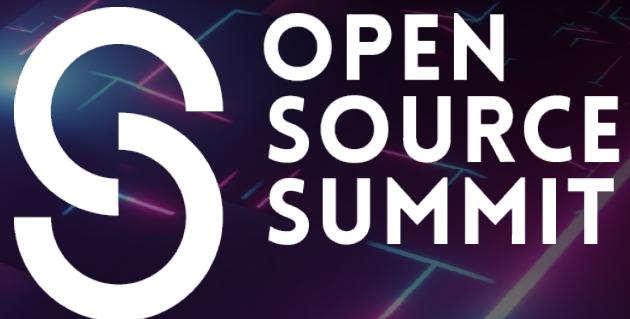


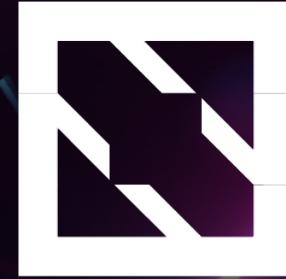


KubeCon

THE LINUX FOUNDATION



China 2024



CloudNativeCon





KubeCon



CloudNativeCon



China 2024

The Challenges of Kubernetes Data Protection

- Real Examples and Solutions with Velero

Wenkai Yin (wenkai.yin@broadcom.com)
Bo Zou (zoubo@jibudata.com)

Agenda

- Velero Introduction
- Challenges and solutions
- Summary

What Is Velero



KubeCon



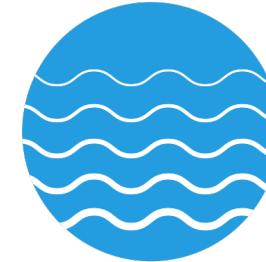
CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



China 2024



VELERO

Open source backup and restore tool

Website: <https://velero.io/>

Github: <https://github.com/vmware-tanzu/velero>

Community: <https://velero.io/community/>

What Is Velero



KubeCon



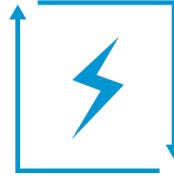
CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT

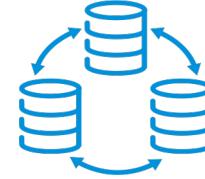


China 2024



Disaster Recovery

Reduces time to recovery in case of infrastructure loss, data corruption, and/or service outages.



Data Migration

Enables cluster portability by easily migrating Kubernetes resources from one cluster to another.



Data Protection

Offers key data protection features such as scheduled backups, retention schedules, pre or post-backup hooks for custom actions.

How Velero Works



KubeCon



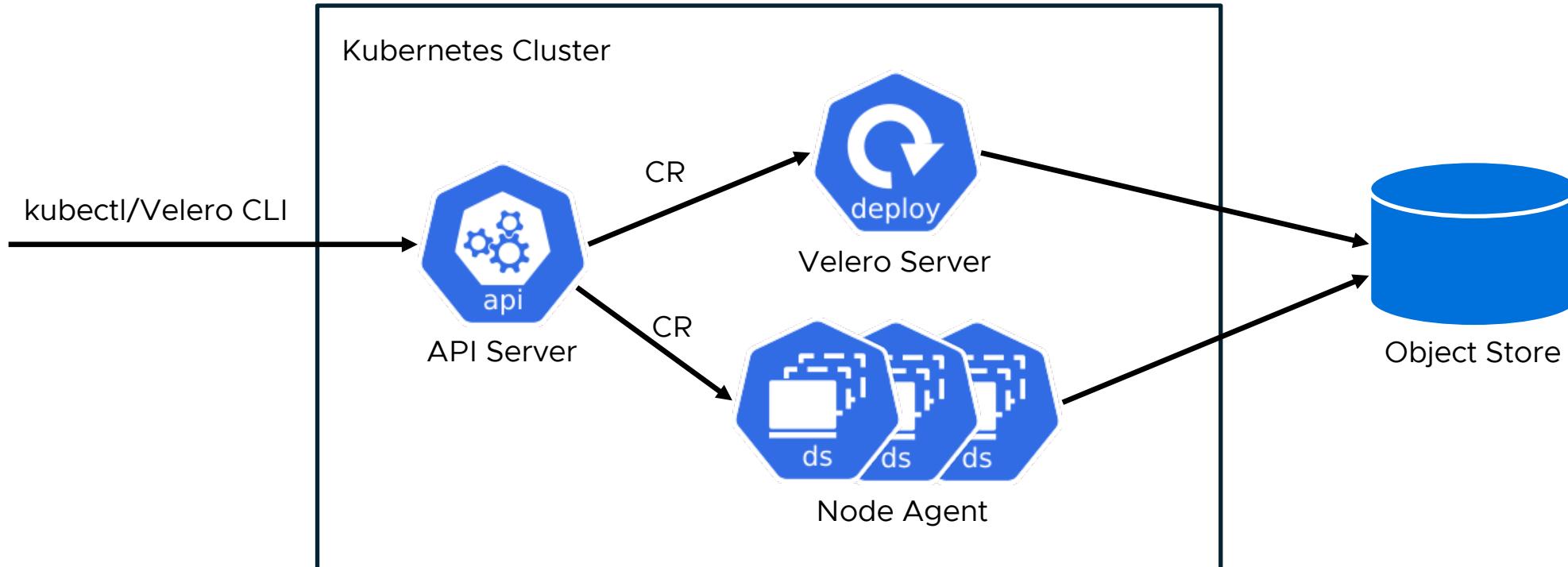
CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



