

GitOps for MacAdmins Device Management with Terraform

Zentral Pro Services GmbH



Henry Stamerjohann



November 15, 2023



Save time - automation efficiency, fewer errors

Reliability - stable, predictable operations

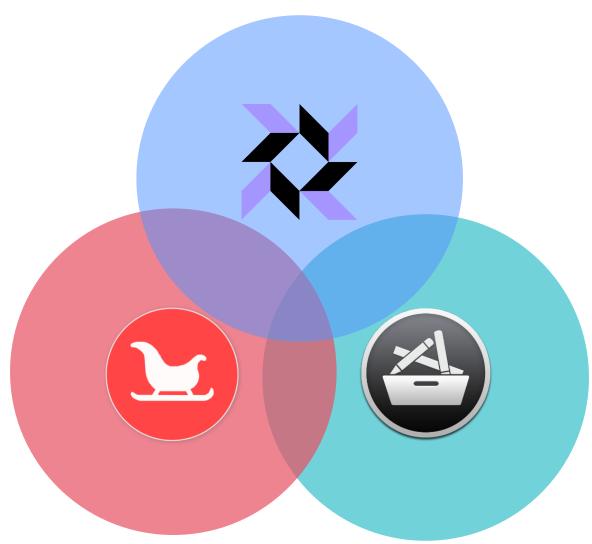
Auditability - authoritativeness in change management



Git - store config & code in repositories

CI/CD - automation pipelines

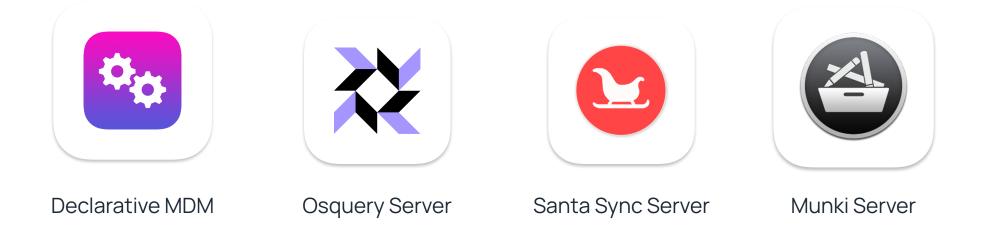
Review - merge requests as an agent of change





Use Case: macOS device management

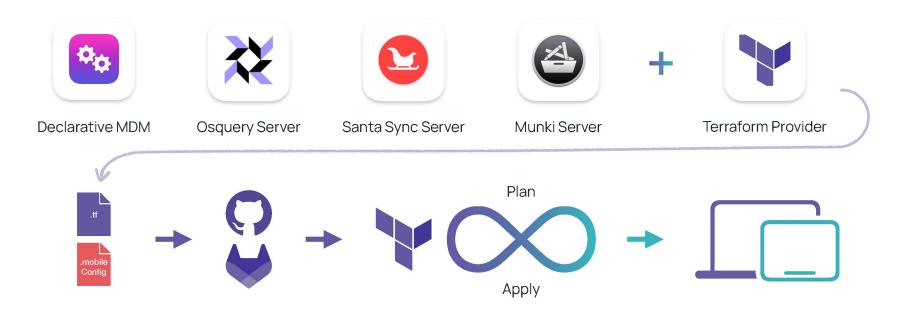
Utilize the best breed of open source tools



