



portworx
backup

Portworx Backup 2.7.2

Walmart


Early Access

Portworx Backup overview.....	3
Before you begin.....	3
Workflow.....	4
Azure Portal Prerequisites.....	5
Azure Kubernetes Cluster Prerequisites.....	5
Install Prerequisites.....	11
Install Portworx Backup.....	14
Install Stork 24.3.0-EA.....	17
Add Azure cloud account.....	19

Portworx Backup overview

Portworx Backup (PX-Backup) is a Kubernetes backup solution that allows you to back up and restore applications, KubeVirt Virtual Machines (VMs) and their data across multiple clusters. Portworx Backup works with Portworx Central (a web console that centralizes various features or products including Portworx Backup into a single user interface), allowing administrators or other users to manage backups and restores of multiple Kubernetes clusters through a web console. Under this principle of multi-tenancy, authorized users connect through authorization providers to create and manage backups for clusters and applications for which they have permissions (without reaching out to the administrators). Portworx Backup maintains a repository of available application backups and restores them to any destination cluster that a user has access to. Portworx Backup communicates with backup locations on regular-basis to check for the availability of new backups.

For more information, refer to [Portworx Backup overview](#).

 **Caution: This is an early access feature meant for testing purposes only. Please do not deploy or use in production environments until GA version is available.**

Before you begin

Refer the following topics from Portworx Backup documentation:

1. [Concepts](#)
2. [Web console](#)
3. [Role privileges matrix](#)
4. [Backup types by driver matrix](#)

Workflow

I. [Azure Portal Prerequisites](#)

II. [Azure Kubernetes Cluster Prerequisites](#)

III. Install prerequisites

IV. Install

1. [Install on-premises](#)
2. [Install Stork](#)

V. [Configure](#)

V. Operate

1. [Add Azure cloud account](#)
2. [Add Azure backup location](#)
3. [Create unlocked schedule policies](#)
4. [Add AKS clusters](#)
5. [Create backup rules](#)
6. [Backup](#)
7. [Restore](#)
8. [Share backups with users and groups](#)
9. [Apply Labels](#)
10. [Delete stranded backup resources](#)

VI. Troubleshoot

- [Uninstall Portworx Backup](#)

VI. Reference

- [Portworx Backup Reference](#)

Azure Portal Prerequisites

1. [Azure Storage account name](#)

```
az storage account list --resource-group  
<ResourceGroupName> --query "[].{Name:name}" --output  
table
```

2. [Azure storage account key](#)

```
az storage account keys list --resource-group  
<ResourceGroupName> --account-name  
<StorageAccountName> --query "[0].value"
```

Azure Kubernetes Cluster Prerequisites

This topic provides the list of permissions and actions required for managing Azure Clusters. These permissions and actions are essential for managing Azure Clusters effectively. Ensuring that the necessary permissions are granted will help in maintaining a secure and well-functioning cluster environment. The topic outlines the necessary permissions required to:

1. Add a Cluster as Application Cluster in Portworx Backup

2. Bring Portworx Backup on any Azure Cluster



Note: Sometimes creation of an Azure custom role takes at least 20 minutes for the role (with the specified permissions) to reflect in your Azure cluster environment.

Permissions to add a Cluster as Application Cluster

You need the following list of permissions/actions required for adding a cluster as an application cluster:

Permissions	Purpose
Microsoft.Compute/disks/beginGetAccess/action	Grants temporary access to a disk, typically used for scenarios where a disk snapshot needs to be accessed or copied.
Microsoft.Compute/snapshots/delete	Allows for the deletion of snapshots, crucial for managing storage and ensuring outdated snapshots are removed.
Microsoft.Compute/snapshots/write	Permits creating or updating snapshots of virtual machine disks, essential for backup and restore operations.
Microsoft.Compute/snapshots/read	Enables reading snapshot properties and metadata, necessary for monitoring and managing snapshots.
Microsoft.Compute/disks/write	Grants permission to create or update managed disks. This is crucial for provisioning storage for virtual machines.

Microsoft.Compute/disks/read	Enables reading the properties and metadata of managed disks. Necessary for monitoring and managing disk resources.
Microsoft.Compute/disks/delete	Allows the deletion of managed disks. This is essential for managing storage and cleaning up unused resources.
Microsoft.Storage/storageAccounts/read	Enables reading the properties and metadata of storage accounts, necessary for accessing and managing storage resources.
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/write	Grants permission to create or update virtual machines within a scale set, important for scaling and managing VM instances.
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read	Allows reading the properties and metadata of virtual machines within a scale set, necessary for monitoring and managing VM instances.
Microsoft.Compute/virtualMachineScaleSets/read	Enables reading the properties and metadata of VM scale sets, important for monitoring and managing scale sets.