China 2024



Backup Kubernetes Resources



KubeCon



CloudNativeCon



OPEN
SOURCE
SUMMIT



China 2024

Backup/Restore Kubernetes Resources:



....

Backup works like:

```
kubectl get <resources> -o yaml > resources.yaml
```

Restore works like:

```
kubectl apply -f resources.yaml
```

Backup Volume Data



KubeCon



CloudNativeCon

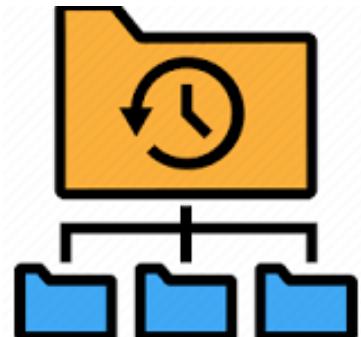


THE LINUX FOUNDATION
OPEN SOURCE SUMMIT



China 2024

Backup/Restore Volume Data:



File System Backup



CSI Snapshot



CSI Snapshot + Data Move



Native Snapshot

Customization/Extension



KubeCon



CloudNativeCon



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT

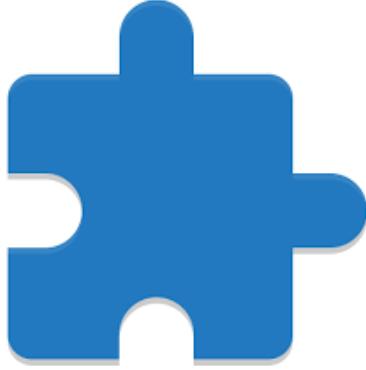


AI_dev
Open Source Dev & ML Summit

China 2024



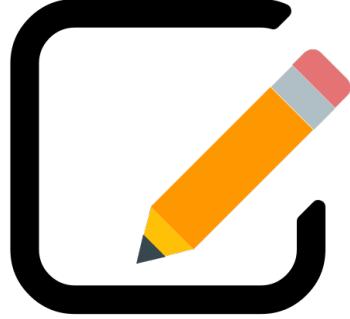
Filter



Plugin



Hooks



Resource Modifier



KubeCon



CloudNativeCon



China 2024

Challenges and Solutions

Defining Complex Applications by Application Templates and Domain Knowledge



KubeCon



CloudNativeCon

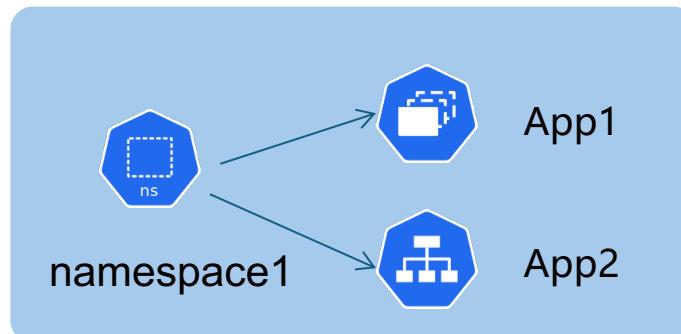


China 2024

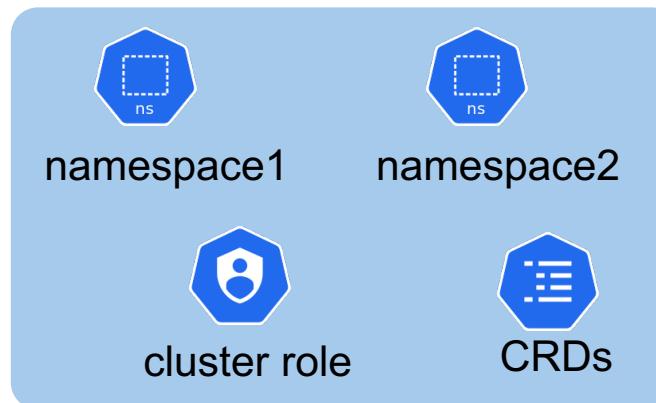


- How to define an application?
 - Application dependency could be very complex - nobody wants to untangle the mess
 - Third-party application - only vendor knows
 - I want to backup a platform - who knows what to backup?
- Kubernetes complex applications
 - Multiple application under one namespace
 - One application may contain multiple namespaces, and some cluster scoped resources
 - From business view, a complete application may contain multiple small applications