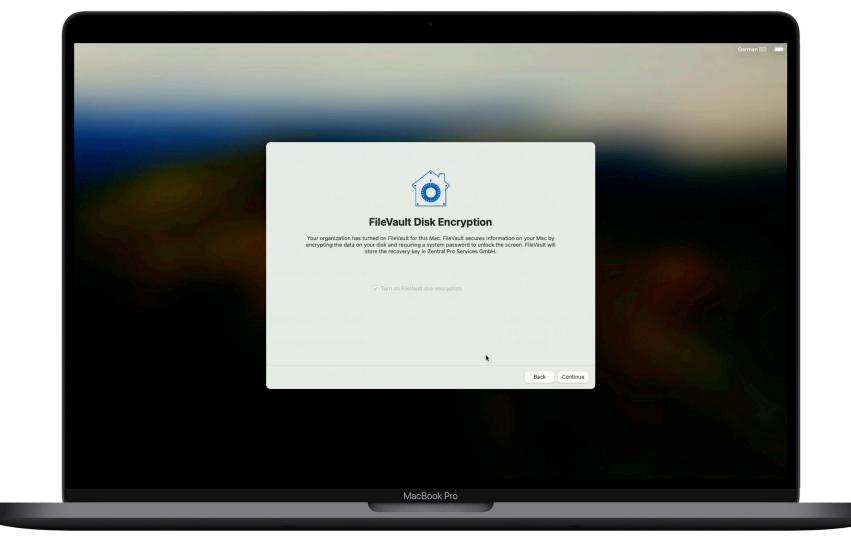


Our scope

Comprehensive Device Management







.



•••	< > Profiles			
Q Search	Device Declarations	es Gmbl	H	and the second
Sign in with your Ar	Profiles			
🛜 Wi-Fi	Login Window settings	>		
8 Bluetooth	Santa TCC settings	>		
🛞 Network	Santa configuration	>		
Notifications	BTM notification settings	>	?	
Focus	Password Policy	>		
Screen Time	Osquery TCC settings	>		Part and the
General	Santa notifications settings	>		
AppearanceAccessibility	Monolith enrollment	>		
😑 Control Centr				
Siri & Spotligh	Managed Login Items settings	>		
		ОК		
😑 Desktop & Do				
88 Wallpaper				

Device Management with Terraform

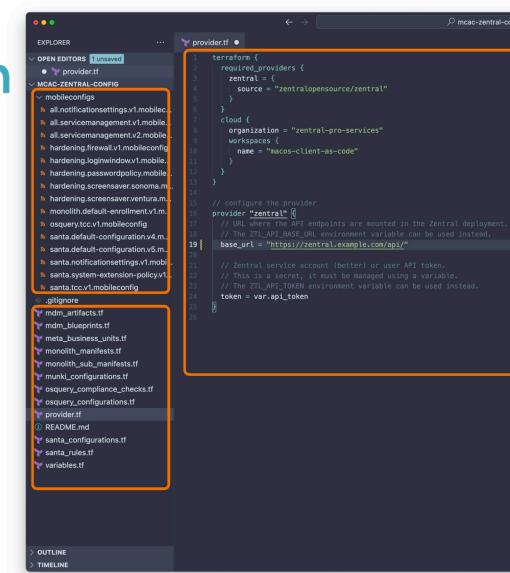
Terraform configuration

Overview

Official Zentral Terraform provider

Resources described as Terraform HCL files

Standard configuration profiles in separate sub folder



Terraform Provider

• < >	🗏 🔒 registry.terraform.io	
Terraform Registry	Browse 🗸 Publish 🗸 Sign-in 🏹 🛛 Use Te	erraform Cloud for free 🤊
Q Search	all resources	
oviders / zentralopensource / zentral	Version 0.1.42 v Latest Version	
zentral 🕿	Overview Documenta	tion 🔮 USE PROVIDER 👻
ZENTRAL DOCUMENTATION	Zentral Provider	ON THIS PAGE Example Usage
Q Filter	The Terraform Zentral provider is a plugin for Terraform that	Schema
app zentral_mdm_filevault_ config	allows for the management of Zentral resources.	
zentral_mdm_profile Example Usage		
zentral_mdm_recovery_ passwotcd_config		
zentral_meta_business_ unit zentral_monolith_catalog	<pre>terraform { required_providers { zentral = { source = "zentralopensource/zentral"</pre>	
zentral_monolith_condition	1	

