Portworx

svcaccount-px-backup-proc-rvw-doc-proj-01

Updated: 1/12/2024

[Concepts 4](#_Toc156819085)

[Binding 4](#_Toc156819086)

[ClusterRole 4](#_Toc156819087)

[Role 4](#_Toc156819088)

[Procedures Overview 5](#_Toc156819089)

[## overview, Design Goals 5](#_Toc156819090)

[All namespaces – PX-Backup ServiceAccount, ClusterRole, ClusterRoleBinding; ConfigMap Role, RoleBinding; ServiceAccount Secret Token 6](#_Toc156819091)

[sa-px-backup-all.yaml 6](#_Toc156819092)

[sa-px-backup - PX-Backup ServiceAccount 6](#_Toc156819093)

[px-backup-all-clusterrole 6](#_Toc156819094)

[px-backup-all-clusterrolebinding 6](#_Toc156819095)

[ks-configmap-role 6](#_Toc156819096)

[ks-configmap-rolebinding 6](#_Toc156819097)

[sa-px-backup-secret 6](#_Toc156819098)

[config\_sa-px-backup - ; ServiceAccount Kubeconfig 8](#_Toc156819099)

[get service account sa-px-backup token 8](#_Toc156819100)

[get service account sa-px-backup certificate 8](#_Toc156819101)

[config\_sa-px-backup 9](#_Toc156819102)

[## 10/26/2023 Next Steps 11](#_Toc156819103)

[sa-px-backup-default.yaml 11](#_Toc156819104)

[sa-px-backup-default - PX-Backup ServiceAccount 11](#_Toc156819105)

[px-backup-default-clusterrole 11](#_Toc156819106)

[px-backup-default-rolebinding 11](#_Toc156819107)

[ks-configmap-role 11](#_Toc156819108)

[ks-configmap-rolebinding 11](#_Toc156819109)

[sa-px-backup-default-secret 11](#_Toc156819110)

[config\_sa-px-backup-default 11](#_Toc156819111)

[Add as or-cluster03-default 11](#_Toc156819112)

[svcaccount-px-backup-proc-rvw-doc-proj-02 12](#_Toc156819113)

[Logs 13](#_Toc156819114)

[Troubleshooting 14](#_Toc156819115)

[Resources 15](#_Toc156819116)

[Adding a Service Account Authentication Token to a Kubeconfig File 15](#_Toc156819117)

[app-with-px-backup – Tom Lapp GitHub 15](#_Toc156819118)

[Configure Service Accounts for Pods | Kubernetes 15](#_Toc156819119)

[Grant access to a namespace for non-admin user – PX-Backup 15](#_Toc156819120)

[How To Create Kubernetes Service Account For API Access 15](#_Toc156819121)

[How to regenerate Service Account tokens in Kubernetes | Support | SUSE 15](#_Toc156819122)

[How to Use ClusterRoleBinding With A ServiceAccount in All Namespaces (or a few) 15](#_Toc156819123)

[jwt - Set Expiry of Kubernetes service tokens - Stack Overflow 15](#_Toc156819124)

[Managing Service Accounts 15](#_Toc156819125)

[TokenRequest API 15](#_Toc156819126)

# Concepts

## Binding

Grants permissions to a Role in a namespace or a ClusterRole in all namespaces

## ClusterRole

Sets permissions as a non-namespaced resource

ClusterRole + RoleBinding = particular namespace

ClusterRole + ClusterRoleBinding = all namespaces

## Role

Sets permissions within a particular namespace

Role + RoleBinding = same namespace

# Procedures Overview

## ## overview, Design Goals

Specify ServiceAccount sa-px-backup to protect clusters with PX-Backup

sa-px-backup, px-backup-all-clusterrole, px-backup-all-clusterrolebinding

Cluster-wide access to all namespaces, current, future

Managed, limited lifecycle

Manageable method(s) to end, begin validity

sa-px-backup-default, px-backup-default-clusterrole, px-backup-default-rolebinding

Access to specific namespace only

Managed, limited lifecycle

# All namespaces – PX-Backup ServiceAccount, ClusterRole, ClusterRoleBinding; ConfigMap Role, RoleBinding; ServiceAccount Secret Token