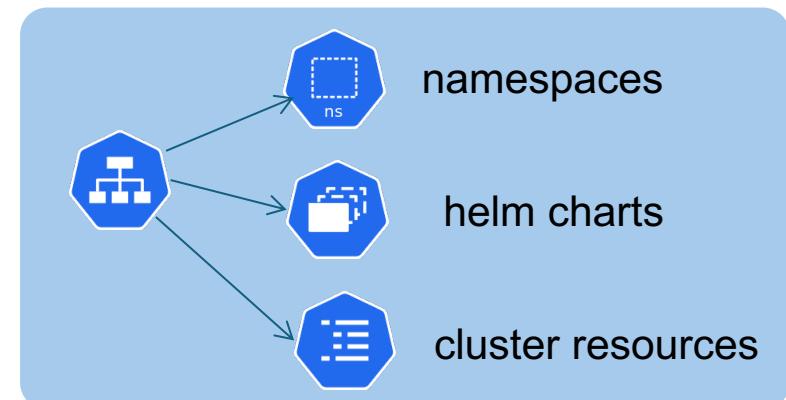
k8s complex application example 1



k8s complex application example 2



k8s complex application example 3



Application Management for Backup and Restore



KubeCon



CloudNativeCon



China 2024



User requirements:

- Backup and restore Kubernetes resources of an application
- Backup and restore data for Persistent Volume Claims (PVCs)
- Backup some of the PVCs
- Selectively restore certain resources
- Backup and restore complex applications
- Backup and restore entire clusters

Application templates

- Using Velero resource filters
- Extended resource filters on backup CR
- Operate on UI

Application backup process:



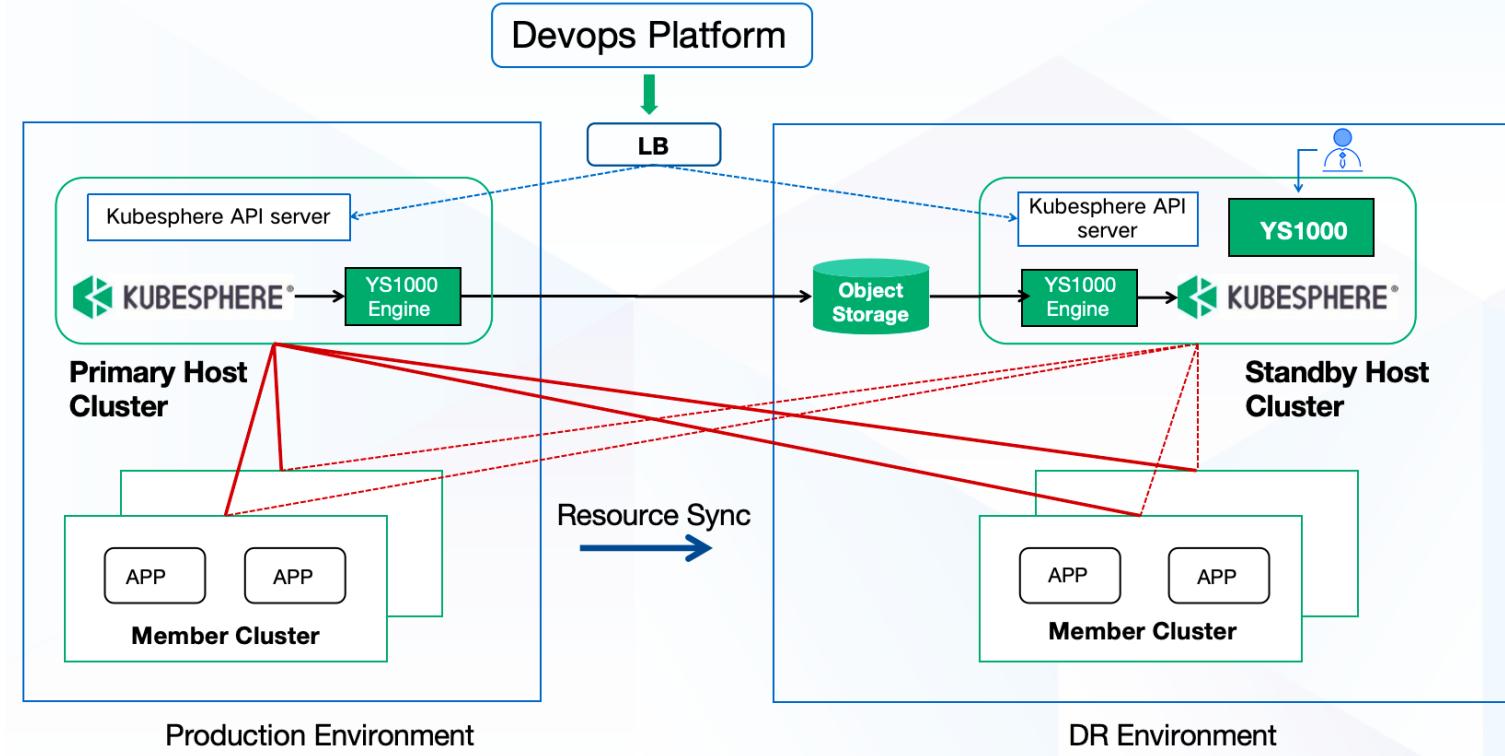
Application restore process:



User Example: Kubesphere Host Cluster Definition



- Customer pain-points:
 - When host cluster is down, it's very time consuming to start the standby cluster and then manage all member clusters
- Tricky part:
 - ✓ How to define host cluster?
 - ✓ Communicated with 4-5 developers across 2+ teams to define clearly what kind of resources are included in a host cluster
- 5 categories of GVK:
 - ✓ Users, roles and projects (10+)
 - ✓ Kubesphere system configurations
 - ✓ Cluster federation (20+)
 - ✓ Alerts and notifications (15+)
 - ✓ System monitoring (5+)



Backup Application Data In Consistent Manner Under Various Situations



KubeCon



CloudNativeCon



How to perform the backup?

- Various databases and middlewares: MySQL/PG/MongoDB/Redis/...
- Using database backup locks: each DB has different means
- Using database snapshot/dumps: no uniformed method
- Deployment mode varies: master/slave, cluster, sharding

How to restore and bring up the database?

- Deployment mode impacts: restore single replica or all replicas?
- Database specific: application is restored, but how to make the DB running without a problem?

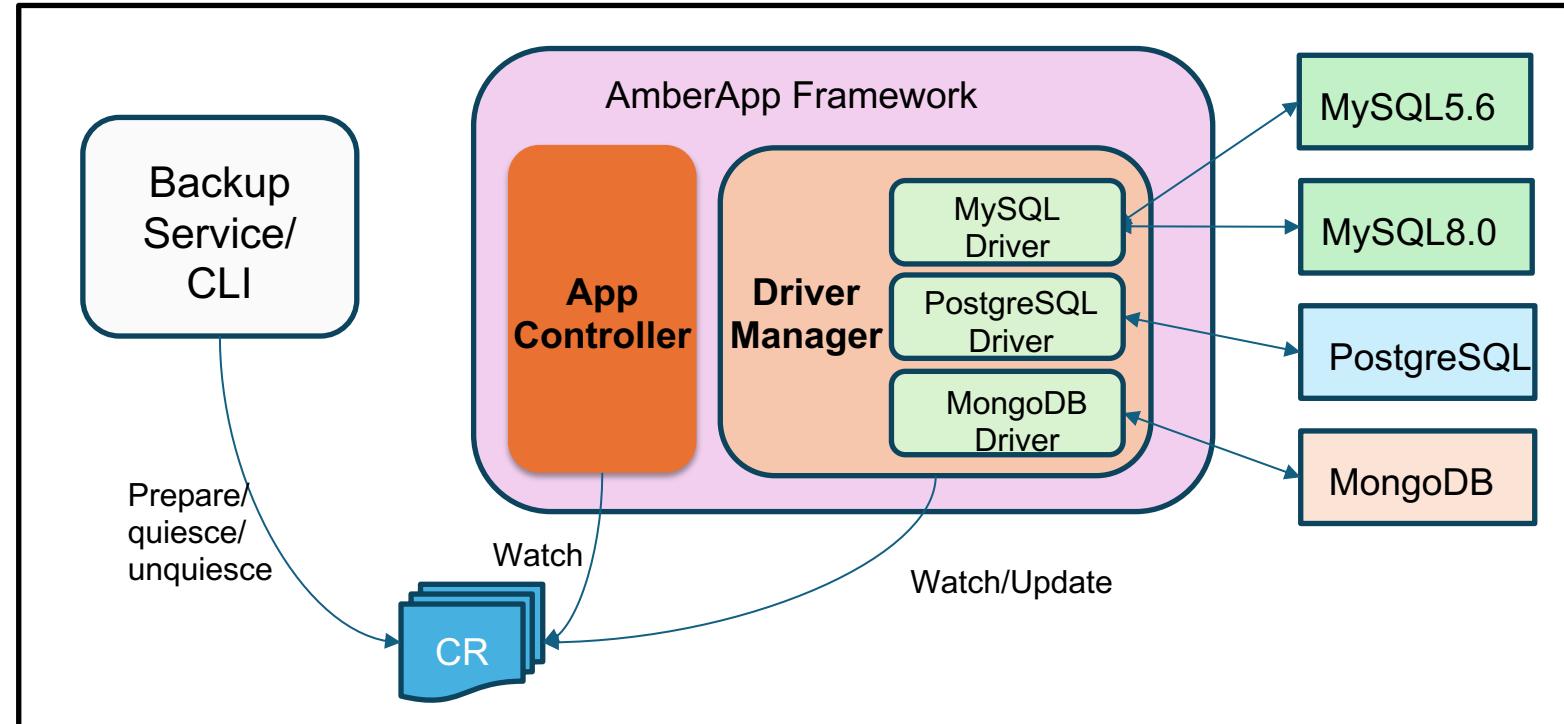
Using Backup Lock to Backup Database In Consistency Manner



