AWS Immersion Day – Data Protection Day

Portworx | AWS

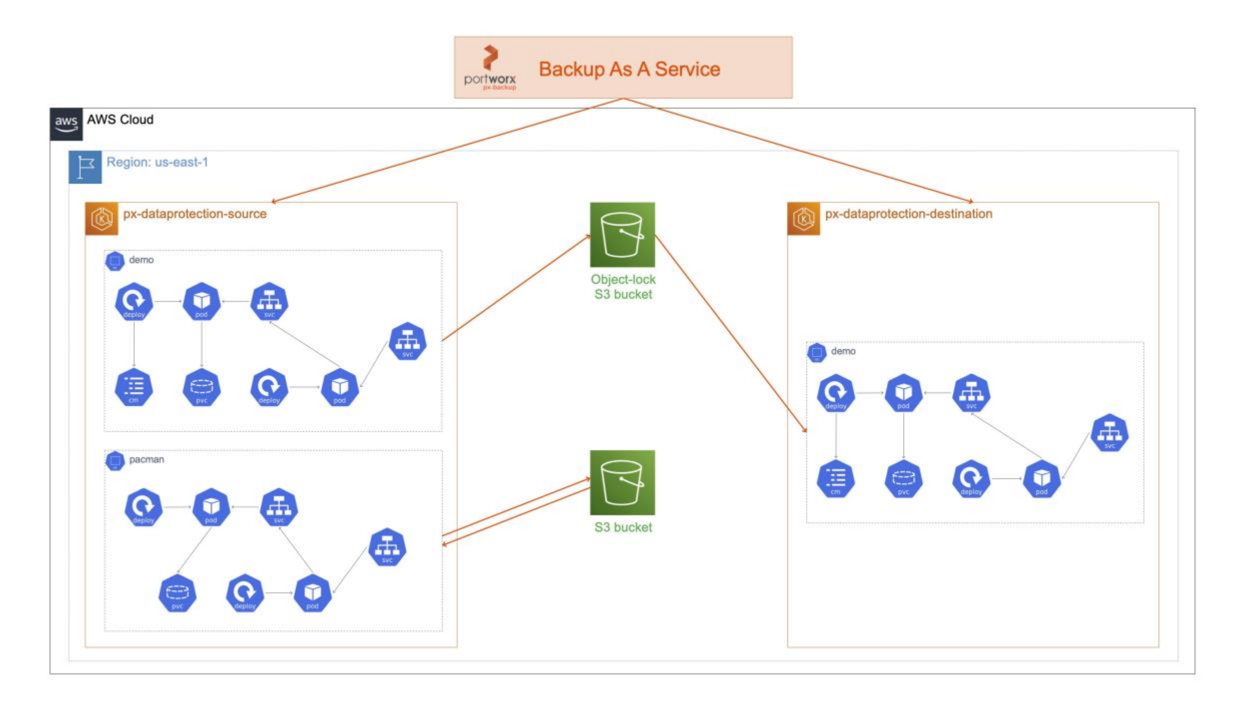
Table of Contents

Author

Bhavin Shah
Sr. Technical Marketing Manager
Portworx by Pure Storage

Lab Overview

This lab guide is built for the Kubernetes Data Protection Day ran by Portworx and AWS, to help users get hands-on experience with an industry leading Kubernetes data protection solution. As part of this lab, users will use an AWS Event Engine AWS account. As part of this lab, we will go through and deploy a couple of Amazon EKS clusters, S3 buckets, containerized applications on the Amazon EKS cluster and also create a sandbox trial account for the Portworx Backup As A Service (BaaS) solution. The applications used in this lab are stateful applications using MongoDB and PostgreSQL as the backend databases respectively. As part of the lab, we will create backup jobs and restore these applications to the same Amazon EKS cluster or a different Amazon EKS cluster using object local enabled backup bucket, to simulate scenarios like accidental deletions and ransomware attacks respectively.

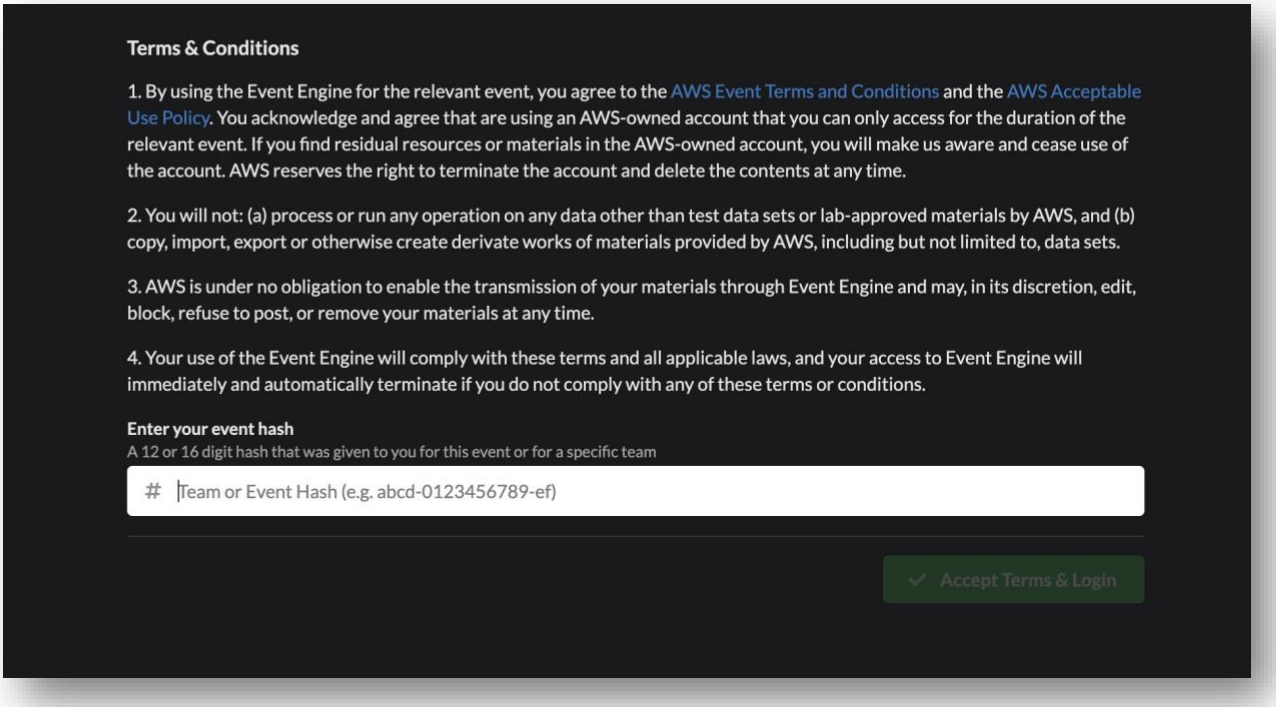


Lab Setup

Accessing AWS Account

1. Navigate to the event engine platform using the link (https://dashboard.eventengine.run/login) and enter your 12- or 16-digit event hash.

Note: Use an incognito window to ensure that you aren't using your existing AWS account for this lab.



Terms & Conditions

1. By using the Event Engine for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.

2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivate works of materials provided by AWS, including but not limited to, data sets.

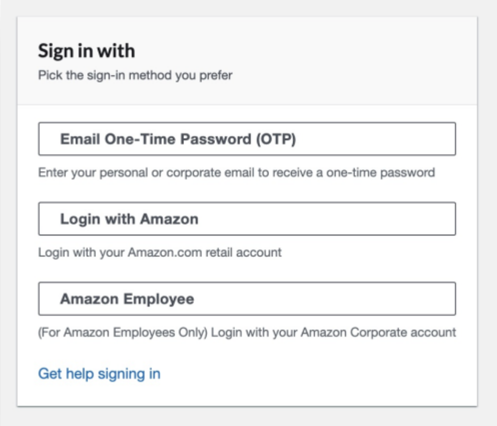
3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.

4. Your use of the Event Engine will comply with these terms and all applicable laws, and your access to Event Engine will immediately and automatically terminate if you do not comply with any of these terms or conditions.

Enter your event hash

A 12 or 16 digit hash that was given to you for this event or for a specific team

2. After entering your event hash, click *"Accept Terms & Login"*.
3. Next, click on *"Email One-Time Password (OTP)"* and enter your email address and hit *"Send Passcode"* to receive the OTP.



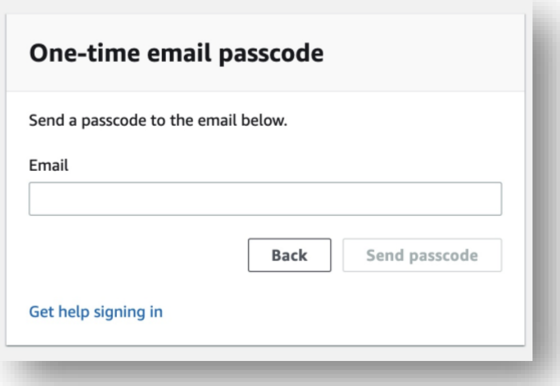
Sign in with

Pick the sign-in method you prefer

Enter your personal or corporate email to receive a one-time password

Login with your Amazon.com retail account

(For Amazon Employees Only) Login with your Amazon Corporate account



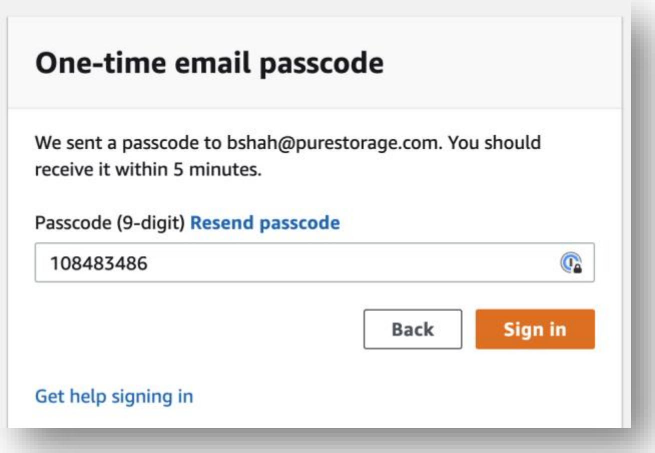
One-time email passcode

Send a passcode to the email below.

Email

4. Check your email for the OTP. Copy the passcode and enter it in the Event Engine platform and hit *"Sign In"*.

At this point, you have an AWS account that can be used for this Immersion Day workshop.



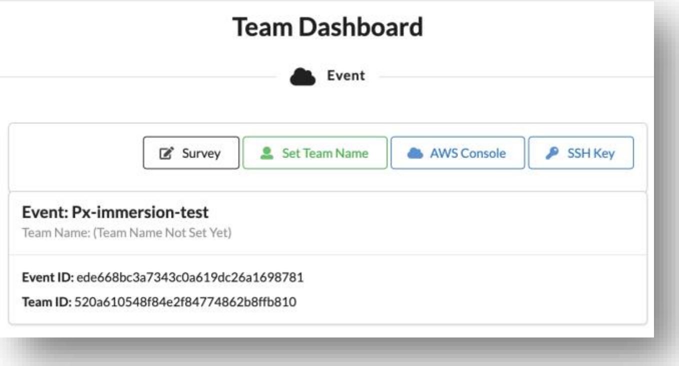
One-time email passcode

We sent a passcode to bshah@purestorage.com. You should receive it within 5 minutes.

Passcode (9-digit) Resend passcode

108483486

5. Next, from the event engine dashboard, click on *"AWS Console"*.



Team Dashboard

Event

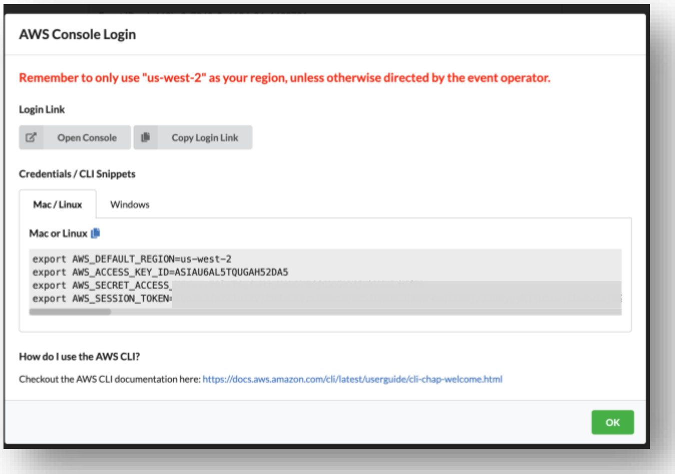
Event: Px-immersion-test

Team Name: (Team Name Not Set Yet)

Event ID: ede668bc3a7343c0a619dc26a1698781

Team ID: 520a610548f84e2f84774862b8ffb810

6. Next, click on Open Console to access the AWS Management console.



AWS Console Login

Remember to only use "us-west-2" as your region, unless otherwise directed by the event operator.

Login Link

Credentials / CLI Snippets

Mac or Linux

```
export AWS_DEFAULT_REGION=us-west-2
export AWS_ACCESS_KEY_ID=ASIAU6AL5TQUGAH52DA5
export AWS_SECRET_ACCESS_
export AWS_SESSION_TOKEN=[redacted]
```

How do I use the AWS CLI?

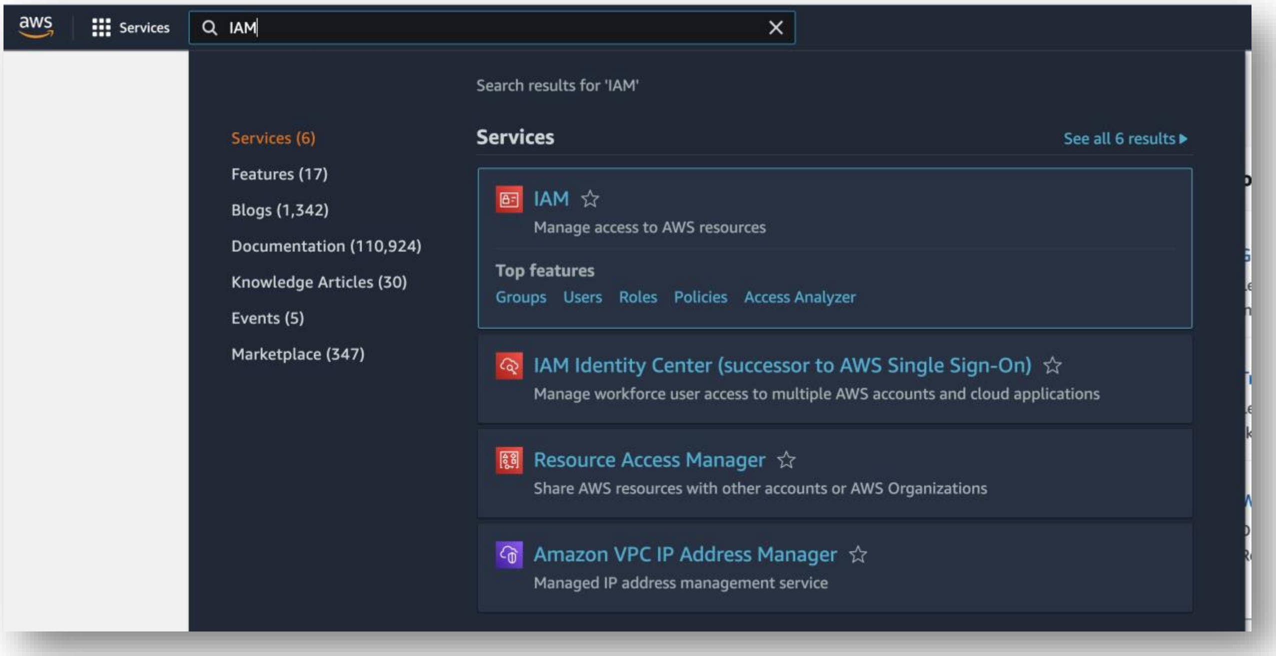
Checkout the AWS CLI documentation here: https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html

At this point, you have an AWS account that can be used for this Immersion Day workshop.

