



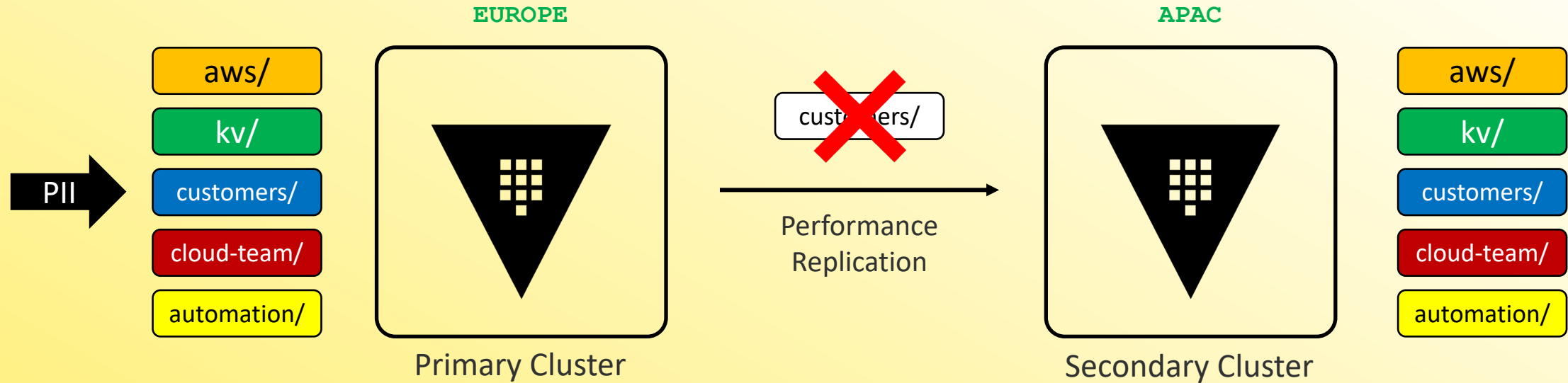
# Creating a Paths Filter



# Replicating Data



Regulatory Compliances may restrict you from replicating certain data (GDPR)



# Paths Filter



Vault has a **Paths Filters** capability when using Performance Replication

- This enables you to configure an **allowlist** or **denylist** for paths in Vault
- Determines what is replicated to other clusters

Paths Filters work on paths such as secrets engines, auth methods, AND namespaces

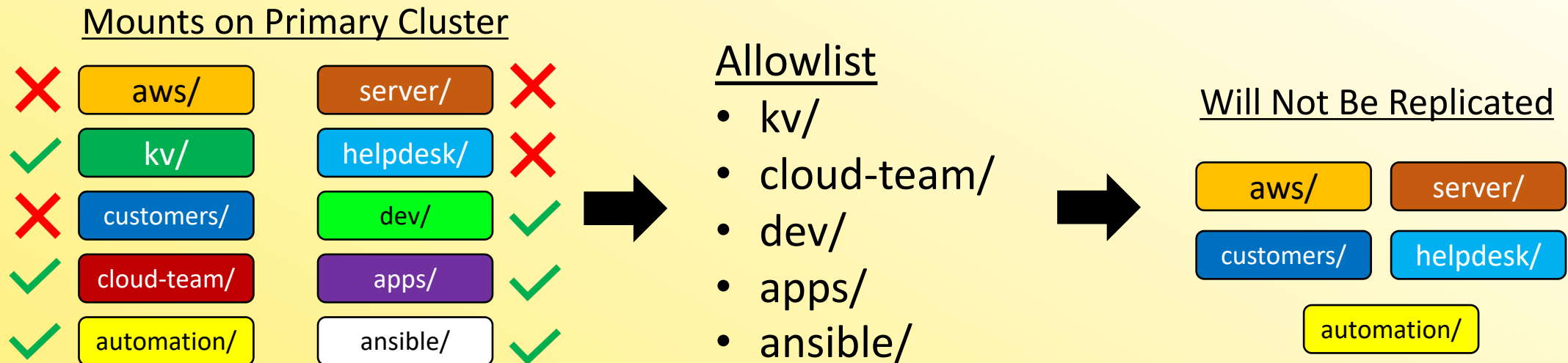


# Paths Filter - Allowlist



## Allowlist:

- only the selected paths are included for replication to the secondary



# Paths Filter - Denylist



## Denylist:

- All paths will be replicated EXCEPT the selected mount paths

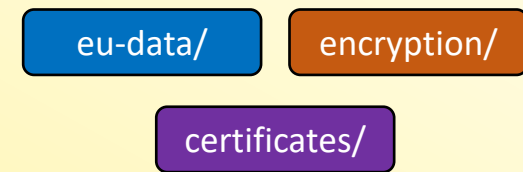
### Mounts on Primary Cluster

✓	gcp/	encryption/	✗
✓	secrets/	mobile/	✓
✗	eu-data/	engineering/	✓
✓	k8s/	certificates/	✗
✓	puppet/	rdt-team/	✓

