Abstract

This document describes how to configure a NetApp® Kubernetes Service (NKS) based Kubernetes cluster by using NetApp Trident as a storage orchestration solution. It also describes the installation of SAP Data Hub in the NKS cluster.
1 Introduction

The installation of SAP Data Hub Foundation inside a NetApp® Kubernetes Service (NKS) cluster includes these general steps:

- Deploy an NKS cluster.
- Install and configure NetApp Trident as storage orchestration solution.
- Validate the prerequisites for installing SAP Data Hub.
- Install SAP Data Hub inside the NKS cluster.

2 NetApp Kubernetes Service Cluster Validation Matrix

Table 1 lists the version combinations of SAP Data Hub 2.x and the validated NKS versions.

Table 1) SAP Data Hub NetApp Kubernetes Service validation matrix.

<table>
<thead>
<tr>
<th>SAP Data Hub</th>
<th>NKS Version</th>
<th>Storage Solution</th>
<th>Storage Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.7</td>
<td>1.14</td>
<td>Trident 19.07.1 or later</td>
<td>iSCSI</td>
</tr>
<tr>
<td>2.7</td>
<td>1.15</td>
<td>Trident 19.07.1 or later</td>
<td>iSCSI</td>
</tr>
</tbody>
</table>

3 Requirements

The general sizing of the NKS environment for deploying SAP Data Hub 2.7 or later must be done according to the SAP Data Hub sizing guide.

The minimum sizing requirements for running nonproductive SAP Data Hub installations are:

- One master node, which must not run SAP Data Hub pods.
- Three worker nodes. Each worker node must be configured with 8 virtual CPUs (vCPUs) and 32GB of RAM.

The minimum sizing requirements for running productive SAP Data Hub installations are:

- One master node, which must not run SAP Data Hub pods.
- Four worker nodes. Each worker node must be configured with 16 vCPUs and 64GB of RAM.

For details regarding the minimum sizing, see the SAP document Minimum Sizing for SAP Data Hub.

3.1 Master Node

The following requirements are for the NKS master nodes:

- **NKS version**: 1.14, 1.15
- **CPU**: 4 vCPUs
- **Memory**: 16GB
- **Disk space**: 100GB for /

3.2 Worker Nodes

The following requirements are for the NKS worker nodes:

- **NKS version**: 1.14, 1.15
- **CPU**: 8 vCPUs or 16 vCPUs (depending on the SAP Data Hub use case—nonproduction or production)
3.3 NetApp Trident

The installation of SAP Data Hub on NKS was tested with Trident version 19.07.1. Therefore, Trident 19.07.1 or later must be used.

For more information about Trident and the supported NetApp back-end storage systems, see the official 
Trident product documentation.

According to the SAP note 2712050, the back-end type `ontap-nas` is not supported. Only back-end type `ontap-san` using iSCSI LUNs is supported with Trident as a storage orchestration solution.

- **SAP Data Hub back-end storage requirements:** 500GB. The storage can be thin provisioned.

3.4 NetApp StorageGRID

When you activate the SAP Data Hub checkpoint store, an object store is required. For the on-premises scenarios, NetApp StorageGRID® storage software can be used as Amazon S3 storage.

StorageGRID is available as an appliance and can also be deployed in a Kubernetes cluster. You can find details about the deployment in a Kubernetes cluster at:

- [StorageGRID/Kubernetes: Sample configuration files for Kubernetes deployments](#)
- [thePub: Deploying StorageGRID in a Kubernetes Cluster](#)

To access the Amazon S3 bucket configured in StorageGRID from SAP Data Hub, use a certificate that has been issued from an official Trust Center.

3.5 Additional SAP Data Hub Requirements

The following additional SAP Data Hub requirements must be fulfilled:

- The local [Docker registry](#) is required for storing the SAP Data Hub container images locally. In the test environment, NetApp configured the Docker registry by using Secure Sockets Layer (SSL) without user authentication. That is, users could access the Docker registry without having to enter a user name and a password. For SSL access, signed certificates (which were issued from [Let’s Encrypt](#) and automatically requested from cert-manager) were used.

  The local Docker registry must have at least 50GB of disk space.

- An appropriate Helm version must be installed; for example, 2.12.1.

- Access to SAP Service Marketplace for downloading the docker images.