Create AWS IAM User

Once you have access to your AWS account using the Event Engine platform, we will go ahead and create an IAM user called *“workshop”*, whose credentials will be used to deploy Amazon EKS clusters and S3 buckets needed for the workshop.

1. From the AWS Console, navigate to Services → IAM.



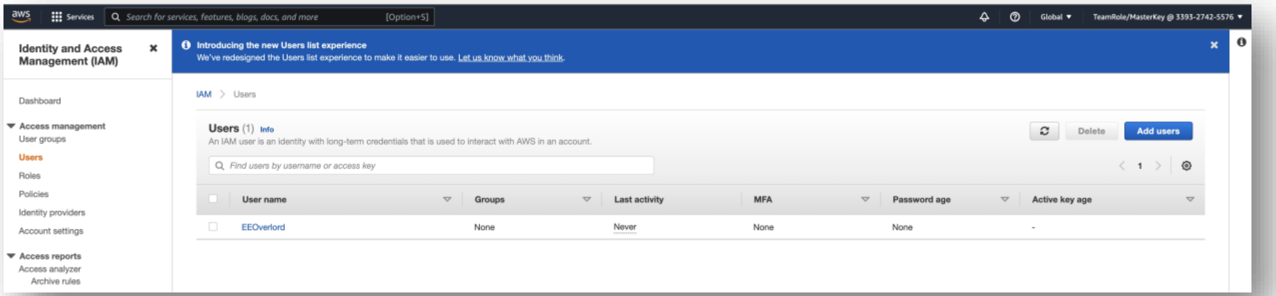
Manage access to AWS resources

Manage workforce user access to multiple AWS accounts and cloud applications

Share AWS resources with other accounts or AWS Organizations

Managed IP address management service

2. Click on Users in the left pane and click *“Add Users”*.

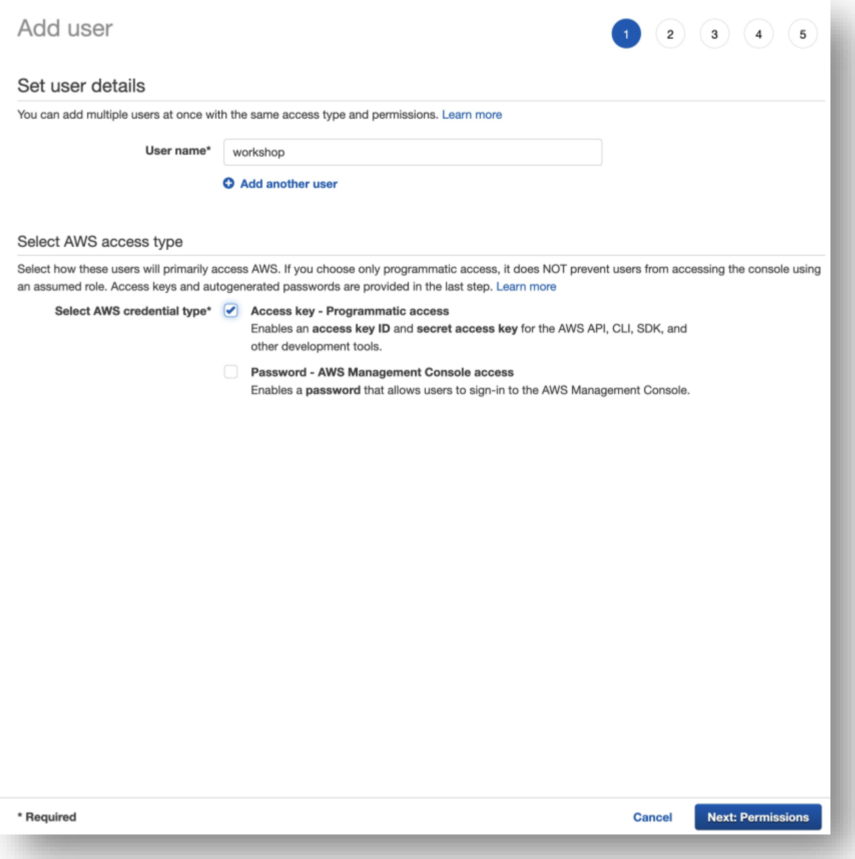


Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

	User name	Groups	Last activity	MFA	Password age	Active key age
□	EEOverlord	None	Never	None	None	-

3. Enter *“workshop”* as the user name, select the *“Access Key – Programmatic Access”* checkbox, and click *“Next: Permissions”*.



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* workshop

Select AWS access type

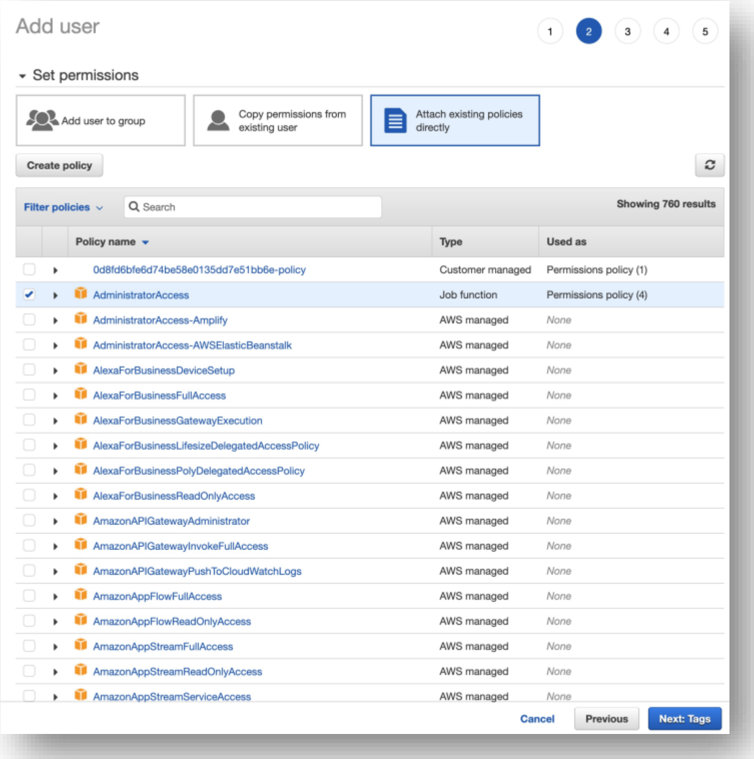
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type* ☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

4. Select *“Attach existing policies directly”* and select *“AdministratorAccess”* in the list of policies and click *“Next: Tags”*.



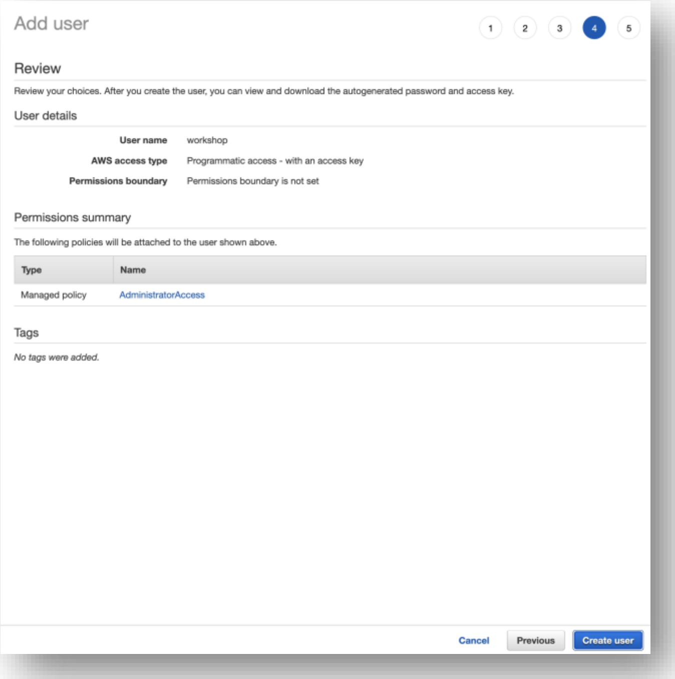
Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies
Search

Showing 760 results

	Policy name	Type	Used as
□	0d8fd6bfe6d74be58e0135dd7e51bb6e-policy	Customer managed	Permissions policy (1)
☑	AdministratorAccess	Job function	Permissions policy (4)
□	AdministratorAccess-Amplify	AWS managed	None
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
□	AlexaForBusinessDeviceSetup	AWS managed	None
□	AlexaForBusinessFullAccess	AWS managed	None
□	AlexaForBusinessGatewayExecution	AWS managed	None
□	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
□	AlexaForBusinessReadOnlyAccess	AWS managed	None
□	AmazonAPIGatewayAdministrator	AWS managed	None
□	AmazonAPIGatewayInvokeFullAccess	AWS managed	None
□	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None
□	AmazonAppFlowFullAccess	AWS managed	None
□	AmazonAppFlowReadOnlyAccess	AWS managed	None
□	AmazonAppStreamFullAccess	AWS managed	None
□	AmazonAppStreamReadOnlyAccess	AWS managed	None
□	AmazonAppStreamServiceAccess	AWS managed	None

5. We won’t assign any tags for this workshop, so click *“Next: Review”*.
6. Verify that the user name, AWS access type and permission boundary matches the screenshot below and click *“Create user”*.



Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name workshop

AWS access type Programmatic access - with an access key

Permissions boundary Permissions boundary is not set

Permissions summary

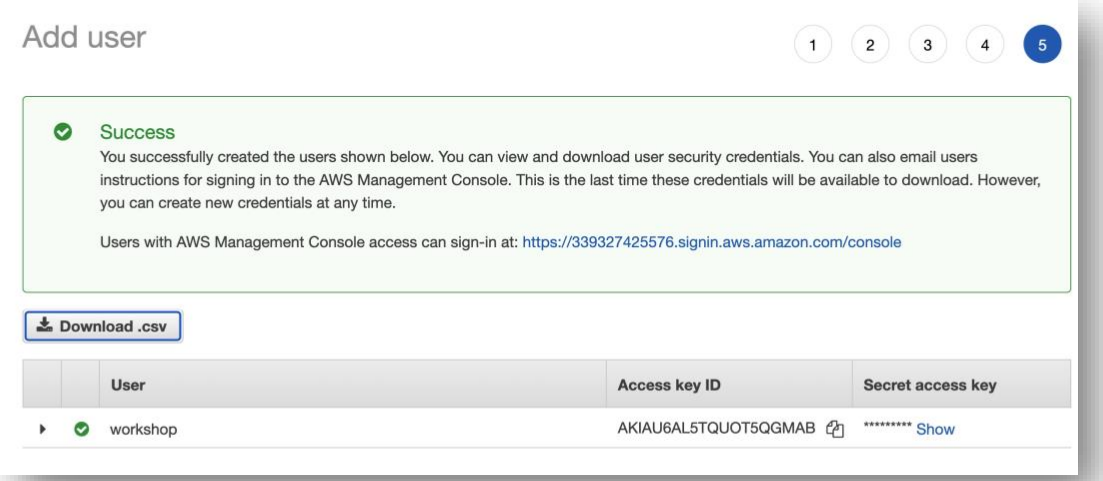
The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess

Tags

No tags were added.

7. **Copy the Access Key ID and Secret Access Key locally and download the csv file.**



Add user

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://339327425576.signin.aws.amazon.com/console

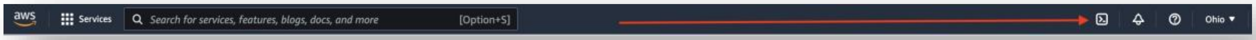
		User	Access key ID	Secret access key
▸	✓	workshop	AKIAU6AL5TQUOT5QGMAB	********* Show

8. Once you have saved your Access Key ID and Secret Access Key, hit Close.

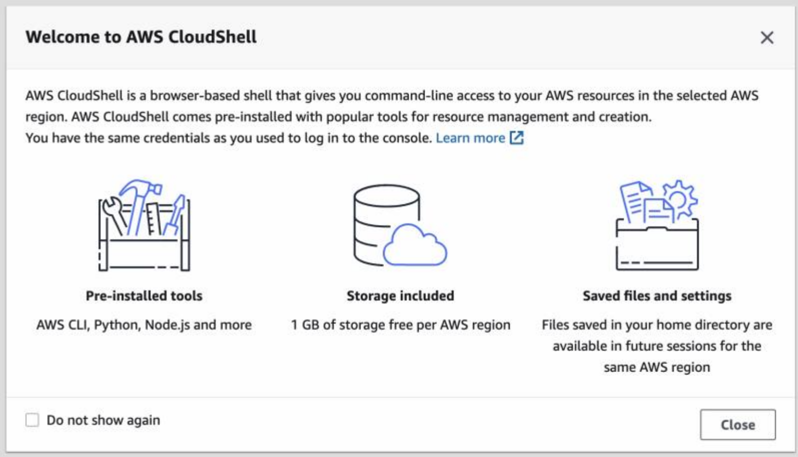
Deploying AWS Resources

Once you have created a new IAM user (workshop), let's navigate to the AWS console and use the steps below to complete the pre-reqs for the lab:

1. Open an AWS CloudShell session from the top right of the AWS management console or, you can also search for CloudShell in the main search box on the left.



2. Read through the Welcome to AWS CloudShell box and click close.



Welcome to AWS CloudShell

AWS CloudShell is a browser-based shell that gives you command-line access to your AWS resources in the selected AWS region. AWS CloudShell comes pre-installed with popular tools for resource management and creation. You have the same credentials as you used to log in to the console. Learn more

Pre-installed tools

AWS CLI, Python, Node.js and more

Storage included

1 GB of storage free per AWS region

Saved files and settings

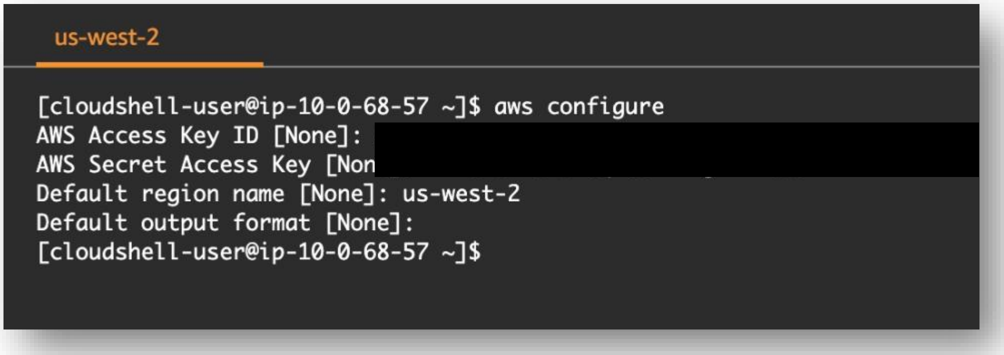
Files saved in your home directory are available in future sessions for the same AWS region

□ Do not show again

Note: It takes a couple of minutes for the CloudShell session to become responsive.