Practical issues:

1. How to configure/change/update the database connection?
2. How to observe the configuration results?
3. How to debug the errors?
4. Can we do it non-intrusively?
5. How to setup the backup/restore for master/slave MySQL?

amberapp: a common app consistency service that can work together with Velero and other k8s backup solutions

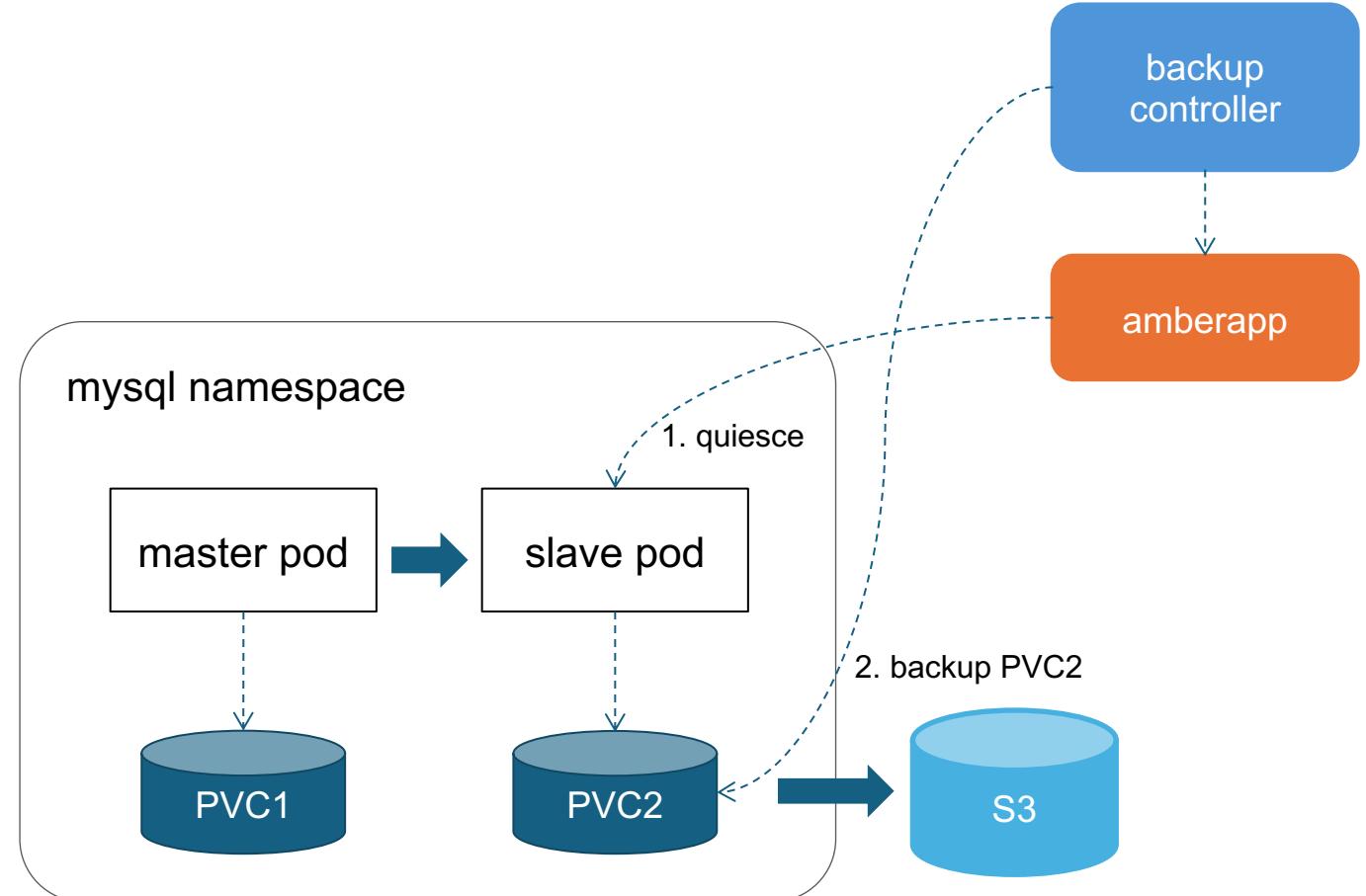


github repo: <https://github.com/jibudata/amberapp>

User Example: Backup MySQL Master/Slave Using Amberapp



- Deployment mode
 - master/slave
- Existing data
 - 400GB
- Incremental data
 - 2GB per day
- Backup plan:
 - Only backup slave PVC