Permissions to bring up Portworx Backup on any Cluster

You need the following permissions/actions to bring up Portworx Backup on any cluster:

Permissions	Purpose
<code>Microsoft.Compute/disks/delete</code>	Allows the deletion of managed disks. This is essential for managing storage and cleaning up unused resources.
<code>Microsoft.Compute/disks/write</code>	Grants permission to create or update managed disks. This is crucial for provisioning storage for virtual machines.
<code>Microsoft.Compute/disks/read</code>	Enables reading the properties and metadata of managed disks. Necessary for monitoring and managing disk resources.
<code>Microsoft.Compute/virtualMachines/write</code>	Permits creating or updating virtual machines. This is essential for provisioning and configuring VMs.
<code>Microsoft.Compute/virtualMachines/read</code>	Allows reading the properties and metadata of virtual machines. This is necessary for monitoring and managing VMs.
<code>Microsoft.Network/loadBalancers/read</code>	Enables reading the properties and metadata of load balancers. This is important for managing and monitoring network traffic distribution.

<code>Microsoft.Network/loadBalancers/write</code>	Permits creating or updating load balancers. This is essential for configuring and managing network traffic distribution.
<code>Microsoft.Network/loadBalancers/delete</code>	Allows for the deletion of load balancers. This is crucial for cleaning up and managing network resources.
<code>Microsoft.Network/publicIPAddresses/read</code>	Enables reading the properties and metadata of public IP addresses. This is necessary for managing public-facing network resources.
<code>Microsoft.Network/publicIPAddresses/write</code>	Permits creating or updating public IP addresses. This is essential for provisioning public-facing network resources.
<code>Microsoft.Network/publicIPAddresses/delete</code>	Allows for the deletion of public IP addresses. This is important for managing and cleaning up network resources.
<code>Microsoft.Network/publicIPAddresses/join/action</code>	Grants permission to join public IP addresses to resources. This is crucial for associating public IP addresses with network resources.
<code>Microsoft.Network/loadBalancers/loadBalancingRules/read</code>	Allows reading the properties and metadata of load balancing rules. This is necessary for monitoring and managing load balancer rules.

Microsoft.Network/loadBalancers/probes/read	Enables reading the properties and metadata of load balancer probes. This is important for managing and monitoring load balancer health checks.
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read	Grants permission to read the properties and metadata of network interfaces attached to VM scale set instances. This is necessary for monitoring and managing network configurations of scale set VMs.
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipconfigurations/publicipaddresses/read	Allows reading the properties and metadata of public IP addresses attached to network interfaces of VM scale set instances. This is crucial for managing and monitoring public-facing network configurations.
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/write	Grants permission to create or update virtual machines within a scale set, important for scaling and managing VM instances.
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read	Allows reading the properties and metadata of virtual machines within a scale set, necessary for monitoring and managing VM instances.
Microsoft.Compute/virtualMachineScaleSets/read	Enables reading the properties and metadata of VM scale sets, important for monitoring and managing scale sets.

Microsoft.Network/networkSecurityGroups/read	Enables reading the properties and metadata of network security groups. This is necessary for monitoring and managing network security configurations.
Microsoft.Network/networkSecurityGroups/write	Grants permission to create or update network security groups. This is essential for configuring and managing network security settings.

Restore prerequisites

If you have to restore a backup created in a cluster and you have to restore a backup to a cluster in a different resource group, follow the below steps.

Note: The below steps are not required:

- a. If you have backed up some applications and want to restore to a cluster in the same resource group

OR

- b. If both the clusters are created with the same managed identity/service principal, then these steps are not required.

1. Create a custom role with the following command and JSON content:

- a. JSON content

```
{
  "Name": "<custom_role_name>",
  "Description": "",
  "AssignableScopes": [
    "/subscriptions/<subscription_ID>"
  ],
  "Permissions": [
    {
```

```

        "Actions": [
            "Microsoft.Compute/disks/beginGetAccess/action"
        ],
        "NotActions": [],
        "DataActions": [],
        "NotDataActions": []
    }
]
}

```

b. Command:

```
az role definition create --role-definition roles.json
```

2. Fetch your **AKS Infrastructure Resource Group Name** with the following command:

```
az aks show -n <aks_cluster_name> -g
<source_backup_resource_group_name> | jq -r
'.nodeResourceGroup'
```