3. Next, use the following command to configure your AWS credentials using the AWS user **(workshop)** that you created in the previous step. Enter us-west-2 as the default region.

```
aws configure
```



```
[cloudshell-user@ip-10-0-68-57 ~]$ aws configure
AWS Access Key ID [None]: [redacted]
AWS Secret Access Key [Non
Default region name [None]: us-west-2
Default output format [None]:
[cloudshell-user@ip-10-0-68-57 ~]$
```

4. Clone the PX-DataProtection repository on to your CloudShell session using the following command:

```
git clone https://github.com/bhavin04890/PX-DataProtection.git
```

5. Once you have the repo cloned, we will go ahead and change directories and update the permissions on a few files.

```
cd PX-DataProtection

chmod 755 pre-req.sh cleanup.sh deletepacman.sh encryptlogo.sh
chmod 755 connect-source-eks.sh connect-destination-eks.sh
```

6. Next, let's run the pre-req.sh file, which will deploy the source and destination Amazon EKS clusters, applications that we need for the lab and an S3 bucket to use for storing our application snapshots.

```
./pre-req.sh
```

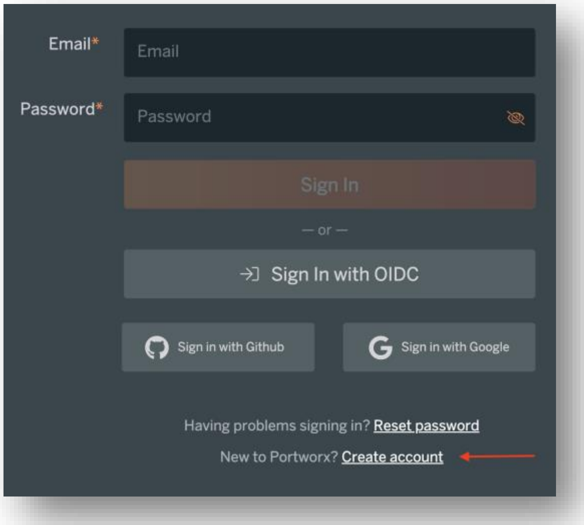
7. Enter a unique name for your S3 bucket when the script prompts you to. Remember this name as we will use it later in the guide!

While we wait for these resources to be deployed, we can proceed and create our BaaS accounts, to complete the pre-req steps.

Create Backup As A Service account

1. Navigate to Portworx Central (https://central.portworx.com/) and create a new account.

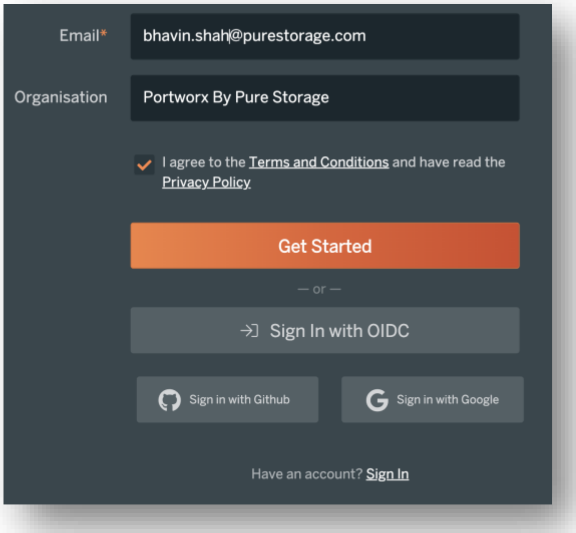
Note: Skip this to Step 6 if you already have a Portworx Central account.



Having problems signing in? Reset password

New to Portworx? Create account

2. Enter your email address and name of your organization.



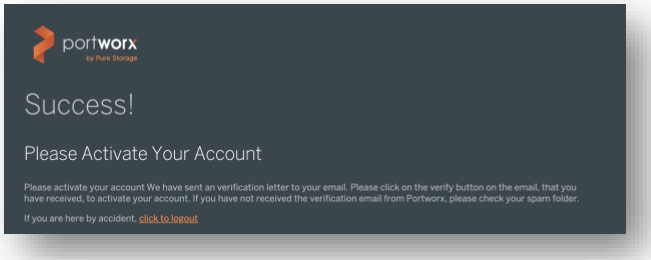
Email* bhavin.shah@purestorage.com

Organisation Portworx By Pure Storage

☑ I agree to the Terms and Conditions and have read the Privacy Policy

Have an account? Sign In

3. Activate your account by clicking the link in the email.



Success!

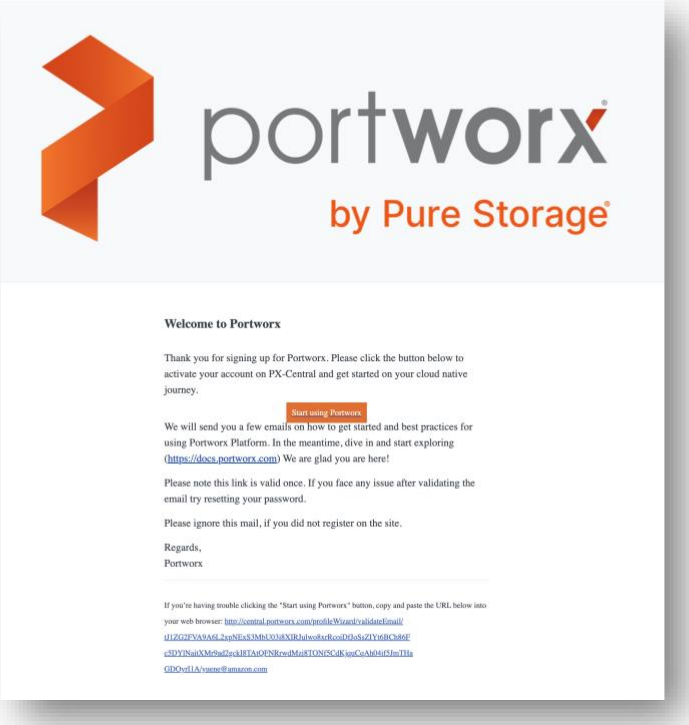
Please Activate Your Account

Please activate your account We have sent an verification letter to your email. Please click on the verify button on the email, that you have received, to activate your account. If you have not received the verification email from Portworx, please check your spam folder.

If you are here by accident, click to logout

4. Check your email and verify your account by clicking *"Start using Portworx"*.

Note: It might take a couple of minutes to get the email.



Welcome to Portworx

Thank you for signing up for Portworx. Please click the button below to activate your account on PX-Central and get started on your cloud native journey.

Start using Portworx

We will send you a few emails on how to get started and best practices for using Portworx Platform. In the meantime, dive in and start exploring (https://docs.portworx.com) We are glad you are here!

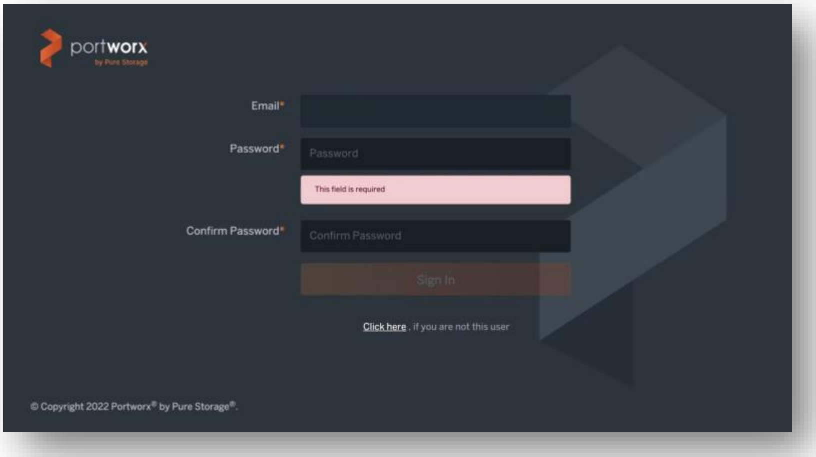
Please note this link is valid once. If you face any issue after validating the email try resetting your password.

Please ignore this mail, if you did not register on the site.

Regards,
Portworx

If you're having trouble clicking the "Start using Portworx" button, copy and paste the URL below into your web browser: http://central.portworx.com/profileWizard/validateEmail/tJ1ZG2FVA9A6L2xpNExS3MbU03i8XIRJulwo8xrRcoiDf3oSsZIYt6BCb86Fc5DYINaitXMr9ad2gckl8TAtQFNRrwdMzi8TONf5CdKjgjCqAh04if5JmTHaGDOyrl1A/yuene@amazon.com

5. Set a new password for Portworx Central and click *"Sign In"*.



Email*

Password* Password

This field is required

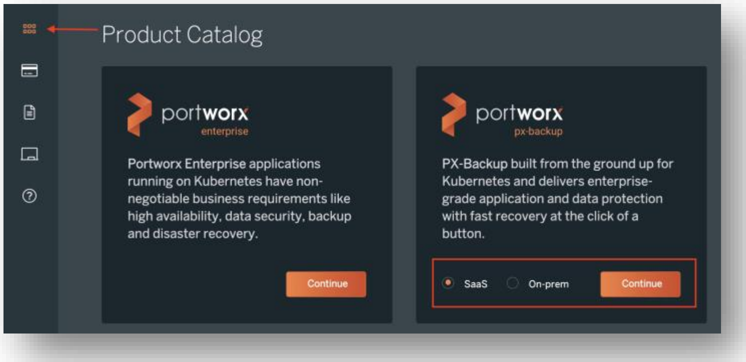
Confirm Password* Confirm Password

Sign In

Click here , if you are not this user

© Copyright 2022 Portworx® by Pure Storage®.

6. Navigate to the *"Product Catalog"* tab on the left pane and select Portworx PX-Backup – SaaS option and click *"Continue"*.



Product Catalog

portworx enterprise

Portworx Enterprise applications running on Kubernetes have non-negotiable business requirements like high availability, data security, backup and disaster recovery.

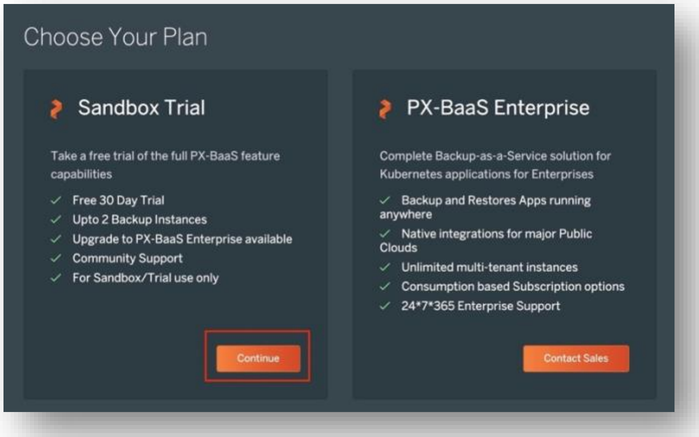
Continue

portworx px-backup

PX-Backup built from the ground up for Kubernetes and delivers enterprise-grade application and data protection with fast recovery at the click of a button.

● SaaS ○ On-prem Continue

7. Select the "Sandbox Trial" and click Continue.



Choose Your Plan

Sandbox Trial

Take a free trial of the full PX-BaaS feature capabilities

- ✓ Free 30 Day Trial
- ✓ Upto 2 Backup Instances
- ✓ Upgrade to PX-BaaS Enterprise available
- ✓ Community Support
- ✓ For Sandbox/Trial use only

Continue

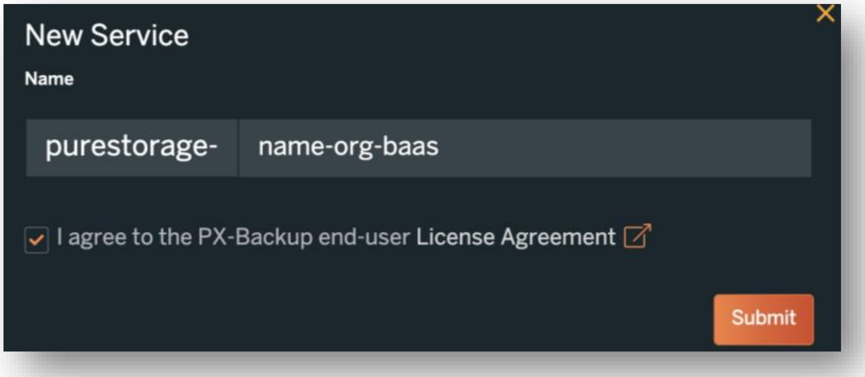
PX-BaaS Enterprise

Complete Backup-as-a-Service solution for Kubernetes applications for Enterprises

- ✓ Backup and Restores Apps running anywhere
- ✓ Native integrations for major Public Clouds
- ✓ Unlimited multi-tenant instances
- ✓ Consumption based Subscription options
- ✓ 24*7*365 Enterprise Support

Contact Sales

8. Enter a name for your service. Ideally use "name-organization-baas", check the box for EULA and hit *"Submit"*.



New Service

Name

purestorage- name-org-baas

☑ I agree to the PX-Backup end-user License Agreement

Submit

At this point, the pre-requisites for the AWS Immersion Day are done, and we will proceed to the slides portion and then come back for the hands-on lab again.

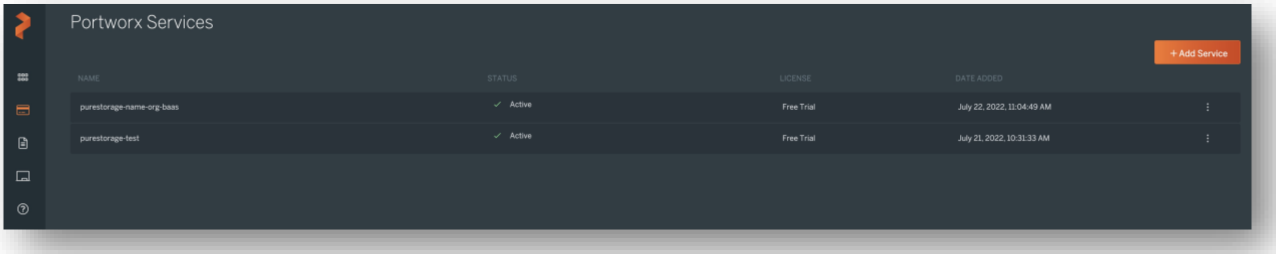
Portworx Backup As A Service (BaaS) overview

Portworx BaaS allows users to leverage a managed Kubernetes data protection tool to protect their containerized applications running on Amazon EKS clusters. As part of this section, we will go ahead and add our cloud accounts, backup targets, auto-discover Amazon EKS clusters.