 - Initial copy no lock
 - Incremental copy with quiesce lock
- Restore plan:
 - Restore slave PVC
 - Replica slave PVC data
 - Re-setup MySQL master/slave



Backup Resource Considerations in Large Environments



KubeCon



CloudNativeCon

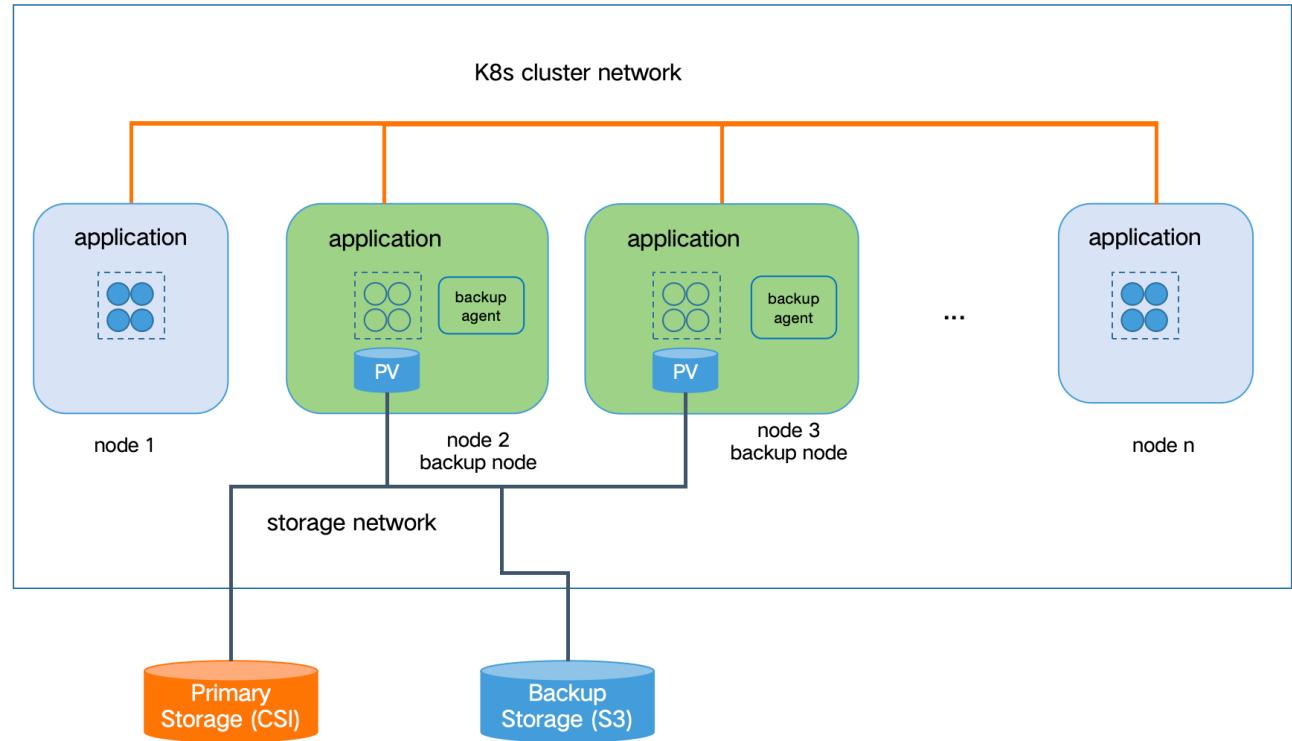


- Application and Backup resource isolation
 - Backup job execution need to minimize impact to business application
 - Backup network isolation
- QoS consideration
 - Job priority
 - Bandwidth limitation
- Scalability consideration
 - How many jobs can run in parallel in a cluster
 - How many jobs can run in parallel in a single node