3.6 Optional Components

In addition to the official required components, the following solutions were installed inside the NetApp NKS cluster, which simplified the overall installation:

- [Ingress NGINX](#)
- [cert-manager](#) using [Let’s Encrypt](#) certificates

4 Install the NetApp Kubernetes Service Cluster

The following NKS deployment options are currently available:

- Cloud environments:
- **Google Compute Engine.** The Google Compute Engine account details for deploying an NKS cluster must be configured according to the following documentation: [Google Compute Engine Credentials](#).
- **AWS.** The AWS account details for deploying an NKS cluster must be configured according to the following documentation: [Amazon Web Services (AWS) Credentials](#).
- **Microsoft Azure.** The Azure account details for deploying an NKS cluster must be configured according to the following documentation: [Azure Credentials and Permissions](#).

**On-premises scenarios:**
- **NetApp HCI.** The prerequisites for deploying an NKS cluster onto a NetApp HCI system are described in the following documentation: [Enable NKS for Your NetApp HCI Account](#).
- **VMware.** The prerequisites for deploying an NKS cluster into a VMware environment are described in the following documentation: [Register Your VMware Environment With NKS](#).
- **FlexPod®.** The prerequisites for deploying an NKS cluster onto a FlexPod storage system are described in the following documentation: [Register Your FlexPod Environment With NKS](#).

These options are presented during the deployment of NKS on NetApp Cloud Central, as shown in Figure 1.

**Figure 1) NetApp Kubernetes Service cluster deployment options.**

This section describes two NKS cluster installation options:

- To deploy the cluster on premises on a NetApp HCI system, see section 4.1, “Deploy NetApp Kubernetes Service on NetApp HCI.”
• To deploy the cluster in a public cloud service infrastructure, see section 4.2, "Deploy NetApp Kubernetes Service in Azure."

It also explains the following required configuration steps:

• To configure Trident as the storage orchestration solution, see section 4.3, “Prepare NetApp Trident and the Back-End Storage Systems.”

• To configure StorageGRID as the object store for the SAP Data Hub checkpoint store, see section 4.4, “Prepare NetApp StorageGRID.”

• To configure Helm, see section 4.5, “Install Helm.”

4.1 Deploy NetApp Kubernetes Service on NetApp HCI

To deploy NKS to an on-premises NetApp HCI system, the NetApp HCI system must be configured and registered at NetApp Cloud Central.

The screen shown in Figure 2 allows you to configure the NKS nodes that you are installing on the NetApp HCI system by clicking Edit.

Figure 2) Configuration of the NKS nodes in a NetApp HCI environment.

1. To change the configuration of the master and worker nodes, click Basic HCI Options.
2. Configure the node size by selecting the desired t-shirt size (M, L, or XL). Selecting a t-shirt size configures the number of vCPUs per virtual machine (VM) and the assigned main memory.

   **Note:** The size of the worker nodes must match the SAP Data Hub sizing, such as 8x vCPUs, 32GB of RAM for nonproduction environments.
3. Configure the hard disk size and the number of master and worker nodes. Increase the number of master and worker nodes as needed and increase the disk size of the / file system. According to the SAP sizing guidelines, the / file system should have at least 100GB. Click Save.
The configuration updates are displayed on the overview page.
4. Specify the name of the Kubernetes cluster (in this example, the proposed name was adopted) and the version of Kubernetes that is going to be installed. In this NetApp HCI example, the version is 1.14.3.

5. Click Submit to start the deployment process.
4.2 Deploy NetApp Kubernetes Service in Azure

To start an NKS deployment in an Azure environment, the credentials for the Azure environment must be configured according to the documentation Azure Credentials and Permissions.

1. Click Edit to configure the NKS nodes that you are installing in the Azure environment.

2. Click D Series. You can select an Azure predefined VM type. This machine type must match the sizing (such as 8 vCPUs and 32GB RAM for nonproduction environments) for the SAP Data Hub scenario.
In this example, the D8s v3 machine type (which determined the number of vCPUs and the size of the main memory) was chosen.
3. Configure the Azure location, resource group, virtual networks, hard disk size, number of master and worker nodes, and the size of the / file system. Click Save.
The configuration updates are displayed on the overview page.
4. Specify the name of the Kubernetes cluster (in this example, it is DataHub_Azure) and the version of Kubernetes that is going to be installed. In this Azure example, the version is 1.15.5.
5. Click Submit to start the deployment process.

4.3 Prepare NetApp Trident and the Back-End Storage Systems

Install and configure Trident according to the Trident documentation. Create a storage class with back-end type san, so that iSCSI LUNs can be created. A file system (either ext4 or xfs) must be used. In the example in “Appendix B: storage-class-basic_iscsi_ext4.yaml,” a NetApp ONTAP® SAN system was configured as the back-end system and the default format for LUNs was set to ext4. Create the storage class with kubectl create -f storage-class-basic_iscsi_ext4.yaml.

Note: If you're using xfs as the default format for new iSCSI LUNs, change fsType: ext4 to fsType: xfs in the storage-class-basic_iscsi_ext4.yaml file.