Configure cloud credentials

Credentials allow BaaS to authenticate with clusters for the purpose of taking backups and restoring to them, as well as with backup locations where backup objects are stored. To add cloud credentials, use the following steps:

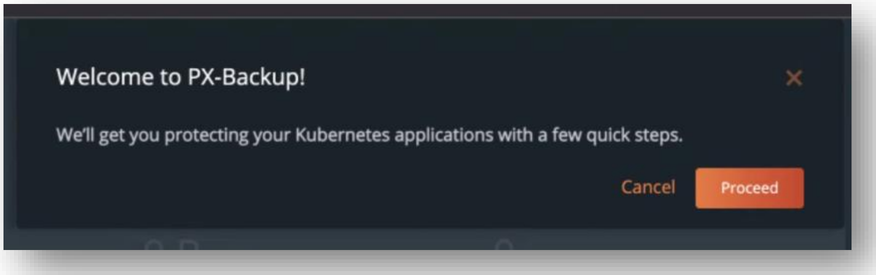
1. Log into Portworx Central (https://central.portworx.com/) and navigate to your BaaS instance.



Portworx Services

NAME	STATUS	LICENSE	DATE ADDED
purestorage-name-org-baas	✓ Active	Free Trial	July 22, 2022, 11:04:49 AM
purestorage-test	✓ Active	Free Trial	July 21, 2022, 10:31:33 AM

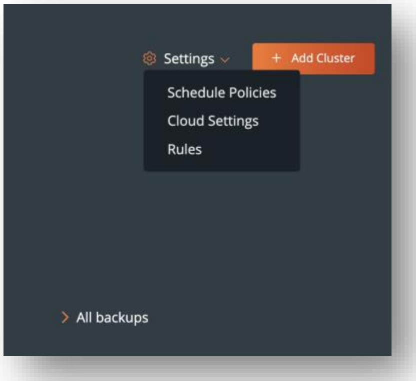
Note: Cancel and close out any tool tip suggestions from the BaaS Interface, like the screenshot below:



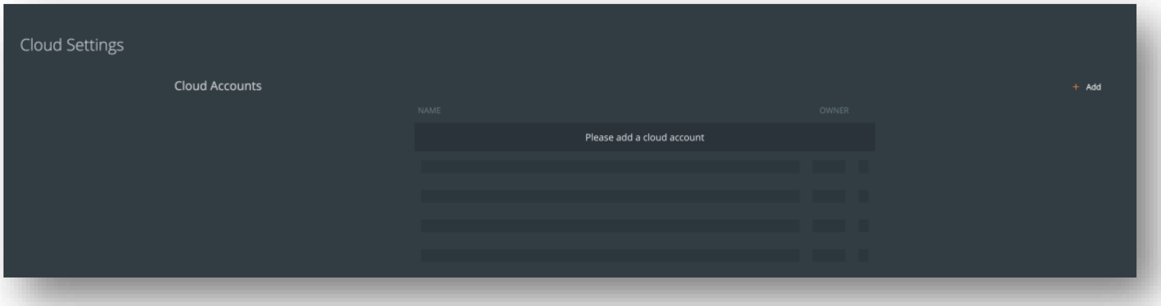
Welcome to PX-Backup!

We'll get you protecting your Kubernetes applications with a few quick steps.

2. From the dashboard, click on **"Settings"** on the top right, and click **"Cloud Settings".**

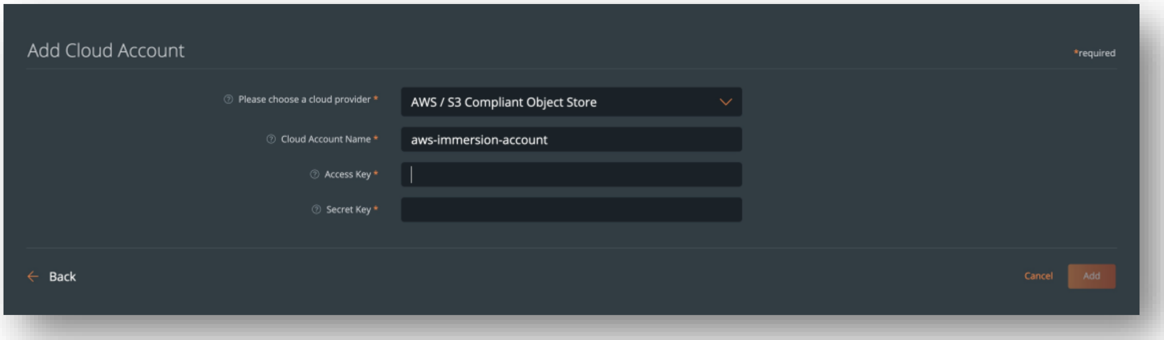


3. Click on **“+ Add”** on the right to add a Cloud Account.



Please add a cloud account

4. Select *“AWS / S3 Compliant Object Store”* as the Cloud Provider and give a name **(aws-immersion-account)** for to the cloud account. This name is just used for managing credentials inside BaaS.



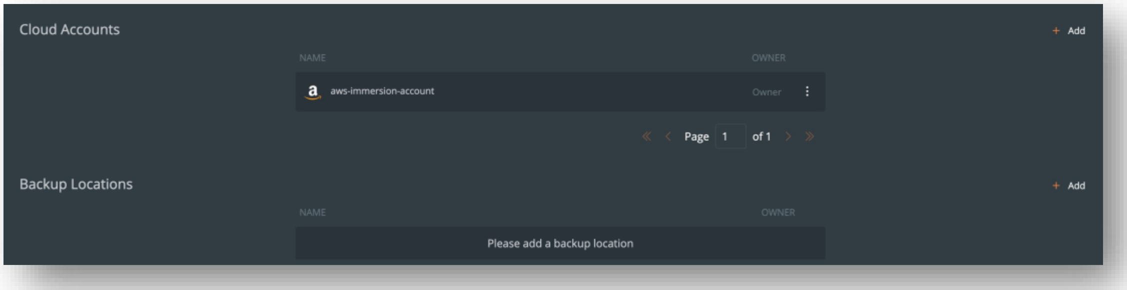
Please choose a cloud provider *: AWS / S3 Compliant Object Store

Cloud Account Name *: aws-immersion-account

Access Key *:

Secret Key *:

5. Enter the Access Key and Secret Key for the AWS IAM user **(workshop)** and click Add. Once complete, you should see your account listed under Cloud Accounts.

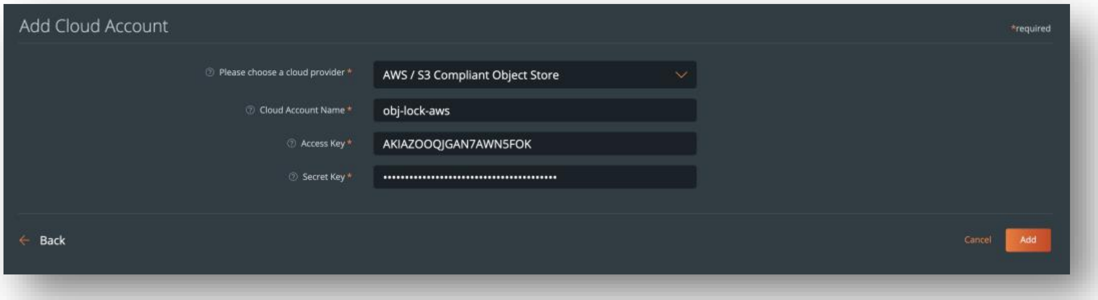


NAME	OWNER
aws-immersion-account	Owner

Please add a backup location

6. Repeat steps 3-5 above, to add another cloud account **(obj-lock-aws)**. This second cloud account will be used to store immutable application snapshots in an object lock enabled S3 bucket. Use the following credentials to access add the cloud account.

```
Access Key ID: AKIAZOOQJGAN7AWN5FOK
Secret Access key: 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
```



Add Cloud Account

*required

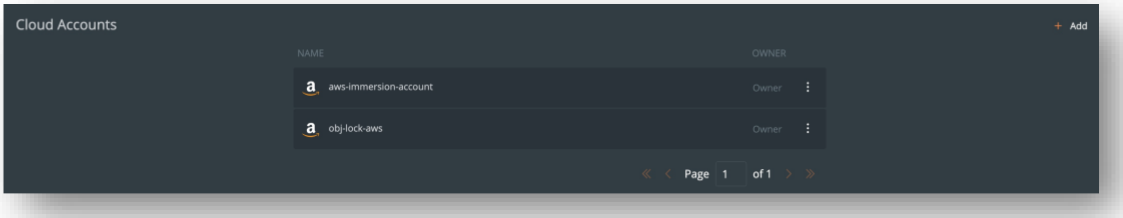
Please choose a cloud provider * AWS / S3 Compliant Object Store

Cloud Account Name * obj-lock-aws

Access Key * AKIAZOOQJGAN7AWN5FOK

Secret Key * ••

7. At this point, you have two AWS Cloud Accounts:
    a. aws-immersion-account: Used to add Amazon EKS clusters and non-object lock enabled backup repository
    b. obj-lock-aws: Used to add object lock enabled S3-bucket as the backup repository.



Cloud Accounts

NAME	OWNER
aws-immersion-account	Owner
obj-lock-aws	Owner

Adding Backup targets

Backup locations are S3-compatible object storage bucket locations that can be added to BaaS and used to store end-to-end application snapshots of your containerized applications running on Amazon EKS.

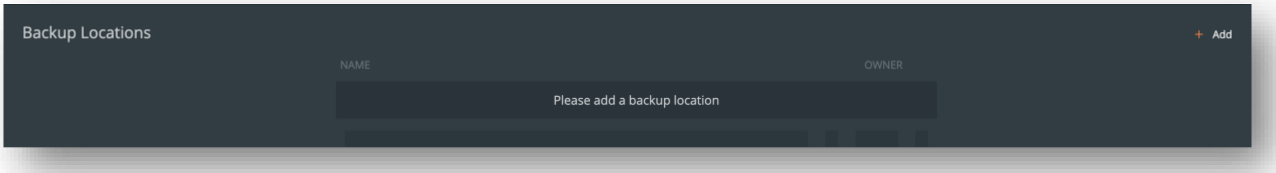
There are two type of backup targets / locations.

1. **Object Lock enabled backup location** – These backup locations can be used to store Write Once Read Many (WORM) snapshot copies. Since, any backup snapshots stored in these backup buckets are immutable, they help organizations protect and recover from Ransomware attacks. During a Ransomware attack, hackers will try to manipulate your backup snapshots. So, having an immutable backup snapshot, allows organizations to always have a golden copy of their application stored in a backup repository that can be used to recover applications to new Amazon EKS clusters.
2. **non-Object lock enabled backup locations** – These are standard backup locations that allow users to configure custom retention periods for their backup snapshots using BaaS. These backup locations can help organizations protect their applications from accidental corruption or data loss issues and allows them to restore applications quickly from a snapshot.

Organizations can typically choose to build a custom backup policy, where they can have an hourly backup, storing snapshots in a non-object lock enabled bucket with custom retention period, and maybe use the object-lock enabled bucket to store daily application snapshots

The steps to add an object lock enabled and a non-object lock enabled bucket to BaaS instance are the same. To add backup targets to your BaaS instance, use the following steps:

1. Click on “+ Add” on the Backup Locations section.



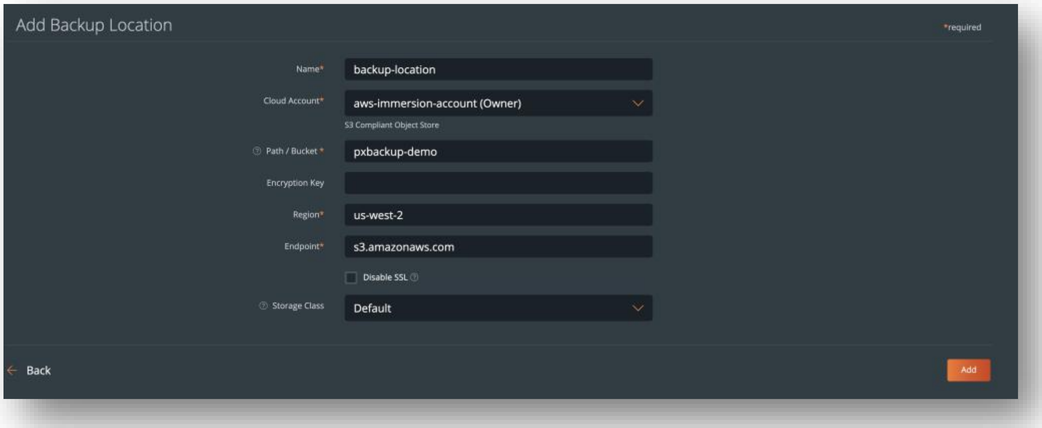
Backup Locations

Please add a backup location

2. Enter a name for the backup location, select the Cloud Account (aws-immersion-account) that we added in the previous step, enter the name of the bucket, and the region where the bucket is available.
    a. **Name:** backup-location
    b. **Cloud Account:** aws-immersion-account (Owner)
    c. **Path / Bucket:** <<name of the bucket your created as part of pre-req>>

Note: To get the name of your S3 bucket, go to AWS CloudShell and use the cmd *“aws s3 ls”*

    d. **Region:** us-west-2
    e. **Endpoint:** s3.amazonaws.com
    f. **Storage Class:** Default



Add Backup Location

*required

Name* backup-location

Cloud Account* aws-immersion-account (Owner)