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



mSCP Demo

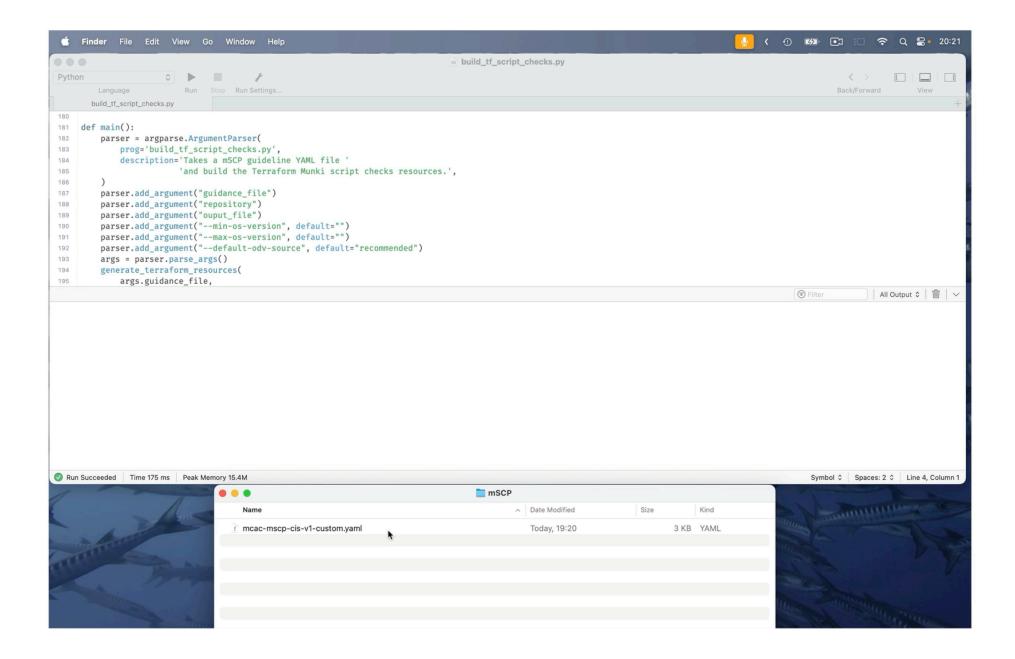
Integrating Munki Compliance Checks

- 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



••• < >	🔒 app.terraform.io	۵ +
	Apply finished 2 hours ago Resources: 64 added, 0 changed, 0 destroyed	
< Workspaces	Started 2 hours ago > Finished 2 hours ago	
mcac-zentral-config	+ 64 created	
Overview	Filter resources by address 🔽 Filter by action 🗸 Terraform 1.5.7 🖸 Download raw log	
Runs	> + V zentral_munki_script_check.mcs-authentication-auth_sma Created name=[mscp] - authentication - allow	
States	> + Y zentral_munki_script_check.mcs-icloud-icloud_sync_disable Created name=[mscp] - icloud - disable icloud	
Variables	> + V zentral_munki_script_check.mcs-macos-os_anti_virus_ins Created name=[mscp] - macos - must use an app	
Settings >	> + W 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	
	> + V zentral_munki_script_check.mcs-macos-os_firewall_log_e	
	> + 💱 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	
開 zentral-pro-services ≎	> + 🦞 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	

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

••• < >				
		s / Projects & workspaces	/ mdoyvr-tfcloud-demo	/ Overview
V Q 🧿 🕻	MCOVIC- ID: ws-pQ5oSaVLT	tfcloud-dem	10	
mdoyvr-tfcloud-demo Overview	## hello 👋 MDO:	YVR		
Runs	Installed GitHub Apps			
States	GitHub Apps augment and extend your w	orkflows on GitHub with commercial,	open source, and homegrown too	bls.
Variables	Terraform Cloud		Config	ure
Settings	Developed by hashicorp			
	Policy checks Add	Estimated cost change None	Plan duration Less than a minute	Resources to +0 ~0 -0
	Resources 37	Outputs 0		
	Filter resources	Q		
	NAME	PROVIDER	TYPE	
	configuration1	zentraloper	nsour zentral_o	osqu
	configurationpa	ick1 zentralopei	nsour zentral_o	osqu



