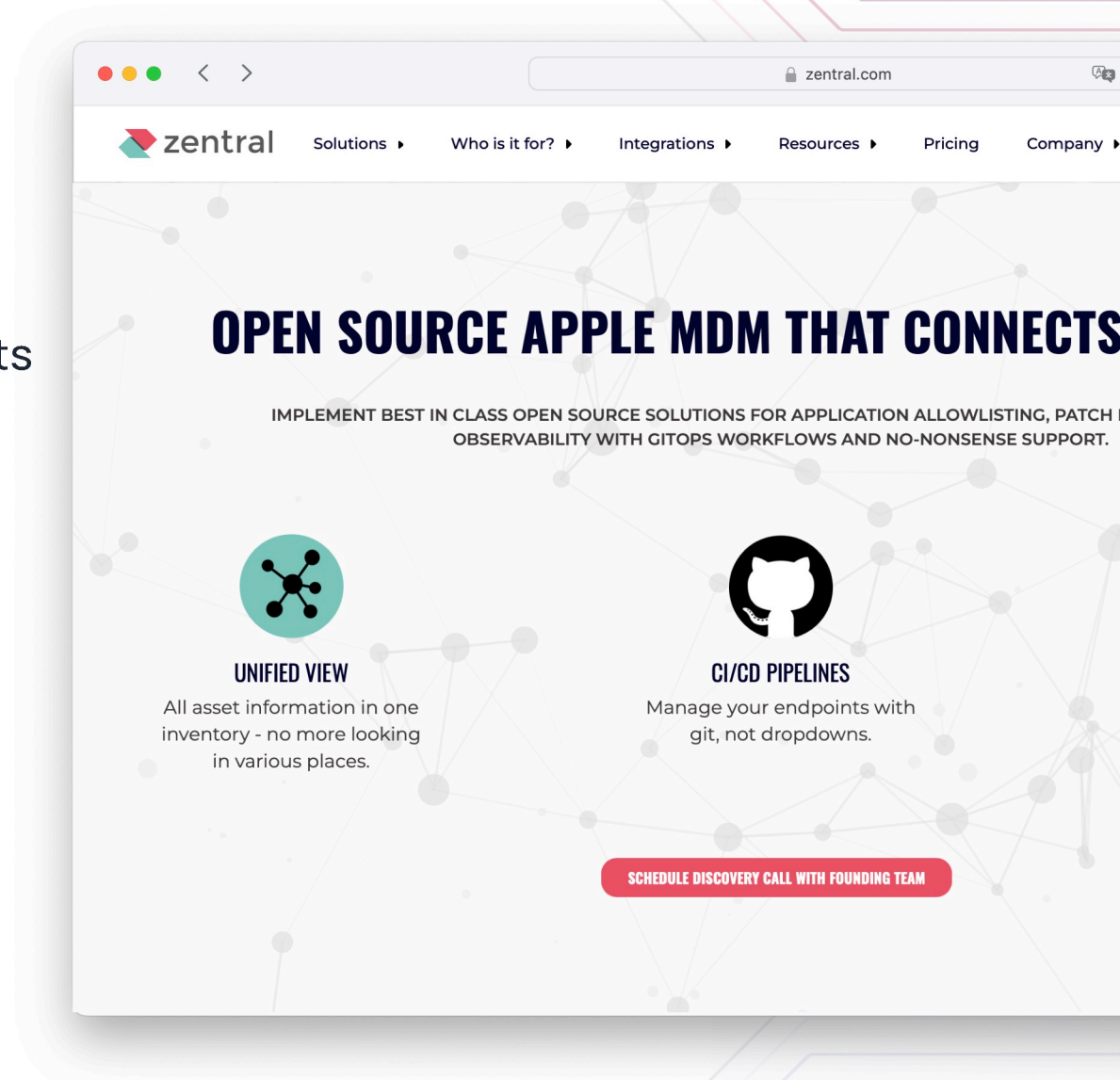
Terraform-Powered Device Management

Pioneering GitOps Declarative MDM

www.zentral.com

[#zentral](#) - Macadmins Slack

Device Management with Terraform





Thank you!

www.zentral.com