S3 Compliant Object Store

Path / Bucket * pxbackup-demo

Encryption Key

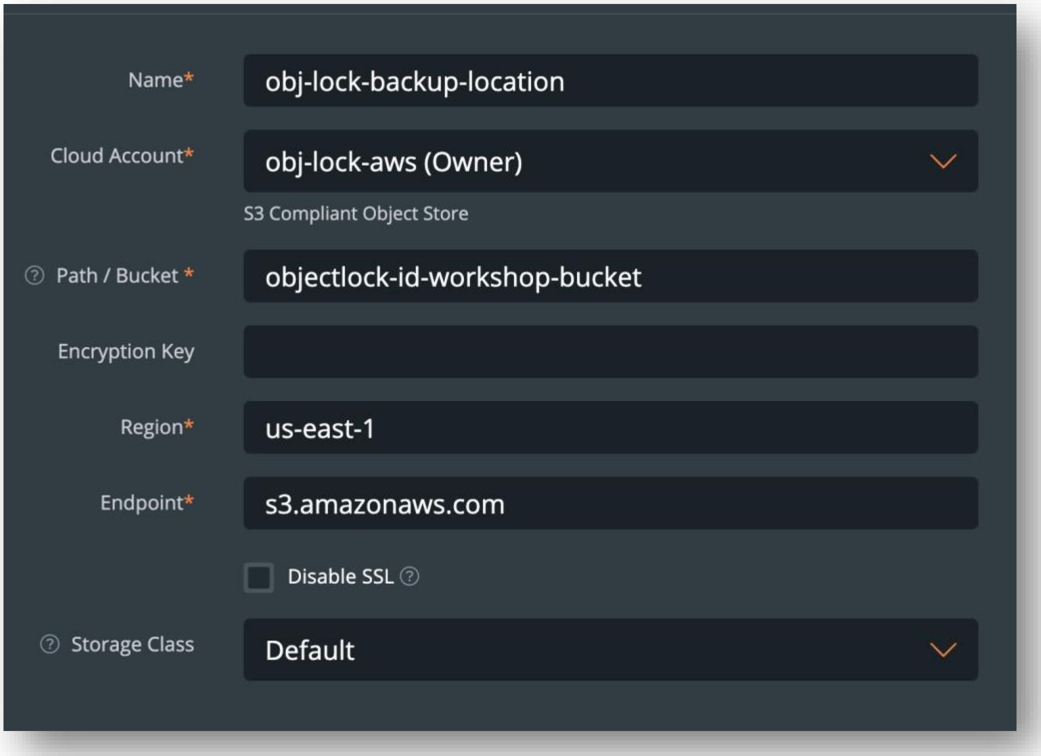
Region* us-west-2

Endpoint* s3.amazonaws.com

□ Disable SSL

Storage Class Default

3. Click **Add** to add the backup location.
4. Repeat steps 2-4 to add another backup location. This time we will add the object lock enabled S3-bucket (name: objectlock-id-workshop-bucket) using the second cloud account (obj-lock-aws).
    a. **Name:** obj-lock-backup-location
    b. **Cloud Account:** obj-lock-aws (Owner)
    c. **Path / Bucket:** objectlock-id-workshop-bucket
    d. **Region:** us-east-1
    e. **Endpoint:** s3.amazonaws.com
    f. **Storage Class:** Default



Name* obj-lock-backup-location

Cloud Account* obj-lock-aws (Owner)

S3 Compliant Object Store

Path / Bucket * objectlock-id-workshop-bucket

Encryption Key

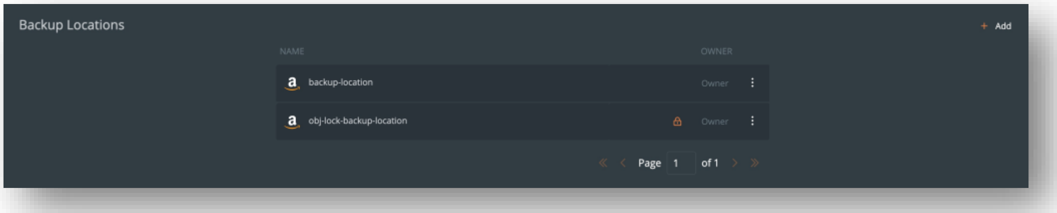
Region* us-east-1

Endpoint* s3.amazonaws.com

□ Disable SSL

Storage Class Default

5. Once the backup location has been added, you can look at all the available backup locations from the Cloud Settings page. The object lock backup location will be listed with the lock icon on the right. This helps users differentiate between the two types of backup targets supported by BaaS.



Backup Locations

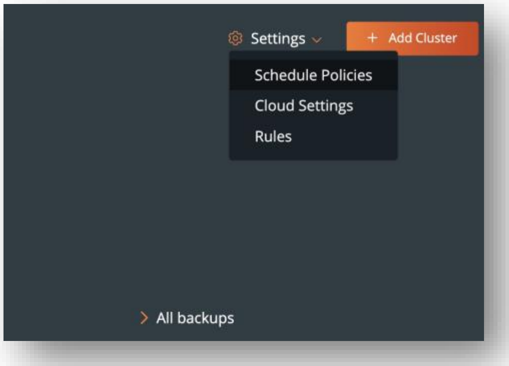
NAME		OWNER
backup-location		Owner
obj-lock-backup-location	🔒	Owner

Schedule Policies

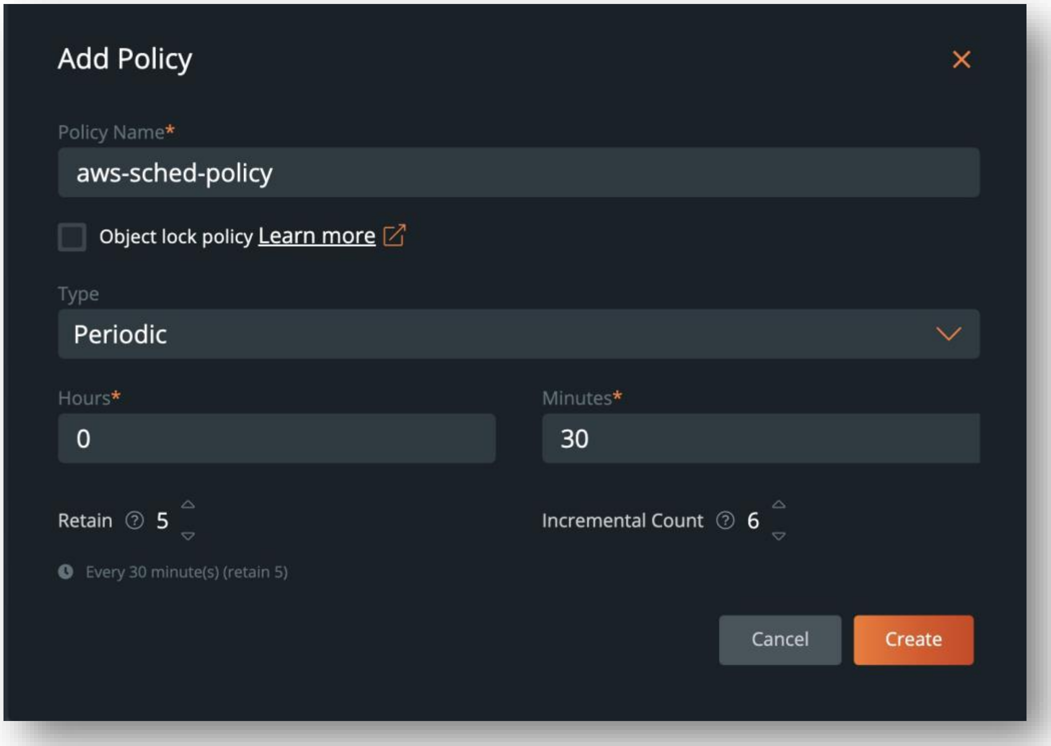
```
Portworx BaaS allows users to set their own schedule policies that can be used
when creating backup jobs. BaaS allows users to either create ad-hoc, manual,
one-time backup to create backup jobs that get triggered at a regular schedule.
Using Schedule policies, users can control when they want to trigger backup
jobs. These can be periodic, hourly, daily, weekly, and monthly policies.
```

Use the following steps to create a 30-min backup policy that we will use to create backup jobs:

1. Navigate to the dashboard and click on the *"Settings"* and *"Schedule Policies"* on the top right.



2. Click the *"+"* sign on the top right to add a new Schedule policy.
3. Give the schedule policy a name. If you are going to use this policy to create object-lock enabled backup jobs, then select the object lock policy checkbox. If you check the box, BaaS won't allow you to configure your own backup retention period but defer to the S3-bucket's retention setting.
    a. **Policy Name:** aws-sched-policy
    b. **Type:** Periodic
    c. **Hours:** 0
    d. **Minutes:** 30


Add Policy

Policy Name*
aws-sched-policy

□ Object lock policy Learn more

Type
Periodic

Hours*
0

Minutes*
30

Retain 5

Incremental Count 6

Every 30 minute(s) (retain 5)

4. Click Create to create the Schedule policy.

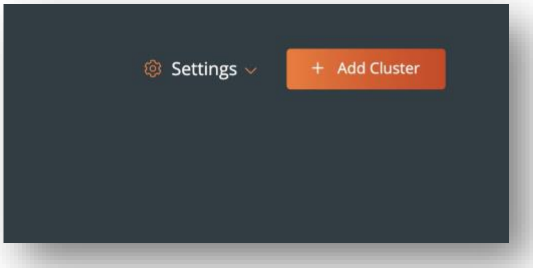
You can create more schedule policies that fit your specific application-level SLAs.

Auto-discover Amazon EKS cluster

> BaaS allows users to auto-discover their Amazon EKS clusters, rather than copy and pasting kubeconfig files between the EKS cluster and the BaaS interface. This allows users to leverage their cloud credentials to access their Amazon EKS cluster, such that BaaS can inventory the cluster for applications, and help users create backup jobs quickly. This also avoids a scenario where the kubeconfig based credentials expire and your scheduled backup jobs start failing.

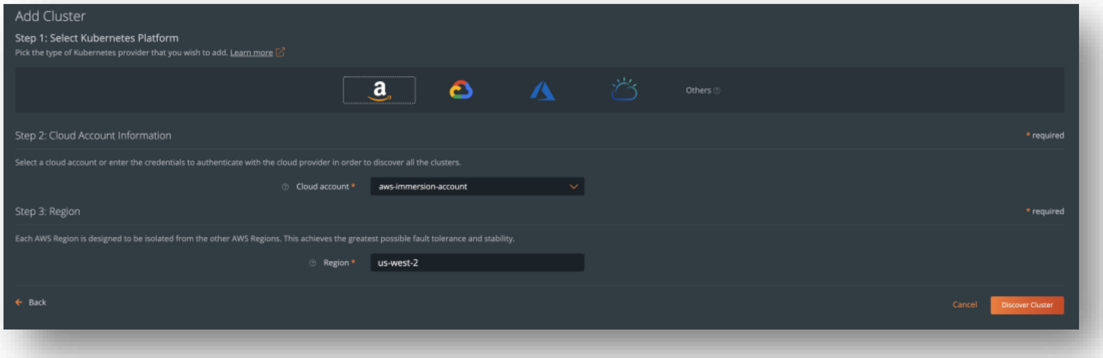
To auto-discover your Amazon EKS clusters, use the following steps:

1. Navigate to the dashboard and click on *"+ Add Cluster"* on the top right of your screen.



2. Select the Cloud Account we created earlier in the lab from the Cloud Account (aws-immersion-account) drop down box and enter the region (us-west-2) where your Amazon EKS cluster is running and click *"Discover Cluster".*

Note: If the cloud account list isn't loading, refresh the webpage.


Add Cluster

Step 1: Select Kubernetes Platform

Pick the type of Kubernetes provider that you wish to add. Learn more

Step 2: Cloud Account Information

Select a cloud account or enter the credentials to authenticate with the cloud provider in order to discover all the clusters.

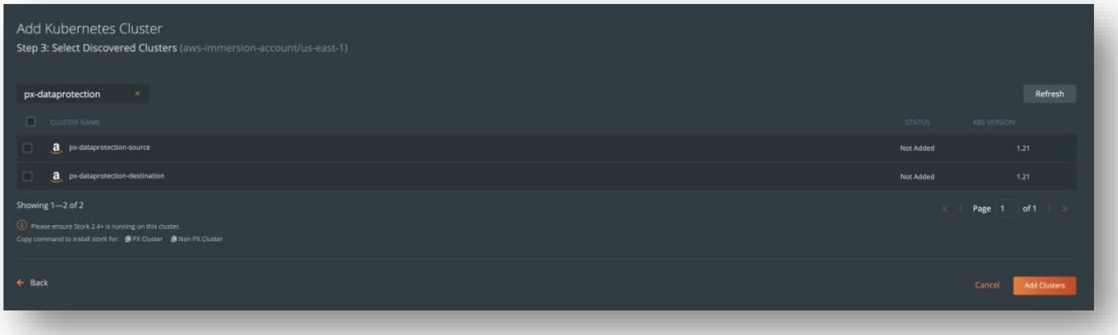
Cloud account * aws-immersion-account

Step 3: Region

Each AWS Region is designed to be isolated from the other AWS Regions. This achieves the greatest possible fault tolerance and stability.

Region * us-west-2

3. Next, you will be shown a list of Amazon EKS clusters that you have access to. Select the clusters deployed as part of the pre-req (px-dataprotection-source and px-dataprotection-destination) and click *"Add Clusters".*



Add Kubernetes Cluster

Step 3: Select Discovered Clusters (aws-immersion-account/us-east-1)

px-dataprotection ×

□	CLUSTER NAME	STATUS	K8S VERSION
□	px-dataprotection-source	Not Added	1.21
□	px-dataprotection-destination	Not Added	1.21

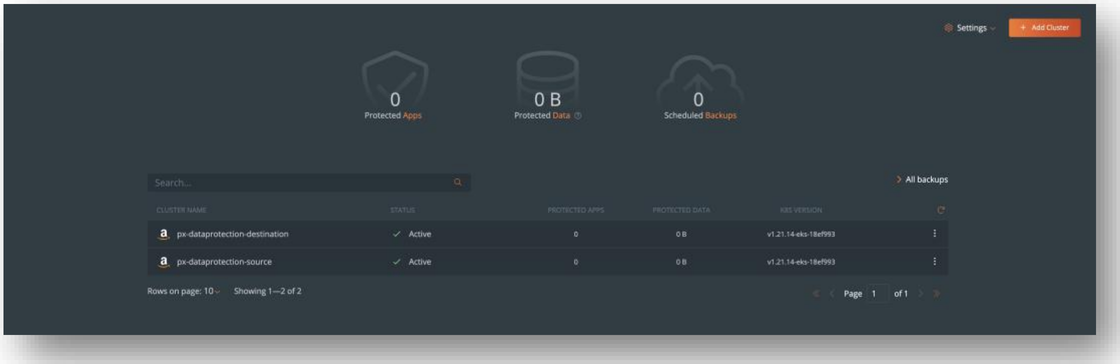
Showing 1—2 of 2

Page 1 of 1

Please ensure Stork 2.4+ is running on this cluster.

Copy command to install stork for: PX Cluster Non PX Cluster

4. Once the clusters are added, it will show up on the dashboard.



0 Protected Apps

0 B Protected Data

0 Scheduled Backups

CLUSTER NAME	STATUS	PROTECTED APPS	PROTECTED DATA	K8S VERSION
px-dataprotection-destination	✓ Active	0	0 B	v1.21.14-eks-18ef993
px-dataprotection-source	✓ Active	0	0 B	v1.21.14-eks-18ef993

Rows on page: 10 Showing 1—2 of 2

Page 1 of 1

In the next section, we will work with Backup and Restore using BaaS.

Kubernetes Backup and Restore

BaaS allows users to create backup jobs to protect their applications. These backup jobs can help users protect Kubernetes resources, application configuration and application data, and store an end-to-end application snapshot in an S3-compatible backup repository. Using Portworx BaaS, users can customize backup rules to include the following scenarios:

1. Backup everything inside a Kubernetes namespace
2. Backup a specific resource (like Persistent Volumes) inside a namespace
3. Backup resources based on a resource label (e.g., app: demo) inside a namespace

This level of flexibility allows users to customize their backup jobs, to comply with their service level agreements (SLAs) or regulations.

In this section, we will cover a couple of different scenarios. We will create a backup for an application, store it in a non-object lock enabled bucket and restore it to the same Amazon EKS cluster and then we will create a backup for another application, store it in an object-lock enabled bucket and then restore it to a completely different cluster.

