Forcepoint

# Forcepoint Data Visibility

## Powered by GetVisibility

### Installation Upgrade K3s

Forcepoint

Report



Forcepoint
4 November 2023
Forcepoint Proprietary

# Table of Contents



© 2023 Forcepoint

# Introduction

This document outlines the steps to install and update K3s servers and how to deploy and backup Data Visibility services.

# K3s Installation - Client

Refer to the following page for the installation details:

K3s Installation (Forcepoint Data Visibility & Forcepoint Data Classification)

# Update – Client

**Data Visibility backend services**

Updates and custom settings are automatically applied to all Data Visibility backend services if the cluster has access to the public internet and can connect to the management server.

In case there is no internet connection, or the management server is down, the cluster agent will keep trying to reach the management server until a connection can be established.

**K3s cluster**

1. To upgrade K3s from an older version to a specific version you can run the following command:

```
curl -sfL https://get.k3s.io | INSTALL_K3S_VERSION=vX.Y.Z-rc1 sh -
```

2. Stop the old k3s binary (for example: systemctl stop k3s) and start it again (for example: systemctl start k3s). For more details, please refer to the official documentation.

**Certificates**

3. By default, certificates in K3s expire in 12 months. If the certificates are expired or have fewer than 90 days remaining before they expire, the certificates are rotated when K3s is restarted.

# Backup - Client

**Consul**

1. Find the IP of the server where Consul is running (in case you have a multi-node cluster):

```
kubectl get pod/gv-essentials-consul-server-0 -o jsonpath='{.spec.nodeName}'
```

2. Log into the server using SSH and run the following command to take a snapshot of Consul:

```
kubectl exec -it gv-essentials-consul-server-0 -- consul snapshot save
/consul/data/backup.snap
```

3. Find the path where the snapshot has been saved to:

```
kubectl get pvc/data-default-gv-essentials-consul-server-0 -o jsonpath='{.spec.volumeName}'
| xargs -I{} kubectl get pv/{} -o jsonpath='{.spec.hostPath.path}'
```

4. Copy the snapshot file to a safe place.

© 2023 Forcepoint Forcepoint Proprietary

**PostgreSQL**

1. Find the IP of the server where the PostgreSQL master is running (in case you have a multi-node cluster):

```
kubectl get pod/gv-postgresql-0 -o jsonpath='{.spec.nodeName}'
```

2. Log into the server using SSH and run the following command to backup all databases:

```
kubectl exec -it gv-postgresql-0 -- bash -c "pg_dumpall -U gv | gzip >
/home/postgres/pgdata/backup.sql.gz"
```

3. Find the path where the backup has been saved to:

```
kubectl get pvc/pgdata-gv-postgresql-0 -o jsonpath='{.spec.volumeName}' | xargs -I{} kubectl
get pv/{} -o jsonpath='{.spec.hostPath.path}'
```

4. Copy the backup file to a safe place.

© 2023 Forcepoint

Forcepoint

**forcepoint.com/contact**

## About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.