User Example: Backup Resource Planning at Production Clusters



- 200+ nodes
- 10+ clusters
- **Backup resource planning**
 - Each cluster has dedicated backup node
 - Configure node affinity to pin backup agent to specific node
- **Shared network**
 - Backup storage network across 2 datacenters
 - Need to configure QoS at day-time
- **Concurrency control**
 - Cluster level job concurrent worker: 4
 - Each node can configure job concurrent works (default: 1)



Handle Application Restore on Heterogenous Environments



KubeCon



CloudNativeCon



- User scenarios:
 - Application migration to new k8s platform
 - Application migration over few k8s versions
 - Storage migration
 - Application restore to different cluster for testing

End to End

- Application dependency
- Application shutdown
- Migration testing
- Roll back

Storage

- Storage class
- PVC/PV conversion
- PV data

Resource conversion

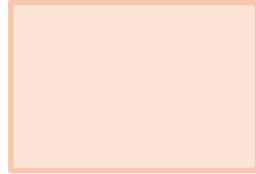
- Resource conversion
- Detection/display
- Human intervene/interaction

Storage Conversion

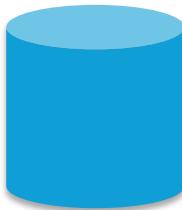


China 2024

Hostpath/NFS Volume

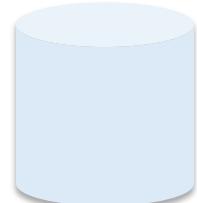


CSI Volume



- Volume include/exclude
- PVC fields change/setup
- Data directories in NFS volume

CSI Storage1

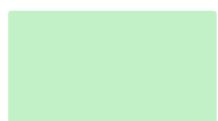


CSI Storage2



- Storage class mapping
- Downtime window
- Migration test

PVC1



PVC2



- PV retain
- Update PV csi.driver name and storageClassName
- volumeHandle keep same

```
volumes:  
- name: nfs-settings  
  persistentVolumeClaim:  
    claimName: yprsetting  
- name: nfs-ypr  
  persistentVolumeClaim:  
    claimName: iuapypr  
- hostPath:  
  path: /bin/docker  
  type: ""  
  name: volume-0  
- hostPath:  
  path: /var/run/docker.sock  
  type: ""  
  name: volume-1  
- hostPath:  
  path: /root/.docker  
  type: ""  
  name: volume-2
```

API Resource Conversion at Restore



China 2024

- Resource restore to new platforms:
 - K8s version difference > 3 major versions
 - Change platform (Istio/Jenkins => new version)
 - New cloud (Load Balancer/Service)

修改任意资源

资源选择

命名空间
wp-ceph,mysql-ceph 2

类型
services

名称
请选择...

匹配标签

资源修改

类型
Strategic Merge Patch

内容(支持格式为yaml或json)
1 {"spec": {"type": "ClusterIP", "ports": [{"port": 80, "targetPort": 80, "protocol": "TCP", "name": "http"}, {"port": 443, "targetPort": 443, "protocol": "TCP", "name": "https"}], "selector": {"app": "nginx"}, "replicas": 2}, "status": {"replicas": 2}}

完成 上一步 取消

- Resource conversion framework:
 - Build on top of Velero resource modifiers
 - Operate on UI for better user experience
 - Build into restore workflow

修改任意资源

资源选择 资源修改

命名空间
wp-ceph 1

类型
deployments.apps

名称
请选择...

匹配标签
请按照格式输入, 例: a=b, a为key, b为值, 输入...
app=nginx

类型
JSON Merge Patch

内容(支持格式为yaml或json)
1 spec:
2 | replicas: 2|

完成 上一步 取消

User Example: Common Requirements



China 2024

- Configmap: change database username/password
- Secret: change username/password
- ingress: v1beta1 => v1
- Openshift route => ingress

Resource Modifiers

Do you need to modify other resources such as ConfigMap, Secret, Ingress, Service, and volumes?

Additional Configuration

Modify ConfigMap

Namespace	Name
nginx	kube-root-ca.crt

Modify key-value pairs

Field Name	Field Value
new-key1	data1

+

Resource Modifiers

Do you need to modify other resources such as ConfigMap, Secret, Ingress, Service, and volumes?