## sa-px-backup-all.yaml

## sa-px-backup - PX-Backup ServiceAccount

## px-backup-all-clusterrole

## px-backup-all-clusterrolebinding

## ks-configmap-role

## ks-configmap-rolebinding

## sa-px-backup-secret

---

apiVersion: v1

kind: ServiceAccount

metadata:

name: sa-px-backup

namespace: default

---

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRole

metadata:

name: px-backup-all-clusterrole

rules:

- apiGroups: ["\*"]

resources: ["namespaces", "clusterrolebindings", "persistentvolumes", "clusterroles", "nodes", "storageclasses"]

verbs: ["get", "list", "watch", "create"]

- apiGroups: ["stork.libopenstorage.org"]

resources: ["schedulepolicies"]

verbs: ["create", "delete", "deletecollection", "get", "list", "patch", "update", "watch"]

- apiGroups: ["stork.libopenstorage.org"] # for controller support

resources: ["\*"]

verbs: ["list", "get", "watch"]

- apiGroups: ["snapshot.storage.k8s.io"]

resources: ["volumesnapshotclasses"]

verbs: ["get", "list"]

- apiGroups: ["", "extensions", "apps"]

resources: ["\*"]

verbs: ["\*"]

- apiGroups: ["batch"]

resources:

- jobs

- cronjobs

verbs: ["\*"]

- apiGroups: ["stork.libopenstorage.org"]

resources: ["\*"]

verbs: ["create", "delete", "deletecollection", "get", "list", "patch", "update", "watch"]

---

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRoleBinding

metadata:

name: px-backup-all-clusterrolebinding

subjects:

- kind: ServiceAccount

name: sa-px-backup

namespace: default

roleRef:

apiGroup: rbac.authorization.k8s.io

kind: ClusterRole

name: px-backup-all-clusterrole

---

apiVersion: rbac.authorization.k8s.io/v1

kind: Role

metadata:

name: ks-configmap-role

namespace: kube-system

rules:

- apiGroups: [""]

resources: ["configmaps"]

verbs: ["get", "list"]

---

apiVersion: rbac.authorization.k8s.io/v1

kind: RoleBinding

metadata:

name: ks-configmap-rolebinding

namespace: kube-system

subjects:

- kind: ServiceAccount

name: sa-px-backup

namespace: default

roleRef:

apiGroup: rbac.authorization.k8s.io

kind: Role

name: ks-configmap-role

---

apiVersion: v1

kind: Secret

type: kubernetes.io/service-account-token

metadata:

name: sa-px-backup-secret

namespace: default

annotations:

kubernetes.io/service-account.name: sa-px-backup

# config\_sa-px-backup - ; ServiceAccount Kubeconfig

## get service account sa-px-backup token

kubectl get secret sa-px-backup-secret -n default -o "jsonpath={.data.token}" | base64 -d

eyJhbGciOiJSUzI1NiIsImtpZCI6Il9SSW11QzRNNFRKU2pNeHIycTRKbjA2VG85VlludTIyMFd5VFJzNWdVTUUifQ.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6InNhLXB4LWJhY2t1cC1zZWNyZXQiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoic2EtcHgtYmFja3VwIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLWFjY291bnQudWlkIjoiYmVmMTQyMzUtMmU5Ny00M2Y0LWE0ODQtZGYzNjA0ZDMyNjVhIiwic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW50OmRlZmF1bHQ6c2EtcHgtYmFja3VwIn0.tvx6GQkmpriEWdUOJ1oAXWEiXP-boyazHnqPr3KTfwjDWQHwG49yyY5CChP9A2Amzjq5CVS60HGkmkcliBVpe2wNiEVtLpBj-ZyxocHcxTxUBQ\_iuYPDILT5LssmEX1k3vzD\_CT1-eW7wxduus\_cAKYVRHt6RVt\_a7VDwbv6v4gJeSX7u3kZ8bbV6opWNyUlJ05uPW0qEruJgxVQzEl4ST8g\_CHdMkBrfGuZ8hvW2hvl3Zyf61V42aroGL\_Ns0\_OJwvCbvixFxUWLjM9mxwgv4-dpNxfqbW3S9oKmF83piiY0qjuSaWCzU1oMNHj7Ze16It7hAc6-2luvCmmogJW9A