Terraform Cloud Gitops

Safari File Edit View History Boo	okmarks Develop Window	Help			
••• < >			app.terraform.io		ଓ କ୍ଷ
mdoyvr-tfcloud-demo/osquery_queries.tf at main · hea	dmin/mdoyvr-tfcloud-demo	Y Overview mdoyvr-tfclo	oud-demo zentral-pro-service	s Terraform Cloud	
	zentral-pro-services / Projects	s & workspaces / mdoyvr-	tfcloud-demo / Overview		
Y Q 🕜 🔲	mdoyvr-tfclou	id-demo			Resourc 37
< workspaces	ID: ws-pQ5oSaVLTP7XcCsU	2			
	## hello 👋 MDO:YVR				
Overview					
Runs					
States	Latest Run				View all run
Variables	add osquery resource	es		× 1	Planned and finished
Settings >	📕 headmin triggered a ru	ın 2 days ago via O main	↔ 6257807	_	
	Policy checks Estimated Add None	cost change Plan durat Less thar	ion Resources n a minute +0 ~0 -0	to be changed	See details
	Resources 37 Outputs	0		Current as of the m	nost recent state version
	Filter resources Q				
	NAME	PROVIDER	TYPE	MODULE	CREATED \downarrow
	configuration1	zentralopensour	zentral_osqu	root	Jun 14 2023
∰ zentral-pro-services ≎	configurationpack1	zentralopensour	zentral_osqu	root	Jun 14 2023
			MacBook Pro		

Dual Pipeline Strategy

GitLab-Based Pipelines (2 protected branches)

Utilizing 2 Zentral Environments (Production & Test)

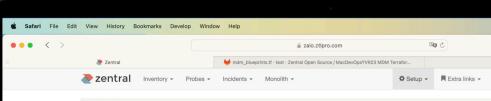
Approval Process Setup (dual control)

... Q 🚻 Next □ + Zentral Open Source > MacDevOpsYVR23 MDM Terraform > Environn \square ເງ 🗹 3 Available 2 Stopped 1 M MacDevOpsYVR23 MDM... v Q Search by environment name Project overview \vee Production 🖈 Pinned රිපි Manage € #14 -0- 2d599bf6 Latest Deployed Success 🗟 Plan Canary shard for approved_background_services_v </>> Code Triggerer Job Branch Q Build @eric.falconnier deploy:prod main Φ Secure ✓ Test Deploy Operate Success Latest Deployed **シ**#13 -0- 2d599bf6 Environments Canary shard for approved_background_services_v Kubernetes clusters Triggerer Job Branch Terraform states @henry-ztl deploy:test test Terraform modules Google Cloud 🛄 Monitor



Gitlab pipeline test/prod

with protected branch & approval merge request



Home / MDM / Artifacts / Cloudflare DNS over HTTPS

Cloudflare DNS over HTTPS

C Update				
Туре	P	Profile		
Channel	u	Jser		
Platforms	iC	iOS, iPadOS, macOS, tvOS		
Depends on	-			
Install during setup assistant	n	10		
Auto update	у	res		
Reinstall interval Never				
Reinstall on OS update No				
Profile				
Payload identifier		com.paulmillr.apple-dns		
Payload description	A	adds the Cloudflare DNS to Big Sur and iOS 14 base	d systems	
Content		Туре	Display name	
		com.apple.dnsSettings.managed	Cloudflare DNS over	