3. Get the **Principal ID** associated with your Kubernetes Source Cluster

```
az aks show --resource-group
<destination_cluster_resource_group_name> --name
<kubernetes_cluster_name> --query identity
```

4. Add **Assignee** with the following command:

```
az role assignment create --assignee <"Principal_Id"> --role
<"Role_name"> --scope
"/subscriptions/<Subscription_Id>/resourceGroups/<AKS_Infrastru
cture_Resource_Name>"
```

Install Prerequisites

Refer the following Portworx Backup prerequisites and ensure that they are met:

a. Install Prerequisites

Make sure you have the following components installed:

Component	Version
Kubernetes	1.29.x
Portworx	3.1.1
Stork	24.3.0-EA

b. Network prerequisites

Make sure that the following ports are open or enabled in Portworx Backup cluster:

Port	Purpose
10001	For REST API communication
10002	For gRPC server communication

c. Portworx Backup image repositories

Image	Version
docker.io/portworx/pxcentral-onprem-api	2.7.2-EA
docker.io/portworx/pxcentral-onprem-ui-frontend	2.7.2-EA

docker.io/portworx/pxcentral-onprem-ui-backend	2.7.2-EA
docker.io/portworx/pxcentral-onprem-ui-lhbackend	2.7.2-EA
docker.io/portworx/pxcentral-onprem-post-setup	2.7.2-EA
docker.io/portworx/px-backup	2.7.2-EA
docker.io/portworx/postgresql	11.19.0-debian-11-r1
docker.io/portworx/keycloak	21.1.2
docker.io/portworx/keycloak-login-theme	2.7.0
docker.io/portworx/busybox	1.35.0
docker.io/portworx/mysql	5.7.44
docker.io/portworx/mongodb	5.0.24-debian-11-r20
docker.io/portworx/kopiaexecutor	1.2.13
docker.io/portworx/nfsexecutor	1.2.13
docker.io/portworx/filesystemctl	1.2.13
docker.io/portworx/prometheus	v2.48.0
docker.io/portworx/alertmanager	v0.26.0
docker.io/portworx/prometheus-operator	v0.70.0
docker.io/portworx/prometheus-config-reloader	v0.70.0
openstorage/stork	24.3.0-EA
openstorage/cmdexecutor	24.3.0-EA

Install Portworx Backup

1. If you are installing Portworx Backup alone without Portworx Enterprise, skip this step. If you want to install Portworx Backup with Portworx Enterprise, you must first [Install Portworx](#), then create the following storage class on your Kubernetes cluster:

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: portworx-sc
provisioner: kubernetes.io/portworx-volume
parameters:
  repl: "3"
```

2. From the CLI, install helm:

```
curl -fsSL -o get_helm.sh
https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3
chmod 700 get_helm.sh
./get_helm.sh
```

3. Access [Portworx Central portal](#).
4. From the home page, navigate to **Explore our Products > Backup Services**.
5. Click on **I agree to EULA** and go through the **Portworx Products Terms of Use** carefully.
6. Navigate back to the [Portworx Central portal](#) and click **Start Free Trial**.
7. In the **Spec Details** tab provide the following values:
 - **Backup Version:** make sure you select version

- **Namespace:** provide the name of the namespace where you want an instance of Portworx Backup to be installed
- **Install using:** choose Helm 3
- **Select your environment:** choose On-Premises or Cloud based on your storage environment
- **StorageClass Name:** name of the StorageClass, refer tooltip for more details
- **Use your OIDC:** select this checkbox only if your external authorization provider is Auth0 and key in the following fields:
 - Endpoint
 - Client ID
 - Client SecretThese values can be fetched from the **Auth0** web console.
- **Use existing Prometheus:** select this checkbox if you have to use your existing Prometheus stack to monitor Portworx Backup and enter the values for the following fields:
 - **Prometheus Endpoint:** enter details of the endpoint where your Prometheus is installed
 - **Alertmanager Endpoint:** enter details of the endpoint where your Alertmanager is installed
 - **Prometheus secret name:** enter secret name of your Prometheus stack
 - **Alertmanager secret name:** enter secret name of your Alertmanager
 - **Custom email template from PX-Backup:** select to upload Portworx Backup's custom email template to your pre-configured Alertmanager for email notifications
- **Use custom registry:** for air-gapped environments
 - **Custom Image Repository Location:** path of custom image repository

- **Image Pull Secret(s):** create a secret only if image pulling from an internal repository requires credentials

8. Click **Next** to navigate to the **Finish** tab.

9. From the machine where you run the `helm3` command, download the latest `px-central` package with the following command.