Kubernetes backup and restore – Same cluster

BaaS allows users to protect their applications from accidental deletions, data corruption and data loss, etc. by creating end-to-end application snapshots, and allowing users to restore these applications when needed.

In this section, we will access an application, generate some data, create a backup, simulate accidental deletion, and the use the application snapshot to restore our application back on the same Amazon EKS cluster.

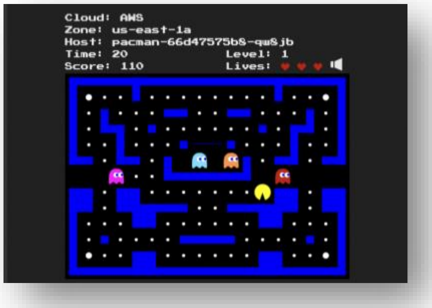
1. From your AWS CloudShell, get the service endpoint (External-IP) for the Pacman application, using the following command:

```
kubectl get svc -n pacman -l name=pacman
```

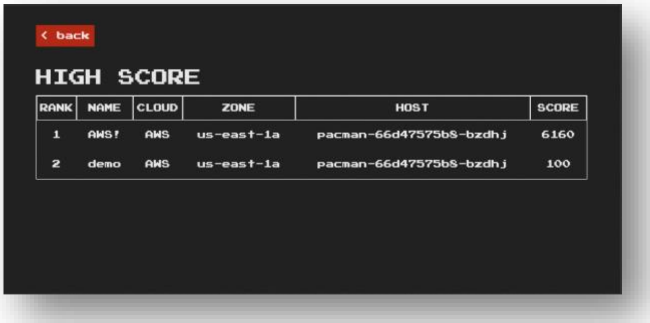
Note: If your CloudShell session has expired, reconnect to CloudShell, change your working directory to PX-DataProtection, and execute the following script.

```
cd PX-DataProtection
./connect-source-eks.sh
```

2. Navigate to the application using a browser and play a game using your arrow keys to generate a high score entry. Enter a name for your score and click Save. Next, click "View Highscore List"



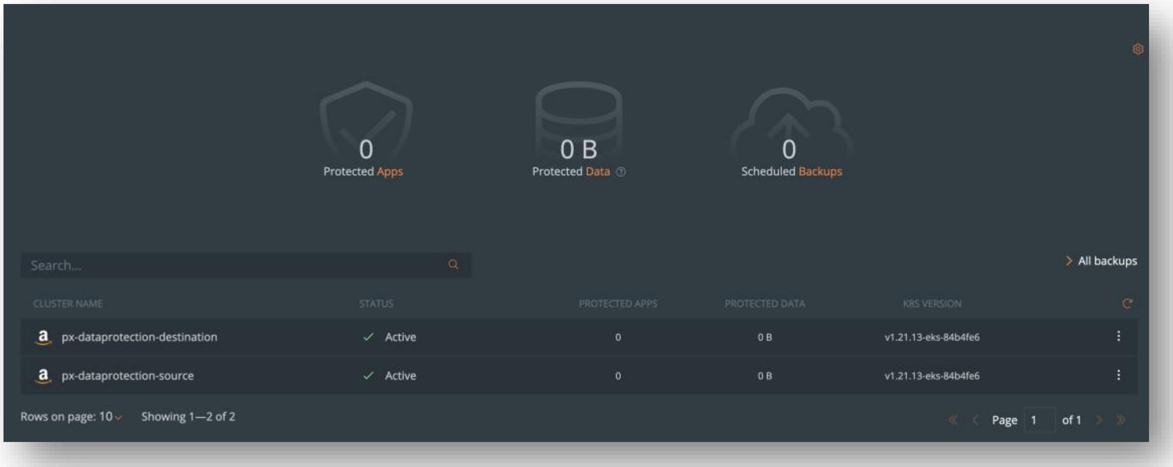
Cloud: AWS
Zone: us-east-1a
Host: pacman-66d47575b8-qw8jb
Time: 20 Level: 1
Score: 110 Lives: ♥ ♥ ♥



HIGH SCORE

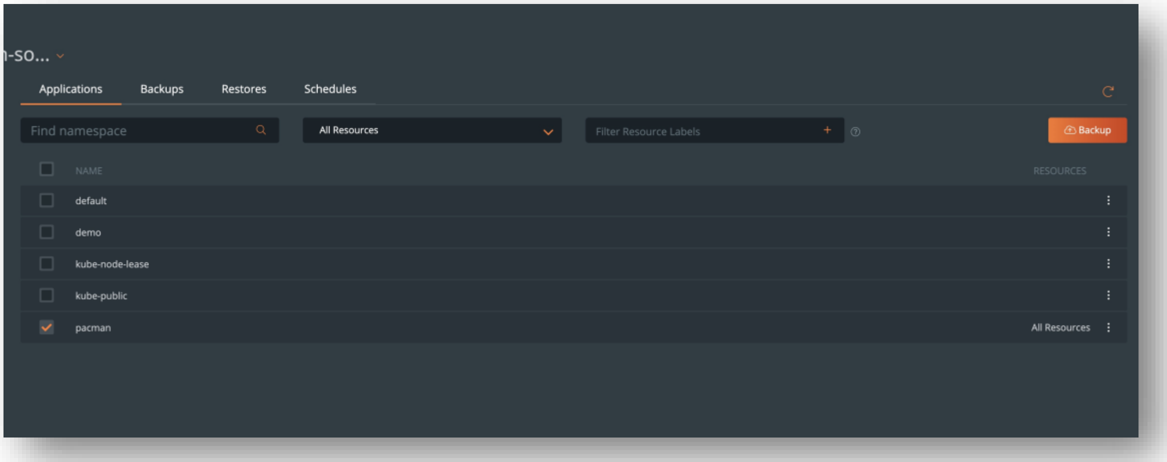
RANK	NAME	CLOUD	ZONE	HOST	SCORE
1	AWS!	AWS	us-east-1a	pacman-66d47575b8-bzdhj	6160
2	demo	AWS	us-east-1a	pacman-66d47575b8-bzdhj	100

3. Now that you have some data stored, let's create a new backup job. Navigate to the BaaS dashboard and select the "px-dataprotection-source" cluster.



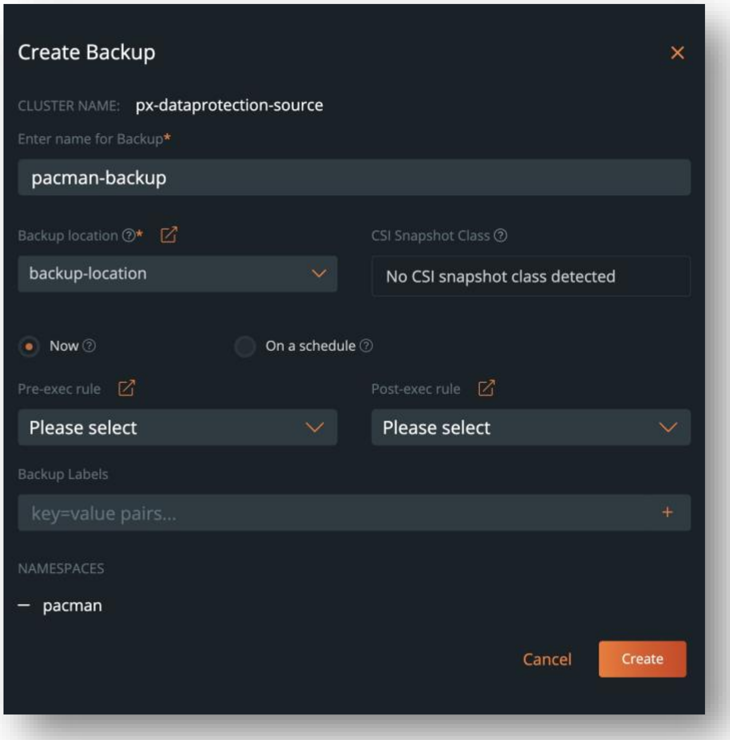
CLUSTER NAME	STATUS	PROTECTED APPS	PROTECTED DATA	K8S VERSION
px-dataprotection-destination	✓ Active	0	0 B	v1.21.13-eks-84b4fe6
px-dataprotection-source	✓ Active	0	0 B	v1.21.13-eks-84b4fe6

4. In this scenario, we are creating a backup for the entire pacman application, so select the *"pacman"* namespace, and click "**Backup**".



	NAME	RESOURCES
□	default	
□	demo	
□	kube-node-lease	
□	kube-public	
☑	pacman	All Resources

5. Enter a name for the backup and select your non-object lock enabled backup location. And then click **"Create"**.
    a. Name: pacman-backup
    b. Backup location: backup-location



Create Backup

CLUSTER NAME: px-dataprotection-source

Enter name for Backup*: pacman-backup

Backup location*: backup-location

CSI Snapshot Class: No CSI snapshot class detected

● Now ○ On a schedule

Pre-exec rule: Please select

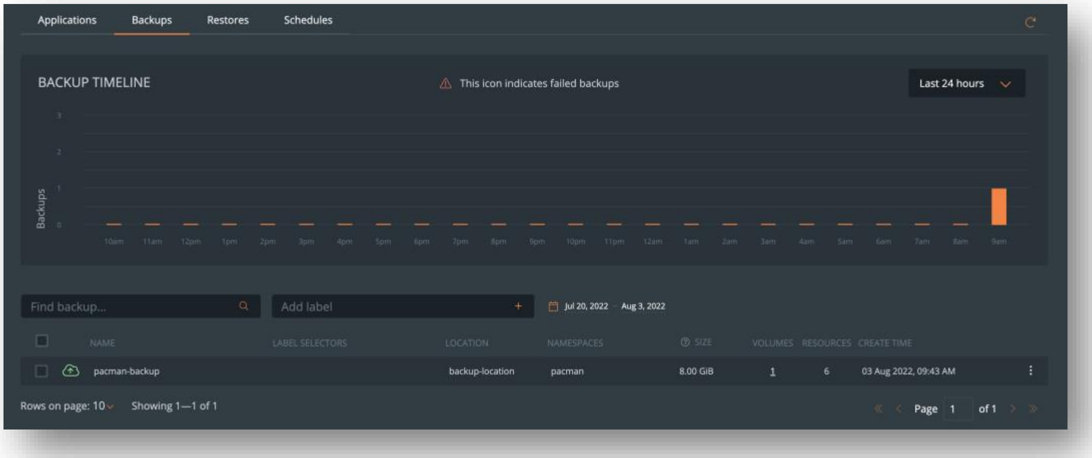
Post-exec rule: Please select

Backup Labels: key=value pairs...

NAMESPACES

– pacman

6. Once created, BaaS will communicate with the source cluster and initiate an end-to-end application backup. You can monitor the backup job using the Backup tab.

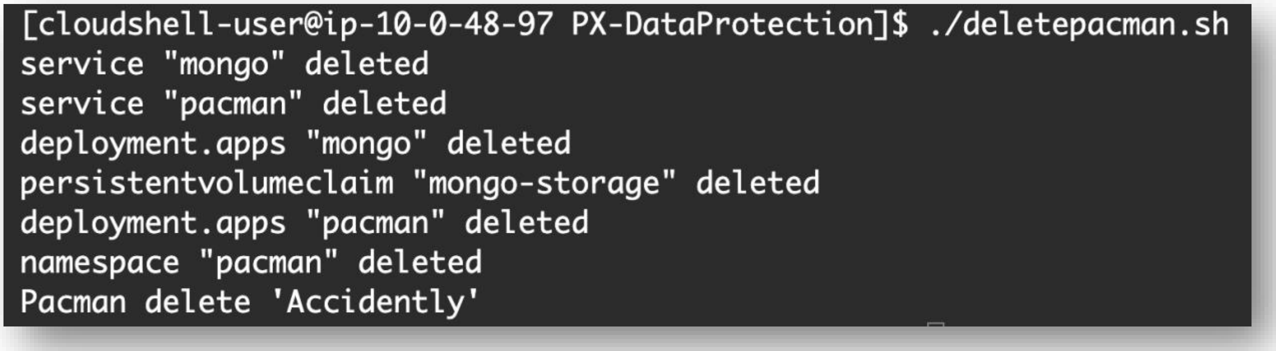


	NAME	LABEL SELECTORS	LOCATION	NAMESPACES	SIZE	VOLUMES	RESOURCES	CREATE TIME
□	pacman-backup		backup-location	pacman	8.00 GiB	1	6	03 Aug 2022, 09:43 AM

Rows on page: 10 Showing 1—1 of 1 Page 1 of 1

6. Once the backup job is completed successfully, it turns green. Let’s simulate a failure and delete your pacman application. To do this, navigate back to your AWS CloudShell, and use the following commands to delete the application.

```
./deletepacman.sh
```



```
[cloudshell-user@ip-10-0-48-97 PX-DataProtection]$ ./deletepacman.sh
service "mongo" deleted
service "pacman" deleted
deployment.apps "mongo" deleted
persistentvolumeclaim "mongo-storage" deleted
deployment.apps "pacman" deleted
namespace "pacman" deleted
Pacman delete 'Accidently'
```

7. It takes a couple of minutes for the application to be deleted. Once deleted, use the following commands to validate that the application has been deleted.

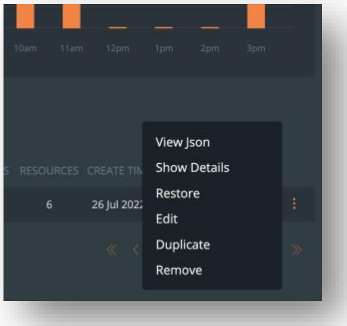
```
kubectl get all -n pacman

kubectl get pvc -n pacman
```

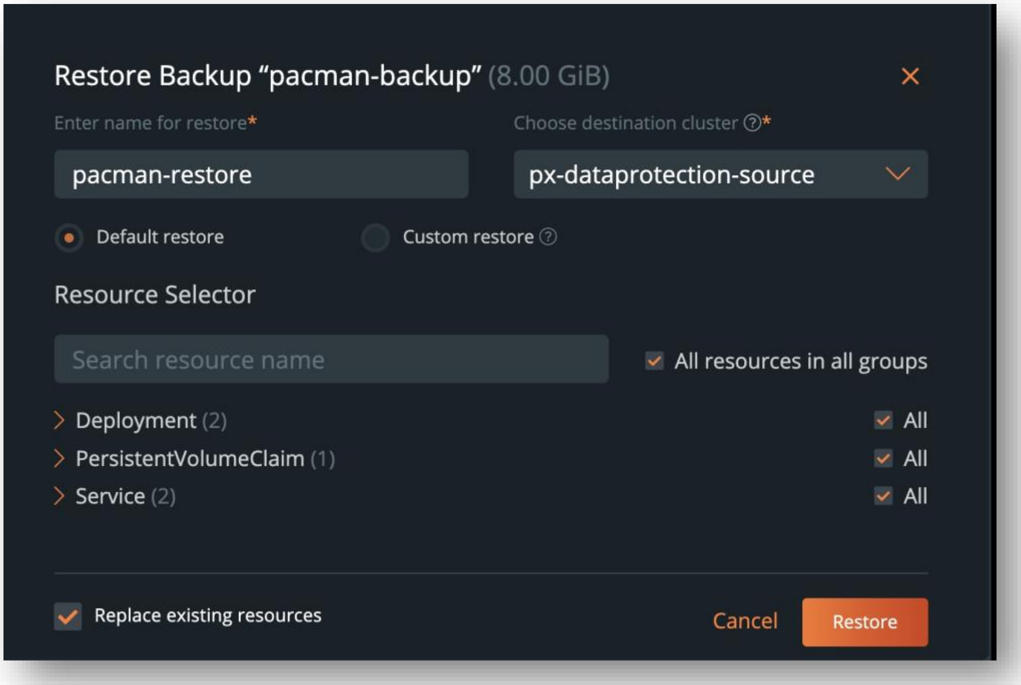
8. Next, navigate back to the BaaS dashboard and click on the px-dataprotection-source cluster and then click on the Backups tab.