## get service account sa-px-backup certificate

kubectl get secret sa-px-backup-secret -n default -o "jsonpath={.data['ca\.crt']}"



## config\_sa-px-backup

apiVersion: v1

clusters:

- cluster:

certificate-authority-data: 

server: https://10.1.6.150:6443

name: or-cluster03

contexts:

- context:

cluster: or-cluster03

namespace: default

user: sa-px-backup

name: or-cluster03-sa-px-backup

current-context: or-cluster03-sa-px-backup

kind: Config

preferences: {}

users:

- name: sa-px-backup

user:

client-key-data: 

token: eyJhbGciOiJSUzI1NiIsImtpZCI6Il9SSW11QzRNNFRKU2pNeHIycTRKbjA2VG85VlludTIyMFd5VFJzNWdVTUUifQ.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6InNhLXB4LWJhY2t1cC1zZWNyZXQiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoic2EtcHgtYmFja3VwIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLWFjY291bnQudWlkIjoiYmVmMTQyMzUtMmU5Ny00M2Y0LWE0ODQtZGYzNjA0ZDMyNjVhIiwic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW50OmRlZmF1bHQ6c2EtcHgtYmFja3VwIn0.tvx6GQkmpriEWdUOJ1oAXWEiXP-boyazHnqPr3KTfwjDWQHwG49yyY5CChP9A2Amzjq5CVS60HGkmkcliBVpe2wNiEVtLpBj-ZyxocHcxTxUBQ\_iuYPDILT5LssmEX1k3vzD\_CT1-eW7wxduus\_cAKYVRHt6RVt\_a7VDwbv6v4gJeSX7u3kZ8bbV6opWNyUlJ05uPW0qEruJgxVQzEl4ST8g\_CHdMkBrfGuZ8hvW2hvl3Zyf61V42aroGL\_Ns0\_OJwvCbvixFxUWLjM9mxwgv4-dpNxfqbW3S9oKmF83piiY0qjuSaWCzU1oMNHj7Ze16It7hAc6-2luvCmmogJW9A

# ## 10/26/2023 Next Steps

sa-px-backup-default, px-backup-default-clusterrole, px-backup-default-rolebinding

## sa-px-backup-default.yaml

## sa-px-backup-default - PX-Backup ServiceAccount

## px-backup-default-clusterrole

## px-backup-default-rolebinding

## ks-configmap-role

## ks-configmap-rolebinding

## sa-px-backup-default-secret

## config\_sa-px-backup-default

## Add as or-cluster03-default

# svcaccount-px-backup-proc-rvw-doc-proj-02

# Logs

# Troubleshooting

# Resources

## Adding a Service Account Authentication Token to a Kubeconfig File

https://docs.oracle.com/en-us/iaas/Content/ContEng/Tasks/contengaddingserviceaccttoken.htm

## app-with-px-backup – Tom Lapp GitHub

https://github.com/tmlapp/app-with-px-backup

## Configure Service Accounts for Pods | Kubernetes

https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/#service-account-token-volume-projection

## Grant access to a namespace for non-admin user – PX-Backup

<https://docs.portworx.com/portworx-backup-on-prem/configure/namespace-access.html>

## How To Create Kubernetes Service Account For API Access

https://devopscube.com/kubernetes-api-access-service-account/

## How to regenerate Service Account tokens in Kubernetes | Support | SUSE

https://www.suse.com/support/kb/doc/?id=000020019

## How to Use ClusterRoleBinding With A ServiceAccount in All Namespaces (or a few)

<https://travis.media/clusterrolebinding-with-service-account-all-namespaces/>

## jwt - Set Expiry of Kubernetes service tokens - Stack Overflow

https://stackoverflow.com/questions/62791028/set-expiry-of-kubernetes-service-tokens

## Managing Service Accounts

https://kubernetes.io/docs/reference/access-authn-authz/service-accounts-admin/

## TokenRequest API

https://kubernetes.io/docs/reference/access-authn-authz/service-accounts-admin/#tokenrequest-api