Portworx

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

Updated: 1/23/2024

[POC Docs Overview 4](#_Toc155953148)

[Troubleshooting Overview 5](#_Toc155953149)

[Preliminary 5](#_Toc155953150)

[Concepts 6](#_Toc155953151)

[Binding 6](#_Toc155953152)

[ClusterRole 6](#_Toc155953153)

[Role 6](#_Toc155953154)

[Procedures Overview 7](#_Toc155953155)

[## overview, Design Goals 7](#_Toc155953156)

[## artifacts, resources prep 7](#_Toc155953157)

[## environment prep 7](#_Toc155953158)

[## step-by-step procedures overview – also refer to svcaccount-px-backup-internal-proc-01.txt, svcaccount-px-backup-external-proc-01.txt 7](#_Toc155953159)

[All namespaces – PX-Backup ServiceAccount, ClusterRole, ClusterRoleBinding; ConfigMap Role, RoleBinding; ServiceAccount Secret Token 8](#_Toc155953160)

[sa-px-backup-all.yaml 8](#_Toc155953161)

[sa-px-backup - PX-Backup ServiceAccount 8](#_Toc155953162)

[px-backup-all-clusterrole 8](#_Toc155953163)

[px-backup-all-clusterrolebinding 8](#_Toc155953164)

[ks-configmap-role 8](#_Toc155953165)

[ks-configmap-rolebinding 8](#_Toc155953166)

[sa-px-backup-secret 8](#_Toc155953167)

[config\_sa-px-backup - ; ServiceAccount Kubeconfig 10](#_Toc155953168)

[get service account sa-px-backup token 10](#_Toc155953169)

[get service account sa-px-backup certificate 10](#_Toc155953170)

[config\_sa-px-backup 11](#_Toc155953171)

[## 10/26/2023 Next Steps 13](#_Toc155953172)

[sa-px-backup-default.yaml 13](#_Toc155953173)

[sa-px-backup-default - PX-Backup ServiceAccount 13](#_Toc155953174)

[px-backup-default-clusterrole 13](#_Toc155953175)

[px-backup-default-rolebinding 13](#_Toc155953176)

[ks-configmap-role 13](#_Toc155953177)

[ks-configmap-rolebinding 13](#_Toc155953178)

[sa-px-backup-default-secret 13](#_Toc155953179)

[config\_sa-px-backup-default 13](#_Toc155953180)

[Add as or-cluster03-default 13](#_Toc155953181)

[svcaccount-px-backup-proc-rvw-doc-proj-02 14](#_Toc155953182)

[Logs 15](#_Toc155953183)

[Troubleshooting 16](#_Toc155953184)

[Resources 17](#_Toc155953185)

[Adding a Service Account Authentication Token to a Kubeconfig File 17](#_Toc155953186)

[app-with-px-backup – Tom Lapp GitHub 17](#_Toc155953187)

[Configure Service Accounts for Pods | Kubernetes 17](#_Toc155953188)

[Grant access to a namespace for non-admin user – PX-Backup 17](#_Toc155953189)

[How To Create Kubernetes Service Account For API Access 17](#_Toc155953190)

[How to regenerate Service Account tokens in Kubernetes | Support | SUSE 17](#_Toc155953191)

[How to Use ClusterRoleBinding With A ServiceAccount in All Namespaces (or a few) 17](#_Toc155953192)

[jwt - Set Expiry of Kubernetes service tokens - Stack Overflow 17](#_Toc155953193)

[Managing Service Accounts 17](#_Toc155953194)

[TokenRequest API 17](#_Toc155953195)

# 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

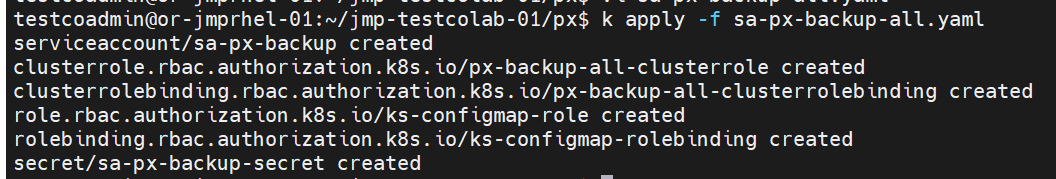
metadata:

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

## this will be inserted in config\_sa-px-backup users.name.token

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

eyJhbGciOiJSUzI1NiIsImtpZCI6IkI2cVhuM25IVnZMamlTX0hwOWRKNXR3UmhCSXRxel9uSVNSMjZITTExc28ifQ.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6InNhLXB4LWJhY2t1cC1zZWNyZXQiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoic2EtcHgtYmFja3VwIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLWFjY291bnQudWlkIjoiZmJkYTkzYWYtYzY4OS00OGIzLWI2MzUtMDhlZThlMTJkNzZjIiwic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW50OmRlZmF1bHQ6c2EtcHgtYmFja3VwIn0.JCLKk0NKOBBI9Zs7O5pnutEM8lheOxpvWS\_jBFLuVyUmyGwhMRis0PI5L1iiEk0G58gVgW3sLXLsSwMEwDarFyW68pVXgaRDbzOcS9PxX4UEkJS4u10eDRlRjYhhCiUYM-R95sYSL5GUysRdtRw13HiOJhRiAilKDoKlHZfKh9TdRROBODbCKDGdRNA8aB25AvNNpZ6Tgv7zcZOPXAd-8DJ3XX3HKypULdp09eNsdRvuTT4eqsFvIVgAfx7LFqWTHTDK7ISbXPZdlrp6xVuY7W5DjonW4CuNuVmhezW2ghkNJbN1SZ4eLQiTRORaquPHObs8\_B345LAO26cLVeS7iA

## 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://10.2.7.131:6443

name: dr-apps-01-sa-px-backup

contexts:

- context:

cluster: dr-apps-01

user: sa-px-backup

name: dr-apps-01-sa-px-backup

kind: Config

preferences: {}

users:

- name: sa-px-backup

user:

client-key-data: 

token: eyJhbGciOiJSUzI1NiIsImtpZCI6IkI2cVhuM25IVnZMamlTX0hwOWRKNXR3UmhCSXRxel9uSVNSMjZITTExc28ifQ.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6InNhLXB4LWJhY2t1cC1zZWNyZXQiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoic2EtcHgtYmFja3VwIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLWFjY291bnQudWlkIjoiZmJkYTkzYWYtYzY4OS00OGIzLWI2MzUtMDhlZThlMTJkNzZjIiwic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW50OmRlZmF1bHQ6c2EtcHgtYmFja3VwIn0.JCLKk0NKOBBI9Zs7O5pnutEM8lheOxpvWS\_jBFLuVyUmyGwhMRis0PI5L1iiEk0G58gVgW3sLXLsSwMEwDarFyW68pVXgaRDbzOcS9PxX4UEkJS4u10eDRlRjYhhCiUYM-R95sYSL5GUysRdtRw13HiOJhRiAilKDoKlHZfKh9TdRROBODbCKDGdRNA8aB25AvNNpZ6Tgv7zcZOPXAd-8DJ3XX3HKypULdp09eNsdRvuTT4eqsFvIVgAfx7LFqWTHTDK7ISbXPZdlrp6xVuY7W5DjonW4CuNuVmhezW2ghkNJbN1SZ4eLQiTRORaquPHObs8\_B345LAO26cLVeS7iA