Note: If you get logged out of BaaS, navigate to Portworx Central and log in using your credentials.

9. Click the “⁝” on the right of your backup snapshot row and click **“Show Details”**. Here you can get additional details about the different resources backed up.



10. You can see that 2 Deployment objects, one persistent volume and one persistent volume claim and 2 service objects were backed up as part of this snapshot.
11. Once you have reviewed the backup snapshot, click “Restore Backup”. If you cancelled out of the previous screen, then select the backup snapshot again, click on the “⁝” on the right of your backup snapshot row and click “Restore”.
12. Let’s give your restore job a name (pacman-restore) and select the destination cluster. In this scenario, we are restoring the application back to the same cluster, so we will select the “px-dataprotection-source” cluster.



Restore Backup “pacman-backup” (8.00 GiB)

Enter name for restore*: pacman-restore

Choose destination cluster*: px-dataprotection-source

● Default restore ○ Custom restore

Resource Selector

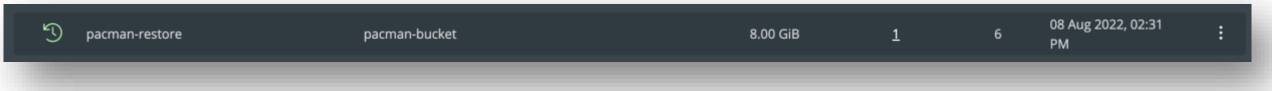
Search resource name

☑ All resources in all groups

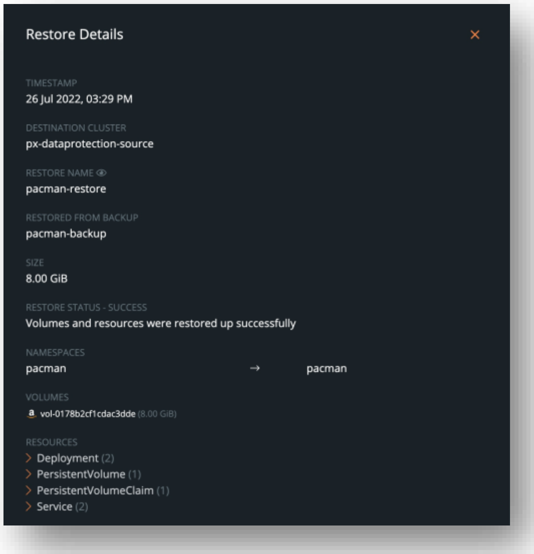
- Deployment (2) ☑ All
- PersistentVolumeClaim (1) ☑ All
- Service (2) ☑ All

☑ Replace existing resources

13. Verify that “All resources in all groups” checkbox is selected and click the “Replace existing resources” check box and hit Restore.
14. Once the restore is successful, you can click on the “:” on the restore object row and click on Show Details. This will give you a list of everything that was restored.



pacman-restore	pacman-bucket	8.00 GiB	1	6	08 Aug 2022, 02:31 PM



Restore Details

TIMESTAMP
26 Jul 2022, 03:29 PM

DESTINATION CLUSTER
px-dataprotection-source

RESTORE NAME
pacman-restore

RESTORED FROM BACKUP
pacman-backup

SIZE
8.00 GiB

RESTORE STATUS - SUCCESS
Volumes and resources were restored up successfully

NAMESPACES
pacman → pacman

VOLUMES
vol-0178b2cf1cdac3dde (8.00 GiB)

RESOURCES
- Deployment (2)
- PersistentVolume (1)
- PersistentVolumeClaim (1)
- Service (2)

Note: If the restore is only partially successful, run the ./deletepacman.sh script again, and wait 5 mins before running through steps 11-14.

15. Navigate back to the AWS CloudShell and use the following commands to validate the restore operation.

```
kubectl get all -n pacman

kubectl get pvc -n pacman
```

16. Use the following command to get the load balancer endpoint (External-IP) for the restored pacman application.

```
kubectl get svc -n pacman -l name=pacman
```

17. Click on High Scores and you can validate that the high scores you created earlier in the lab, are still persistent through an accidental deletion event.

This is how easy it is to use Portworx BaaS to protect your containerized applications running on Amazon EKS clusters!

Ransomware protection using Backup As A Service

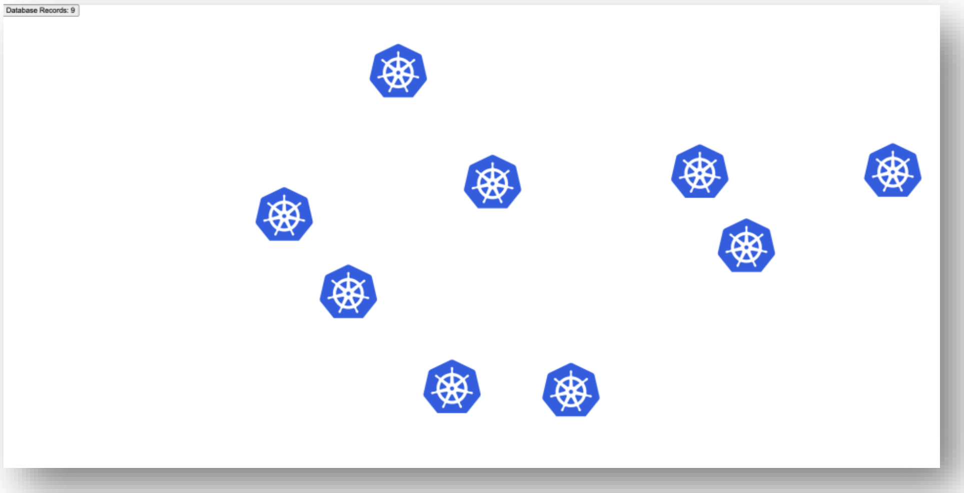
> According to the Data Protection Trends report 2022, 76% of the organizations have suffered from at least one ransomware attack. These attacks are not limited to traditional or legacy infrastructure stacks, but also cover Kubernetes and modern applications running on Kubernetes. Organizations need a solution that can help them protect against such attacks and ensure that they have an insurance policy in place, to recover their applications securely on non-infected infrastructure. In this case, having an insurance policy is synonymous to having an immutable copy of your application snapshot stored offsite, so even if your primary infrastructure gets compromised, hackers can't modify your backups.
> To support this use case, Portworx Backup As A Service allows users to leverage object lock enabled backup buckets to store their application snapshots. This allows app snapshots to be Write Once Read Many (WORM), and thus immutable from any ransomware attack.

In this scenario, we will look at how we can leverage BaaS to take a WORM snapshot for our application and then restore the application to a secondary Amazon EKS cluster.

1. Navigate to the AWS CloudShell tab and use the following command to get the load balancer endpoint for our demo application (k8s-counter-service). This is a different application running in the *"demo"* namespace.

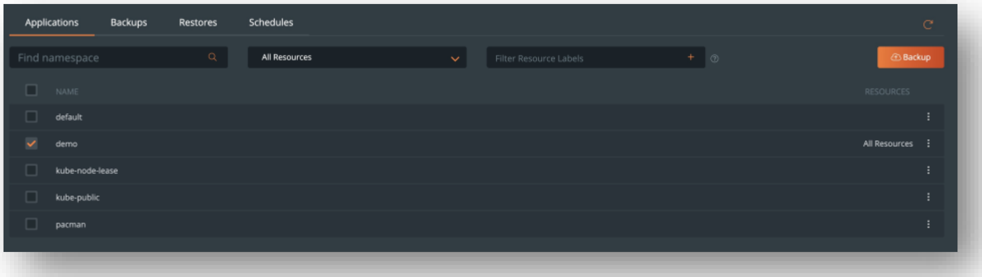
```
kubectl get svc -n demo
```

2. Copy the load balancer endpoint for the *"k8s-counter-service"* and navigate to the application using your web browser. This is a simple application, which generates a Kubernetes logo wherever your click on the screen and then updates the database record by storing the (x,y) coordinates in a backend Postgres database.



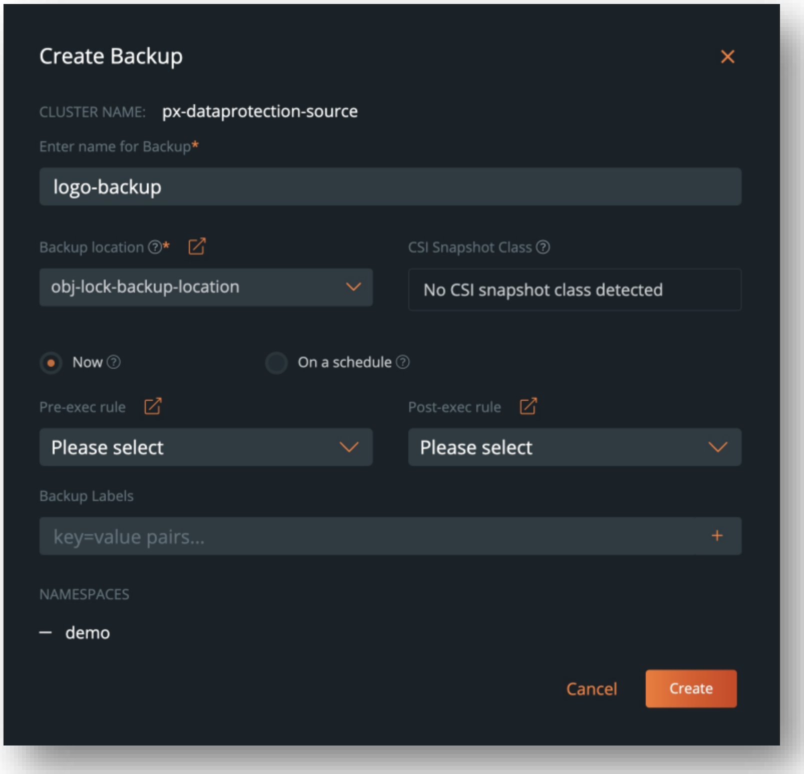
Database Records: 9

3. Once you have some data generated, let’s head to the BaaS interface to create an immutable backup job. Navigate back to the BaaS Dashboard and click on the px-dataprotection-source cluster and select the **“demo”** namespace and click Backup.



□	NAME	RESOURCES
□	default	
☑	demo	All Resources
□	kube-node-lease	
□	kube-public	
□	pacman	

4. Give the backup job a name and select the object lock enabled backup bucket as the backup location and hit *“Create”*.
    a. Enter name for Backup: logo-backup
    b. Backup location: obj-lock-backup-location


Create Backup ×

CLUSTER NAME: px-dataprotection-source

Enter name for Backup*: logo-backup

Backup location*: obj-lock-backup-location

CSI Snapshot Class: No CSI snapshot class detected

● Now ○ On a schedule

Pre-exec rule: Please select

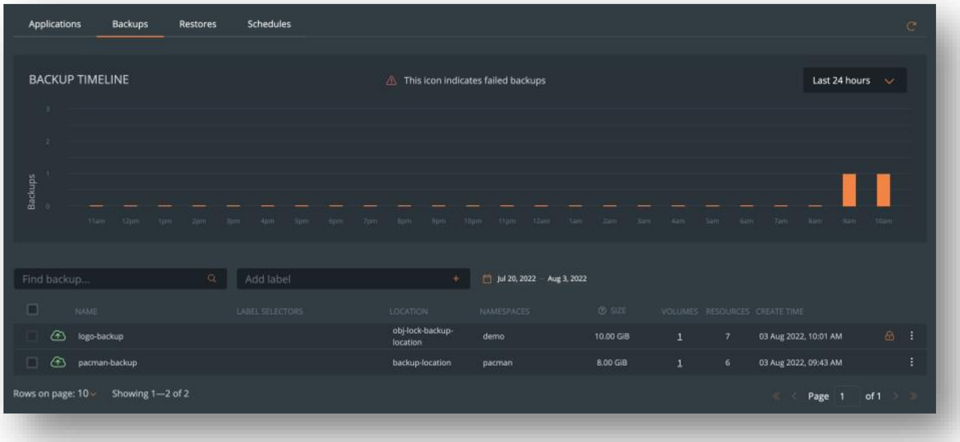
Post-exec rule: Please select

Backup Labels: key=value pairs...

NAMESPACES

– demo

5. This will create an immutable backup snapshot and store it in the Object lock enabled S3 bucket. Once the backup is successfully complete, you will see a lock sign on the snapshot, indicating that this is a WORM backup snapshot.