```
curl -L
https://github.com/portworx/helm/raw/2.7.2_EA/stable/px-central-2.7.2.tgz -o px-central-2.7.2.tgz
```

10. Execute the command under **Step 2** of the web console under **Install using the 'set' command**. To Install Portworx Backup with set command, replace

- `portworx/px-central` with `px-central-2.7.2.tgz`
- `--version 2.7.1` with `--version 2.7.2`

```
helm install px-central px-central-2.7.2.tgz --namespace
<px-backup-namespace> --create-namespace --version 2.7.2
--set
persistentStorage.enabled=true,persistentStorage.storageClass=
"<storage-class-name>",pxbackup.enabled=true
```

- (Optional) For azure clusters configured with azure proxy, provide `proxy.azureProxyEnabled=true` with `--set` command:

```
helm install px-central px-central-2.7.2.tgz --namespace
<px-backup-namespace> --create-namespace --version 2.7.2
--set
persistentStorage.enabled=true,persistentStorage.storageClass=
"<storage-class-name>",pxbackup.enabled=true,proxy.azureProxyEnabled=true
```



Note: Refrain from using the **Install using the 'values-px-central.yaml' file** option.

11. Click **Finish** to complete the installation.

Install Stork 24.3.0-EA

You can install Stork with or without Portworx Enterprise with Deployment method, steps are outlined in the following section:

Without Portworx Enterprise

To install Stork version 24.3.0-EA on your Kubernetes cluster without installing Portworx Enterprise, run the below commands:

1. Download the Stork deployment spec:

```
curl -fsL -o stork-spec.yaml  
"https://install.portworx.com/pxbackup?comp=stork&storkNonPx=true"
```

2. In the `stork-spec.yaml`, change the Stork version to 24.3.0-EA if the version differs.

3. Apply the `stork-spec.yaml` to install the latest Stork version:

```
kubectl apply -f stork-spec.yaml
```

With Portworx Enterprise

If you have to install Stork 24.3.0-EA along with Portworx Enterprise, you can opt-in for Portworx Operator installation

Stork fresh installation for Portworx Backup through web console

If Stork is not installed as part of Portworx deployment, perform the following steps:

1. From the home page, click **Add cluster**.
2. Choose your Kubernetes platform.
3. Provide cluster name and Kubeconfig details.
4. Click Px-cluster to copy the stork installation command.
5. Run the Stork installation command.



Note: If Stork is installed through the PX-Cluster option from the web console in a namespace other than the namespace where Portworx Enterprise is deployed, perform Step 6 or else go to Step 7.

6. Update the following key-value pairs in stork deployment's (`stork-spec.yaml`) environment variable section, using `kubectl edit` command.