## Copy existing admin kubeconfig to what will be svc account kubeconfig - cp config\_dr-apps-01 config\_sa-px-backup



## Copy/paste all to/from vanilla text editor with no Word Wrap

Changes to config\_sa-px-backup

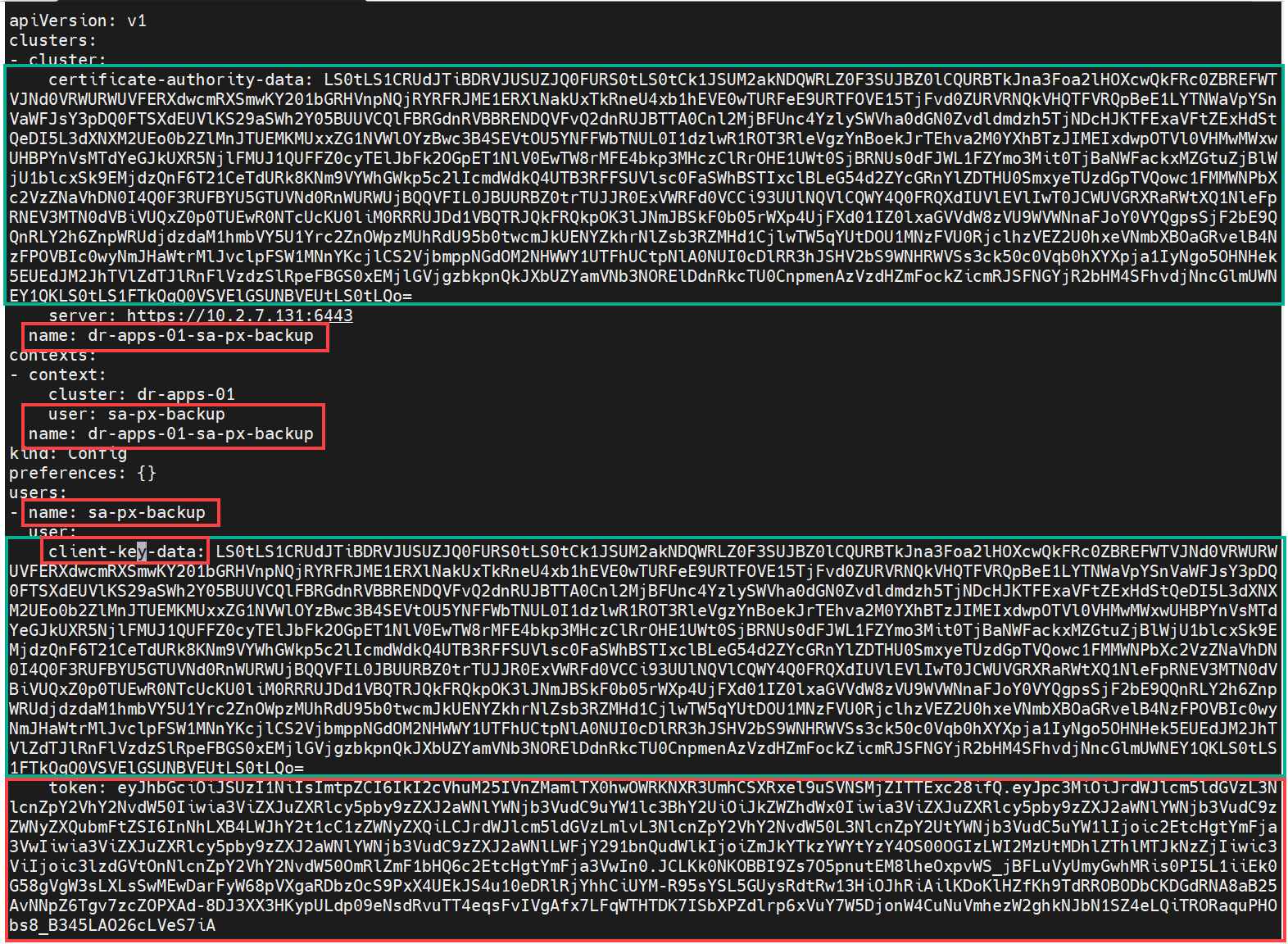
Clusters.cluster.certificate-authority-data – same as admin kubeconfig

Clusters.name append with sa-px-backup

Users.name append with sa-px-backup

Contexts.context.user = users.name

Users.user.**client.key-data** – same as admin kubeconfig



# 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