### Denylist

- eu-data/
- certificates/
- encryption/

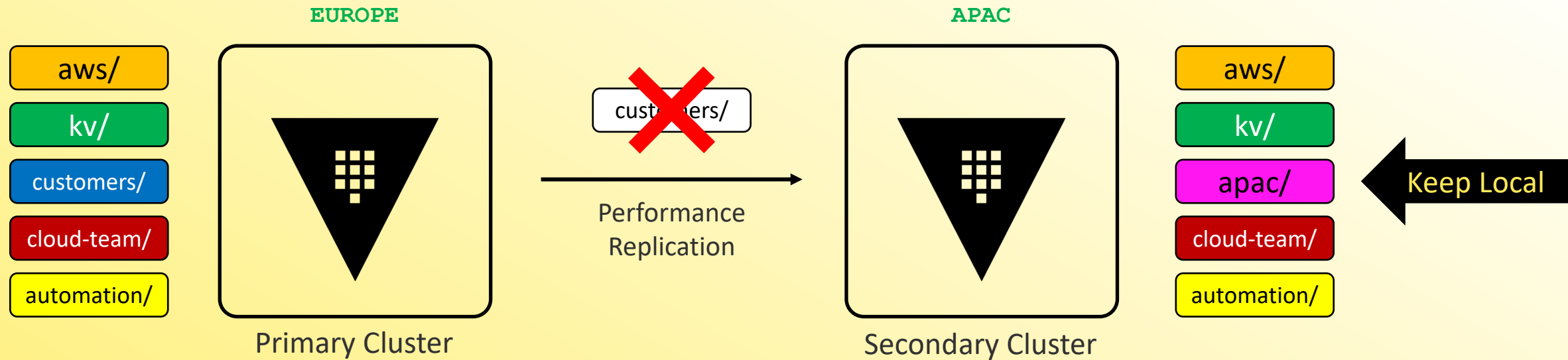
### Will NOT Be Replicated



# Local Mounts



What if we want a mount on the Perf Secondary but we do NOT want it be replicated throughout the replica set?

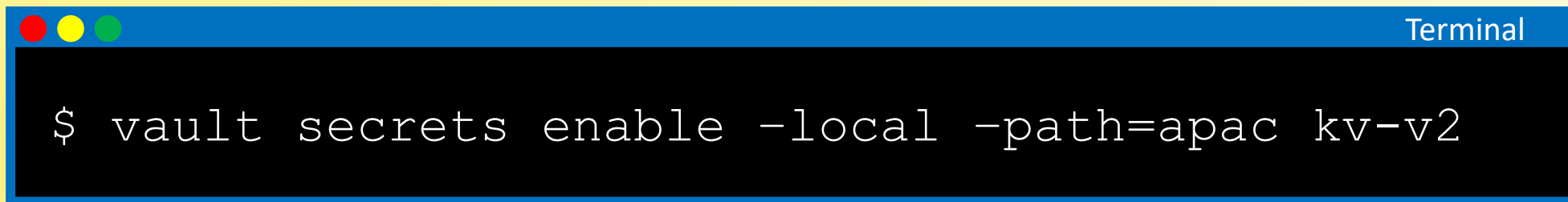


# Create a Local Mount



You can mark a secrets engine or auth method as **local** so it is not replicated or removed by replication configurations

Enable the secrets engine/auth method on the secondary cluster using the **-local** flag

A terminal window with a blue title bar labeled "Terminal" and three colored window control buttons (red, yellow, green) on the left. The terminal has a black background with white text showing a command to enable a local secrets engine.

```
$ vault secrets enable -local -path=apac kv-v2
```



# Create a Paths Filter



**Performance** primary 157c52ca

Details Manage **Secondaries**

**Generate a secondary token**

Generate a token to enable performance Replication or change primaries on secondary cluster.

**Secondary ID**

secondary

This will be used to identify secondary cluster once a connection has been established with the primary.

**TTL**

30 seconds

This is the Time To Live for the generated secondary token. After this period, the generated token will no longer be valid.

**Filtered paths**

**Include everything**

All namespaces and mounts in this cluster will be replicated

☐

**Allow**

Only include the selected namespaces and mounts

☐

**Deny**

Do not include the selected namespaces and mounts

☒

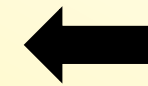
**Paths in this deny**

Search

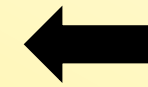
eu\_data/

automation/

**Generate token** **Cancel**



Configure within the Secondary configuration section on the Primary Cluster when creating a Secondary token



Select the type of list you want to create – Allow or Deny



Type the path to add



Paths in list





# Create a Paths Filter



```
Terminal
$ vault write sys/replication/performance/primary/paths-filter/us-east-dr \
mode=allow \
paths=aws/,hcvop/,customers/
```

Allow or  
Deny List?

Paths to include in the list

The Secondary  
Cluster ID



# Create a Paths Filter

Result of Previous Command



[Replication](#) < Performance

## Performance primary

[Details](#) [Manage](#) [Secondaries](#)

### Mount filter config for us-east-dr

Mode	allow
Paths	aws/ customers/ hcvop/