Installed payload identifier

Created at Tue, 13 Jun 2023 14:37:18 +0000

com.ztlpro.zaio.artifact.769ccd0c-bcb2-4202-b4b7-ed326d4bccd

MacBook Pro

Updated at Tue, 13 Jun 2023 14:37:18 +0000

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



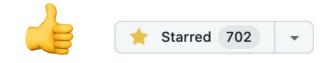


Open codebase

https://github.com/zentralopensource/zentral

https://docs.zentral.io

https://registry.terraform.io



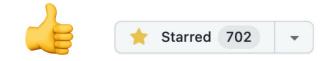
•••		☐ github.com	(Ala
= 💭 zentralopensource / zentral		Q Type [] to s	search
<> Code	uests 3 🖓 Discussions 🕑 A	Actions ① Security 3	🗠 Insights
Zentral (Public)	\bigcirc :	Sponsor 🔗 Edit Pins 👻	ⓒ Unwatch 31
양 main ▾ 양 4 branches ▷ 30 t	ags	Go to file Add fi	le - <> Co
np5 Fix enrolled device secret displ	ау	✓ 2cb3b64 2 days ago	🕑 2,235 comr
.github	Update actions in docker github wor	kflow	2 months
Conf	UI redesign		3 weeks
docs	Update the AWS docs to use SSM fo	or console access	last m
ee	fix: WsONE Table spacing vs font siz	e	5 days
server	fix: making pre scrollable on tables		3 days
tests	fix: PR review - API enrollment save	method	3 days
z entral	Fix enrolled device secret display		2 days
🗋 .dockerignore	Update .gitignore and .dockerignore		2 years
🗋 .gitignore	UI redesign		3 weeks
.readthedocs.yaml	Add .readthedocs.yaml		last m
CHANGELOG.md	Separate Monolith public endpoints		3 weeks
Dockerfile	UI redesign		3 weeks

Open codebase

https://github.com/zentralopensource/zentral

https://docs.zentral.io

https://registry.terraform.io



Device Management with Terraform

Architecture overview	Supported agents
CONFIGURATION Intro	Jamf ProtectMunki
API Django	OsquerySanta
Event stores Secret engines	Inventory sources
Users Azure AD - SAML Okta - SAML OneLogin - SAML	JamfPuppetWorkspace OneWatchman
APPS Inventory	• Filewave Event stores
MDM Monolith Munki Osquery Santa	 AWS Kinesis Azure log analytics DataDog Elasticsearch OpenSearch Snowflake
Workspace One GitHub Next :	 Splunk sumo logic Generic HTTP POST endpoint

F

adocs.zentral.io

A

••• < >

Vendor Support with SLA

Leverage Best-In-Class Open Source Agents

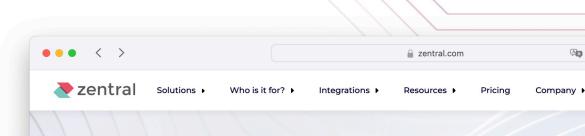
Terraform-Powered Device Management

Pioneering GitOps Declarative MDM

www.zentral.com

#zentral - Macadmins Slack

Device Management with Terraform



DEVICE MANAGEMENT WITH GITOPS.

TOGGLE SWITCHES CAN BE A THING OF THE PAST NOW.

Configuration-as-code.

GitOps workflows are associa the same principles to manag

For the best experience, use t manage the Zentral <u>Munki</u>, <u>O</u>

Take your favourite source ma configuration changes for au CI/CD pipeline to push the up production environments. Ze configuration item operation for debugging or further ana

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

OPEN SOURCE APPLE MDM THAT CONNECTS

Integrations >

IMPLEMENT BEST IN CLASS OPEN SOURCE SOLUTIONS FOR APPLICATION ALLOWLISTING, PATCH OBSERVABILITY WITH GITOPS WORKFLOWS AND NO-NONSENSE SUPPORT.



Solutions

Who is it for?

 $\bullet \bullet \bullet < >$

zentral

UNIFIED VIEW All asset information in one inventory - no more looking in various places.



zentral.com

Resources I

Pricing

Ax

Company

SCHEDULE DISCOVERY CALL WITH FOUNDING TEAM



Thank you!

www.zentral.com