NAME	LABEL SELECTORS	LOCATION	NAMESPACES	SIZE	VOLUMES	RESOURCES	CREATE TIME
logo-backup		obj-lock-backup-location	demo	10.00 GiB	1	7	03 Aug 2022, 10:01 AM
pacman-backup		backup-location	pacman	8.00 GiB	1	6	03 Aug 2022, 09:43 AM

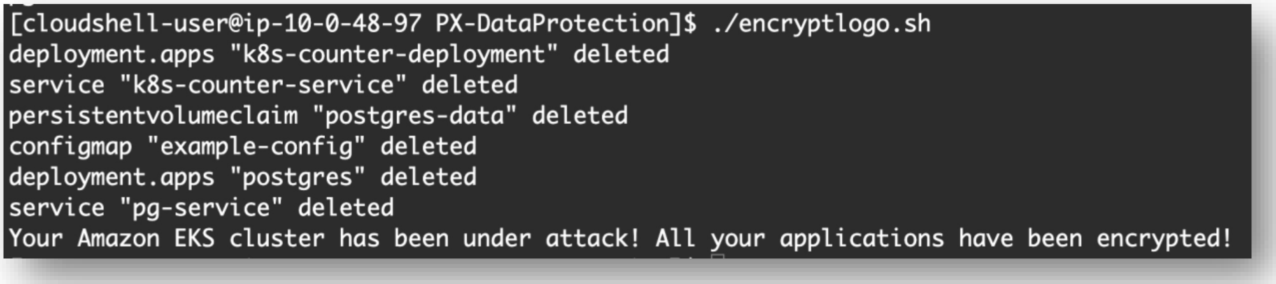
Rows on page: 10 Showing 1—2 of 2 Page 1 of 1

6. Next, let's go ahead and delete the application from our source cluster, simulating a ransomware attack, where the hacker has encrypted your primary application. In our simulation, we are just deleting the application completely from our source Amazon EKS cluster. To do this, navigate to the AWS CloudShell and run the following command:

```
./encryptlogo.sh
```

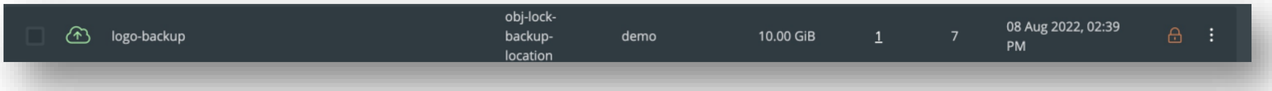
```
kubectl get all -n demo

kubectl get pvc -n demo
```



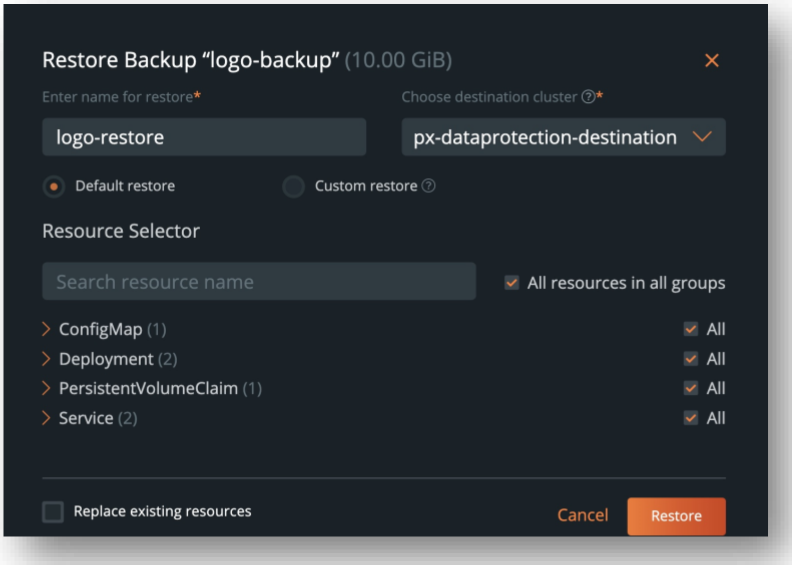
```
[cloudshell-user@ip-10-0-48-97 PX-DataProtection]$ ./encryptlogo.sh
deployment.apps "k8s-counter-deployment" deleted
service "k8s-counter-service" deleted
persistentvolumeclaim "postgres-data" deleted
configmap "example-config" deleted
deployment.apps "postgres" deleted
service "pg-service" deleted
Your Amazon EKS cluster has been under attack! All your applications have been encrypted!
```

7. Now, that your primary Amazon EKS cluster has been compromised, you will have to use your immutable application snapshot and restore your application to a second Amazon EKS cluster. To do that, let's navigate back to the BaaS dashboard, select the **"px-dataprotection-source"** cluster, backups tab, and select the object lock protected backup snapshot.
8. Click on the ":" on the backup snapshot row and click Restore.



□ logo-backup obj-lock-backup-location demo 10.00 GiB 1 7 08 Aug 2022, 02:39 PM

9. Give the restore job a name (logo-restore) and select the **"px-dataprotection-destination"** cluster as the destination cluster. Verify that all the resources are selected and click *"Restore"*.
   a. Enter name for restore: logo-restore
   b. Choose destination cluster: px-dataprotection-destination



Restore Backup "logo-backup" (10.00 GiB)

Enter name for restore*: logo-restore

Choose destination cluster*: px-dataprotection-destination

● Default restore ○ Custom restore

Resource Selector

Search resource name

☑ All resources in all groups

ConfigMap (1) ☑ All

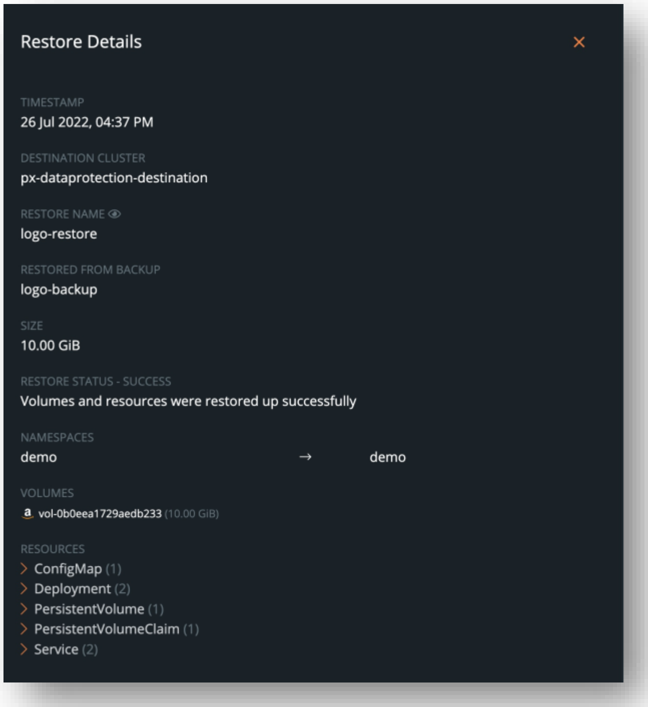
Deployment (2) ☑ All

PersistentVolumeClaim (1) ☑ All

Service (2) ☑ All

□ Replace existing resources

10. This initiates a restore operation on the second Amazon EKS cluster. Once the restore is successfully complete, click on the “⁝” and click Show Details. Here you can see a list of all the resources that were restored from your immutable backup to your new Amazon EKS cluster.



Restore Details

TIMESTAMP
26 Jul 2022, 04:37 PM

DESTINATION CLUSTER
px-dataprotection-destination

RESTORE NAME
logo-restore

RESTORED FROM BACKUP
logo-backup

SIZE
10.00 GiB

RESTORE STATUS - SUCCESS
Volumes and resources were restored up successfully

NAMESPACES
demo → demo

VOLUMES
vol-0b0eea1729aedb233 (10.00 GiB)

RESOURCES
- ConfigMap (1)
- Deployment (2)
- PersistentVolume (1)
- PersistentVolumeClaim (1)
- Service (2)

11. Navigate back to the AWS CloudShell, so we can log into our second cluster and validate that all our application data was restored. To do that use the following commands:

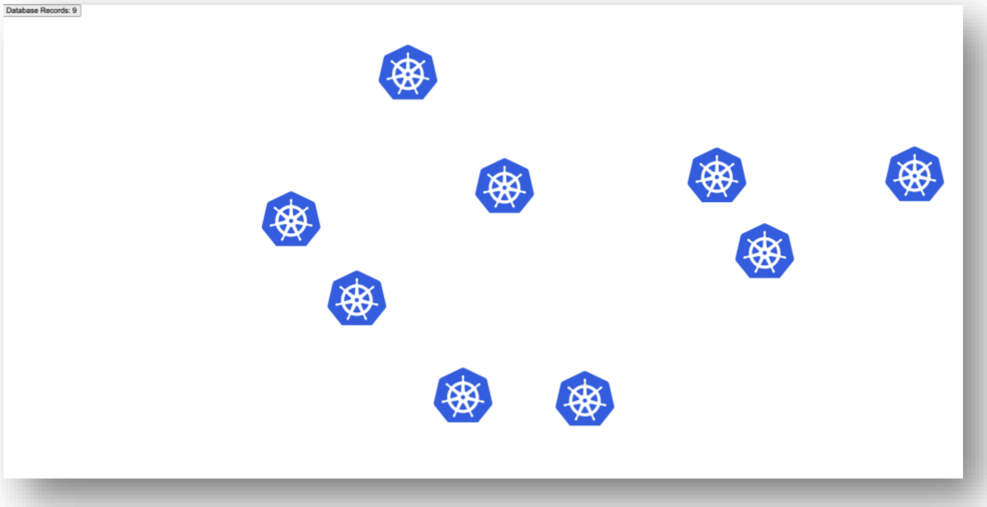
```
./connect-destination-eks.sh

kubectl get all -n demo
kubectl get pvc -n demo
```

12. Get the load balancer endpoint using the following command and navigate to our application using a web browser.

```
kubectl get svc -n demo
```

13. Here, you should see the same number of Kubernetes logos at the exact same location, indicating that our application restore has been successful.



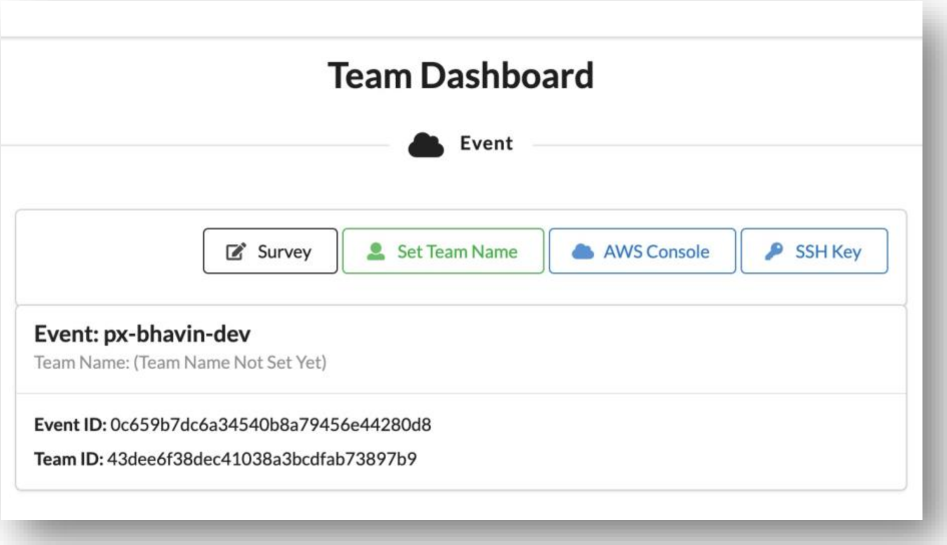
This is how users can leverage BaaS to protect their applications and recover them in case of a ransomware attack.

Clean Up

1. Once you are done with the lab, navigate back to AWS CloudShell and use the following commands to clean up the resources deployed.

```
./cleanup.sh
```

2. Go back to the AWS Event Engine dashboard and click *"Survey"* to complete the survey.



Team Dashboard

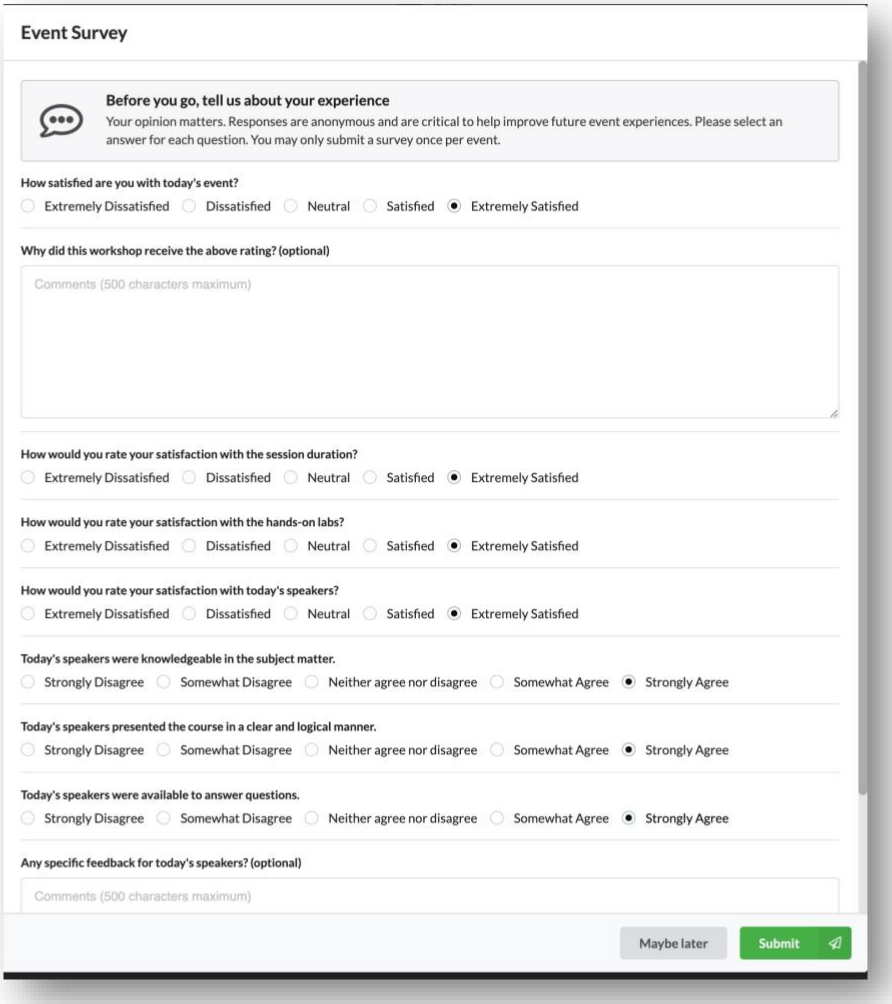
Event

Event: px-bhavin-dev

Team Name: (Team Name Not Set Yet)

Event ID: 0c659b7dc6a34540b8a79456e44280d8

Team ID: 43dee6f38dec41038a3bcdfab73897b9



Event Survey

Before you go, tell us about your experience
Your opinion matters. Responses are anonymous and are critical to help improve future event experiences. Please select an answer for each question. You may only submit a survey once per event.

How satisfied are you with today's event?
○ Extremely Dissatisfied ○ Dissatisfied ○ Neutral ○ Satisfied ● Extremely Satisfied

Why did this workshop receive the above rating? (optional)
Comments (500 characters maximum)

How would you rate your satisfaction with the session duration?
○ Extremely Dissatisfied ○ Dissatisfied ○ Neutral ○ Satisfied ● Extremely Satisfied

How would you rate your satisfaction with the hands-on labs?
○ Extremely Dissatisfied ○ Dissatisfied ○ Neutral ○ Satisfied ● Extremely Satisfied

How would you rate your satisfaction with today's speakers?
○ Extremely Dissatisfied ○ Dissatisfied ○ Neutral ○ Satisfied ● Extremely Satisfied

Today's speakers were knowledgeable in the subject matter.
○ Strongly Disagree ○ Somewhat Disagree ○ Neither agree nor disagree ○ Somewhat Agree ● Strongly Agree

Today's speakers presented the course in a clear and logical manner.
○ Strongly Disagree ○ Somewhat Disagree ○ Neither agree nor disagree ○ Somewhat Agree ● Strongly Agree

Today's speakers were available to answer questions.
○ Strongly Disagree ○ Somewhat Disagree ○ Neither agree nor disagree ○ Somewhat Agree ● Strongly Agree

Any specific feedback for today's speakers? (optional)
Comments (500 characters maximum)

3. Once you have filled out the survey, click *"Exit Event"* from the top right of the dashboard.

Additional Resources

- Portworx Blogs
- Portworx Demos
- Portworx Backup As A Service Documentation
- Portworx PX-Backup Documentation