```
kubectl edit deployment stork -n <stork-namespace>
```

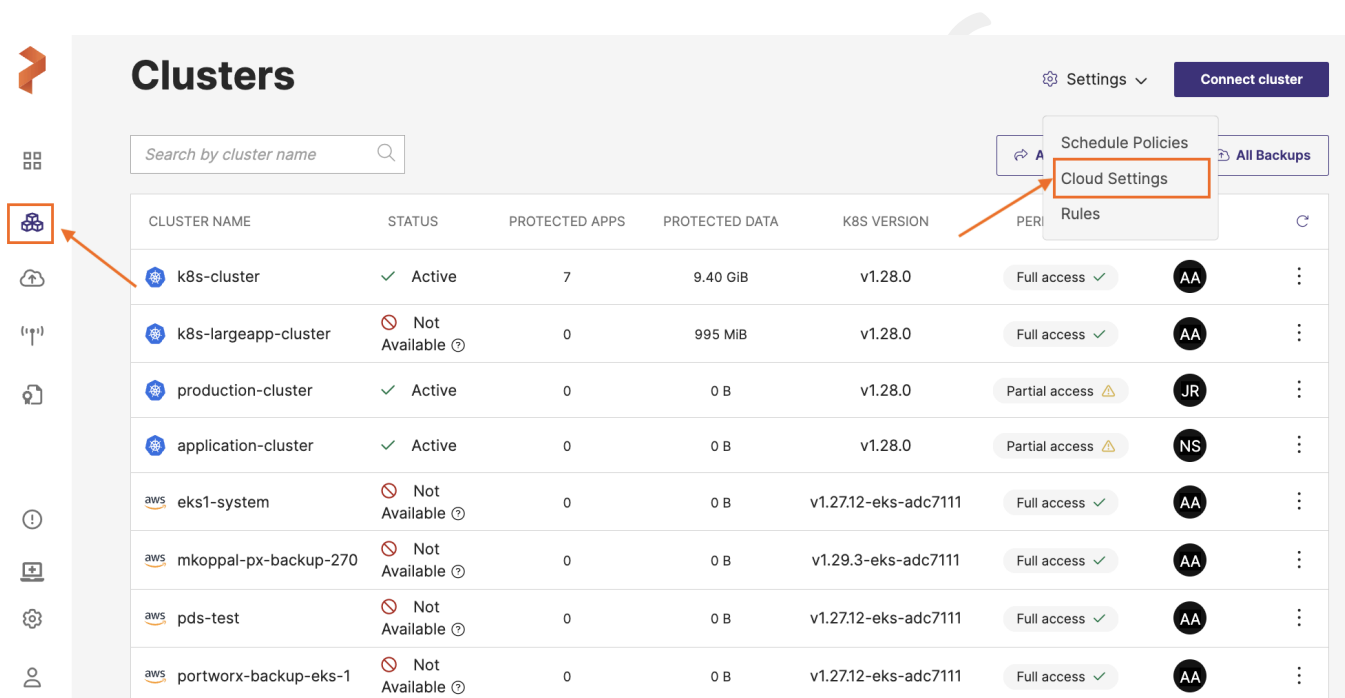
```
env:
  - name: PX_NAMESPACE
    value: <portworx-deployed-namespace>
  - name: PX_SERVICE_NAME
    value: portworx-api
  - name: STORK-NAMESPACE
    value: portworx
```

7. Click **Add Cluster**.

Add Azure cloud account

Once you have all the parameters specified in [Azure Cluster prerequisites](#) topic, you can add your Azure cloud account in Portworx Backup. To add, perform the following steps:

1. In the home page, from the left navigation pane, click **Clusters** .
2. In the upper-right corner, click **Settings > Cloud Settings**:



Clusters

Search by cluster name

CLUSTER NAME	STATUS	PROTECTED APPS	PROTECTED DATA	K8S VERSION	PERI	Rules
k8s-cluster	Active	7	9.40 GiB	v1.28.0	Full access	AA
k8s-largeapp-cluster	Not Available	0	995 MiB	v1.28.0	Full access	AA
production-cluster	Active	0	0 B	v1.28.0	Partial access	JR
application-cluster	Active	0	0 B	v1.28.0	Partial access	NS
eks1-system	Not Available	0	0 B	v1.27.12-eks-adc7111	Full access	AA
mkoppal-px-backup-270	Not Available	0	0 B	v1.29.3-eks-adc7111	Full access	AA
pds-test	Not Available	0	0 B	v1.27.12-eks-adc7111	Full access	AA
portworx-backup-eks-1	Not Available	0	0 B	v1.27.12-eks-adc7111	Full access	AA

3. In **Cloud Accounts** section, click **Add**:



Cloud Settings

Cloud Accounts

NAME	OWNER	
s3-minio	Owner	⋮
rke	Owner	⋮
s3-account	Owner	⋮
azure-account	Owner	⋮
aws-cluster	Owner	⋮
rancher-account	Owner	⋮
tencentcloud	Owner	⋮

+ Add

4. Choose **Azure** from the **Please choose a cloud provider** drop-down and populate the following fields:



Add Cloud Account

*required

ⓘ Please choose a cloud provider *

Azure

ⓘ Cloud Account Name *

azure-cloud-account

ⓘ Storage Account Name *

<azure-storage-account-name>

ⓘ Storage Account Key *

.....

ⓘ Following fields are mandatory to restore or delete cloud-native backups taken prior to Portworx Backup version 2.7.0

ⓘ Client Id

ⓘ Client Secret

ⓘ Tenant Id

ⓘ Subscription Id

← Back

Cancel

Add



Note: **Cloud account name**, **storage account name**, and **storage account key** are mandatory fields to associate your Azure cloud account with Portworx Backup

- **Cloud Account Name:** enter a descriptive account name
- **Storage account name:** specify the name of your Azure storage account
- **Storage account key:** specify your Azure storage account key



Note: **Client Id**, **Client Secret**, **Tenant Id**, and **Subscription Id** fields are optional and can be updated later.

- **(Optional) Client Id:** specify your Azure application client ID
- **(Optional) Client Secret:** specify your Azure application client secret
- **(Optional) Tenant Id:** specify your Azure Active Directory tenant ID
- **(Optional) Subscription Id:** specify your Azure subscription ID

5. Click **Add**.



portworx[®]

by Pure Storage[®]

