



Cloud Native Posture Management for All

Introducing cnquery & cnspec

Ben Rockwood
@benr

Security

Protecting what matters.



Compliance

Doing what you say you do.

Posture

Situational Awareness

Tool Sprawl

You ain't got time for all dat!

Assurance

The reconciliation loop that aligns your **desired** (expected) state with **reality**.... So you can sleep at night.

cnquery

Cloud Native **Query**: A GraphQL Interface to All the Things

GraphQL in a Nutshell

```
~: vi — Konsole <2>

users {
  name
  uid
  shell
}

10,0-1 Top
```

```
~: vi — Konsole <2>

[]
users.list: [
  0: {
    shell: "/bin/bash"
    uid: 0
    name: "root"
  }
  1: {
    shell: "/usr/sbin/nologin"
    uid: 1
    name: "daemon"
  }
  ....

3,0-1 Top
```



GraphQL in a Nutshell

```
~: vi — Konsole <2>  
  
users.where(name == "benr"){ * }  
  
[  
~  
~  
  
13,0-1 All
```

```
~: vi — Konsole <2>  
users.where.list: [  
  0: {  
    name: "benr"  
    gid: 1000  
    group: group name="benr" gid=1000  
    sid: ""  
    uid: 1000  
    enabled: false  
    shell: "/bin/bash"  
    home: "/home/benr"  
    authorizedkeys.list: [  
      0: authorizedkeys.entry key="AAA...py/"  
      1: authorizedkeys.entry key="AAA..aDo=" ]  
    sshkeys: [  
@@@  
2,3 Top
```

For your systems

```
> ~: vi — Konsole <2>
$ cnquery run -c 'users{ name }'
```

```
users.list: [
  0: {
    name: "root"
  }
  1: {
    name: "daemon"
  }
  2: {
    name: "bin"
  }
  3: {
    name: "sys"
  }
  4: {
    name: "sync"
  }
  5: {
```

1,1 Top

For your fleet

```
> ~: vi — Konsole <2>
$ cnquery shell ssh benr@cuddletech.com --identity-file ~/.ssh/id_ed25519

cnquery> ports.where( state == 'listen' && address != "127.0.0.1" ) | address port protocol
ports.where.list: [
  0: {
    port: 60396
    address: "100.100.81.124"
    protocol: "tcp4"
  }
  1: {
    port: 111
    address: "0.0.0.0"
    protocol: "tcp4"
  }
  2: {
    port: 30931
    address: "0.0.0.0"
    protocol: "tcp4"
  }
]

3,92 Top
```

For your cloud

```
> | ○ ~ : vi — Konsole <2>
$ cnquery shell gcp org 2XXXXXXXXXXXXX4
[]
cnquery> gcloud.project.cloudRun.services{ name annotations }
gcloud.project.cloudRun.services: [
  0: {
    annotations: {
      client.knative.dev/user-image: "gcr.io/mondoo-web/registry-dev:latest"
    }
    name: "registry-dev"
  }
  1: {
    annotations: {
      client.knative.dev/user-image: "gcr.io/mondoo-web/registry-public:latest"
    }
    name: "registry-public"
  }
}

2,0-1 Top
```



cnspec

Cloud Native Specification: Creating and reporting on **assertions** about code, infrastructure, etc.

For your systems

```
> ~: vi — Konsole <2>
$ cnspec shell

cnspec> users.none(name == 'benr')
[failed] users.none()
  actual: [
    0: user id = user/1000/benr
  ]

[]
cnspec> users.contains(name == 'benr')
[ok] value: 1

12,0-1 Top
```

For your Code Repositories

```
> ~: vi — Konsole <2>
$ export GITHUB_TOKEN=ghp_e6XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXTi
$ cnspec run github org mondoohq -c '
  github.organization{
    twoFactorRequirementEnabled == true
  }'

github.organization: {
  twoFactorRequirementEnabled == true: true
}
```

5,13 All

Start with
query-packs & **policies**
ready to use!

Integrations Ready To Use For:

AWS

GCP

Azure

Kubernetes

Docker

Registries

VMware

Github

Gitlab

Google Workspace

MS365

Okta

Slack

Linux

macOS

Linux

Arista

DNS

TLS

Terraform

Vagrant

... And anything you can dream of!



Search or jump to...