Additional Configuration

Modify Secret

Namespace	Name
mysql	default-token-v5q56

Modify key-value pairs

Field Name	Field Value
new-username	new-password

+

Finish

Back

Cancel

Finish

Back

Cancel

User Example: LB Conversion on Huawei CCE



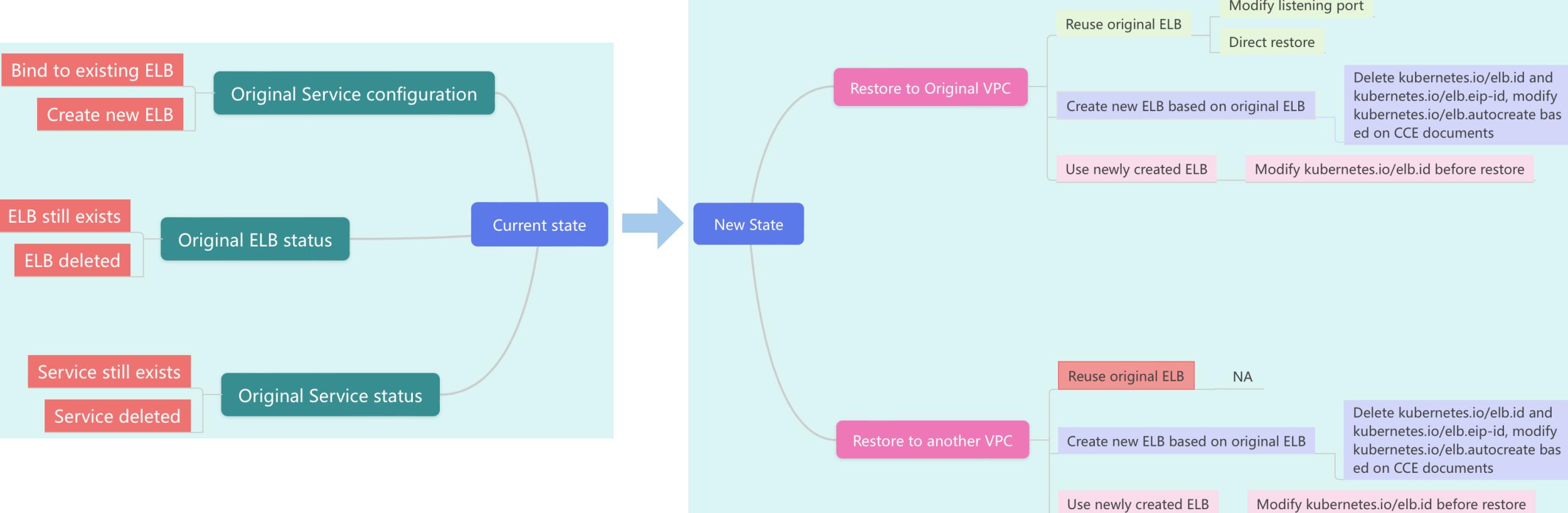
China 2024

Major scenarios for restore:

1. Original cluster exists,
restore application to
remote cluster for testing

2. Application deleted, need
to restore to original cluster

3. ELB is mistakenly deleted,
need to create new ELB and link
service to new ELB



Summary: Future Outlook



KubeCon



China 2024



- Application Definition and Resource Capture
 - Work with application developers
 - Build domain knowledge into software
 - Contribute to the community
- Application Data Consistency
 - Physical backup with backup lock is a basis
 - Logical backup still need lots of work
- Backup resource planning
 - Lan-free backup is popular
 - Production environment needs QoS planning
 - Backup job scalability has room for improvements
- Application Restoration in Heterogeneous Environments
 - Need to work out end-2-end solution
 - Storage conversion is not just storage class change
 - Resource conversion need application and business knowledge
 - Need to work with cloud provider for Load Balancer and networking issues

Welcome to Join the Velero CN Community



China 2024

https://velero.cn

Velero中文社区

搜索 简体中文 换肤 jerry-jibu

发布主题 最近回复

L 报告解读: GigaOm K8s 数据保护关键能力报告
lonelamp 发布于 13 days ago
技术讨论 原创 1

H velero的常见问题之: 备份恢复任务卡住很久是怎么回事
half-life 发布于 17 days ago
技术讨论 原创 1

S 使用 Velero 对 k8s 集群进行完整备份和还原
shaof 发布于 6 Sep
技术讨论 原创 1

L Velero v1.6 有哪些新功能
lonelamp 发布于 6 Sep
技术讨论 原创 1

J 转载 - 灾备知识总结: 容灾与备份区别、灾备技术、容灾体系规划
jerry-jibu 发布于 14 Aug
技术讨论 转载 0

H Velero代码深入分析之 (二)
half-life 发布于 12 Aug
技术讨论 原创 0



Wechat Pub Account



KubeCon



CloudNativeCon



China 2024

Q & A