New issue

Jump to bottom

vault_gcp_auth_backend_role does not apply bound_labels #996

Closed **BrandonIngalls** opened this issue on Mar 12, 2021 · 1 comment · Fixed by #1028

BrandonIngalls commented on Mar 12, 2021 Contributor

The `vault_gcp_auth_backend_role` resource does not apply bound_labels to the vault auth method.

Earlier this week while debugging an issue I tried to authenticate to my vault from a VM that did not have the the `bound_label` that I had defined in my terraform configuration... To my surprise my authentication was successful, this led me down the route of finding out why terraform was lying to me.

Terraform Version

```
[~]$ terraform -v
Terraform v0.14.7
+ provider registry.terraform.io/hashicorp/vault v2.18.0
```

Affected Resource(s)

- vault_gcp_auth_backend_role

Terraform Configuration Files

```
terraform {
  required_providers {
    vault = {
      source  = "hashicorp/vault"
      version = "2.18.0"
    }
  }
}

provider "vault" {
  address = "http://127.0.0.1:8200"
  token   = "root"
}

resource "vault_gcp_auth_backend" "gcp" {
  path = "gcp"

  description = "debug gcp auth endpoint; automation=terraform"
}

resource "vault_gcp_auth_backend_role" "gcp" {
  backend = vault_gcp_auth_backend.gcp.path

  role = "test-role"
  type = "gce"

  bound_labels = ["role:test"]
}
```

Expected Behavior

Terraform **should** apply the security controls that it says it does for the vault provider.

Actual Behavior

Terraform does not install the `bound_labels` configuration to the `vault_gcp_auth_backend_role` resource.

Steps to Reproduce

```
# Start a dev vault instance
[~]$ vault server -dev -dev-root-token-id=root

# Apply my example terraform state
[~]$ terraform init
[~]$ terraform apply

# Run a plan to show that terraform thinks that it has set the bound_labels
# correctly and that "no changes are required"
[~]$ terraform plan

# Setup vault vars
[~]$ export VAULT_ADDR='http://127.0.0.1:8200'
[~]$ export VAULT_TOKEN='root'

# Check the terraform created gcp auth role's config...
# Note that `bound_labels` is missing
[~]$ vault read auth/gcp/role/test-role
Key                         Value
---                         -----
add_group_aliases           false
role_id                     57b6301e-6368-1e1b-51e7-2b31361e8589
token_bound_cidrs           []
token_explicit_max_ttl      0s
token_max_ttl               0s
token_no_default_policy     false
token_num_uses              0
token_period                0s
token_policies              []
```

```
token_ttl                0s
token_type               default
type                     gce

# Use the vault CLI / API to actually install a `bound_labels`
[~]$ vault write auth/gcp/role/test-role/labels add=role:dog

# Verify the manual change we just made...
[~]$ vault read auth/gcp/role/test-role
Key                      Value
---                      -----
add_group_aliases        false
bound_labels             map[role:dog]
role_id                  57b6301e-6368-1e1b-51e7-2b31361e8589
token_bound_cidrs        []
token_explicit_max_ttl   0s
token_max_ttl            0s
token_no_default_policy  false
token_num_uses           0
token_period             0s
token_policies           []
token_ttl                0s
token_type               default
type                     gce

# Try to run a terraform plan and terraform will panic
[~]$ terraform plan
# https://gist.github.com/BrandonIngalls/5c8d1089aa443580dd71d3f755600a29
```

👍 1

This was referenced on Apr 14, 2021

Fix bound_lables not being set in gcp auth #1025

Closed

gcp auth: fix bound_labels not being applied #1028

Merged

jasonodonnell closed this as completed in #1028 on Apr 19, 2021

---

chair6 commented on Apr 21, 2021

Thanks for reporting, **@BrandonIngalls**! We released a fix for this issue today, and published a security bulletin at https://discuss.hashicorp.com/t/hcsec-2021-11-terraform-s-vault-provider-did-not-correctly-configure-bound-labels-for-gcp-auth/23464/2. I've filed a request with MITRE to publish CVE-2021-30476 and provided them with an updated description.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

gcp auth: fix bound_labels not being applied
hashicorp/terraform-provider-vault

Fix bound_lables not being set in gcp auth
hashicorp/terraform-provider-vault

2 participants