[Pull requests](#) [Issues](#) [Codespaces](#) [Marketplace](#) [Explore](#)



[mondoohq / cnquery-packs](#) Public

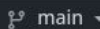
[Edit Pins](#)

[Unwatch](#) 7

[Fork](#) 1

[Star](#) 17

[Code](#) [Issues](#) 1 [Pull requests](#) 1 [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#) [Settings](#)



main

[cnquery-packs / core /](#)

[Go to file](#)

[Add file](#)



[czunker](#) ✨ [Extend k8s inventory with RBAC and containers \(#48\)](#) ...

✓ f81a779 2 weeks ago [History](#)

..		
.gitkeep	★ initial pack structure	5 months ago
mondoo-aws-incident-response.mql.yaml	✓ add versions to query packs (#43)	last month
mondoo-aws-inventory.mql.yaml	✓ add versions to query packs (#43)	last month
mondoo-gcp-inventory.mql.yaml	📞 fix platform tag and asset filter for gcp (#49)	2 weeks ago
mondoo-github-incident-response.mql.yaml	✓ add versions to query packs (#43)	last month
mondoo-github-inventory.mql.yaml	Enable spellchecking on policies (#47)	3 weeks ago
mondoo-kubernetes-incident-response.mql.yaml	✓ update policy platform tags (#50)	2 weeks ago
mondoo-kubernetes-inventory.mql.yaml	✨ Extend k8s inventory with RBAC and containers (#48)	2 weeks ago
mondoo-linux-incident-response.mql.yaml	✓ add versions to query packs (#43)	last month
mondoo-linux-inventory.mql.yaml	✓ add versions to query packs (#43)	last month
mondoo-macos-incident-response.mql.yaml	Enable spellchecking on policies (#47)	3 weeks ago



Search or jump to...

[Pull requests](#) [Issues](#) [Codespaces](#) [Marketplace](#) [Explore](#)



[mondoohq / cnspec-policies](#) Public

[Edit Pins](#)

[Unwatch](#) 5

[Fork](#) 6

[Starred](#) 28

[Code](#) [Issues](#) 13 [Pull requests](#) 9 [Discussions](#) [Actions](#) [Security](#) 385 [Insights](#) [Settings](#)

main

[cnspec-policies / core /](#)

[Go to file](#)

[Add file](#)

...

[tas50 and misterpantz control -> check and mondoo to cnspec \(#185\)](#) ... ✓ d08fa00 7 hours ago [History](#)

..		
.gitkeep	add readme to describe different channels	6 months ago
mondoo-aws-security.mql.yaml	control -> check and mondoo to cnspec (#185)	7 hours ago
mondoo-azure-security.mql.yaml	control -> check and mondoo to cnspec (#185)	7 hours ago
mondoo-dns-security.mql.yaml	fix yaml issues detected by new linter (#99)	2 months ago
mondoo-gcp-security.mql.yaml	Remove extra words from the spelling list (#186)	7 hours ago
mondoo-github-best-practices.mql.yaml	Fix titles and some descriptions (#167)	last week
mondoo-github-security.mql.yaml	control -> check and mondoo to cnspec (#185)	7 hours ago
mondoo-gitlab-security.mql.yaml	add additional tags to policies (#95)	3 months ago
mondoo-kubernetes-best-practices.mql.yaml	update policy platform tags (#151)	2 weeks ago
mondoo-kubernetes-security.mql.yaml	Query titles should end in a period (#159)	2 weeks ago
mondoo-linux-security.mql.yaml	Apparmor as alternative to SELinux in auditd (#177)	3 days ago
mondoo-linux-workstation-security.mql.yaml	Remove incorrect SSM instructions (#143)	3 weeks ago
mondoo-macos-security.mql.yaml	control -> check and mondoo to cnspec (#185)	7 hours ago
mondoo-microsoft-vulnerability.mql.yaml	add microsoft vuln policy for CVE-2023-21716 (#150)	2 weeks ago
mondoo-ms365-security.mql.yaml	control -> check and mondoo to cnspec (#185)	7 hours ago
mondoo-ocp-security.mql.yaml	control -> check and mondoo to cnspec (#185)	7 hours ago



xSPM

Extensible Security Posture Management ==
Open Source, Cloud Native

github.com/mondoohq

Learn more at Mondoo.com



Thank you



Ben Rockwood



@benr



ben@mondoo.com



mondoo.com