Make sure that the back-end systems are properly set up for the iSCSI protocol and that all initiator names from the NKS nodes have been added to the corresponding igroup on the back-end system. For an ONTAP based system, complete the following steps:

1. Log in to each NKS node and do the following:
   a. Edit /etc/iscsi/iscsid.conf and set node.startup = automatic.
   b. Get the initiator names and make sure that all initiator names are unique:
      cat /etc/iscsi/initiatorname.iscsi
The last line should look like this:
InitiatorName=iqn.1996-04.de.suse:01:86ce8bfdded

If the initiator names are not unique, create a new one by using the command `/sbin/iscsi-iname` and enter the new initiator name in `/etc/iscsi/initiatorname.iscsi`. If there is no initiator name in `/etc/iscsi/initiatorname.iscsi`, then execute `iscsiadm -m discovery -t st -p <IP of ONTAP iSCSI LIF>` and recheck the content of `/etc/iscsi/initiatorname.iscsi`. There should now be an initiator name inside.

c. Restart the iSCSI service by executing `systemctl restart iscsi`.

2. Make sure that iSCSI for the used storage virtual machine (SVM) is activated according to the instructions in Configuring iSCSI on an Existing SVM.

3. Use Secure Shell (SSH) to log in to ONTAP and complete the following steps:
   a. Create a trident igroup.

   ```
   igroup create -vserver <vserver> -igroup trident -protocol iscsi -ostype linux -initiator <initiator from NKS master node>
   ```

   b. Add the initiator names from all NKS worker nodes.

   ```
   igroup add trident <initiator from NKS workers>
   ```

   c. Go back to your NKS worker nodes and verify that the iSCSI discovery works by running the following command:

   ```
   iscsiadm -m discovery -t st -p <IP of ONTAP iSCSI LIF>
   ```

4.4 Prepare NetApp StorageGRID

If an SAP Data Hub checkpoint store is used, an object store is required. In this example, NetApp StorageGRID is used.

To use StorageGRID as an object store for SAP Data Hub, complete the following installation (if StorageGRID is not used an appliance) and configuration steps:

1. Use the instructions on thePub: Deploying StorageGRID in a Kubernetes Cluster to install StorageGRID in the cluster.

2. Select Manage Certificates, and make sure that the certificates being used are issued from an official Trust Center: NetApp-StorageGRID/SSL-Certificate-Configuration.

3. Following the instructions in Configuring tenant accounts and connections, configure a tenant.

4. Following the instructions in Creating an S3 bucket, log in to the created tenant and create a bucket (such as datahub).

5. Use the instructions in Creating another user's S3 access keys to define an access key; then save the generated access key and the corresponding secret.

4.5 Install Helm

To install Helm, complete the following steps:

1. Extract the downloaded Helm file (in this example, Helm version 2.12.1) and move the following files to `/usr/local/bin`:
   - helm
   - tiller

2. Create a Helm service account:
   - Create the file helm.yaml with the content described in “Appendix A: helm.yaml.”
   - Issue the following command:
3. Initialize Helm and install Tiller.

```
kubectl apply -f helm.yaml
helm init --service-account helm
```

5 Install SAP Data Hub

This section describes the installation of SAP Data Hub using two options: `install.sh` and the Software Lifecycle (SL) plug-in.

The installation of SAP Data Hub is the same regardless of whether you are using an on-premises NKS version or deploying NKS in a public cloud environment. Therefore, for all NKS deployments, the installation process is:

1. Download the SAP Data Hub 2.7 Foundation installation zip file: `DHFOUNDATION07_<Patch Level>.ZIP`.
2. Extract the zip file.

5.1 Install SAP Data Hub Using `install.sh`

To install SAP Data Hub by using `install.sh`, complete the following steps:

1. Log in to the NKS master node.
2. Set the following two environment variables:
   - `export NAMESPACE=nkslocal`
     This parameter defines the namespace for the SAP Data Hub installation in the NKS cluster.
   - `export DOCKER_REGISTRY=registry.nkslocal.com:32120`
     This parameter defines the Docker registry that will be used for storing the SAP Data Hub images locally.
3. Start the installation:
   - Change the directory to your SAP Data Hub installation source and run the following command:
     ```
     ./install.sh --pv-storage-class ontap-iscsi --vsystem-disable-load-nfs-modules
     ```
     This command starts the SAP Data Hub installation and sets the default storage class to `ontap-iscsi`.
   - If you need to specify different storage classes, run `install.sh` with the following arguments:
     ```
     ./install.sh --vsystem-storage-class ontap-iscsi --pv-storage-class ontap-iscsi --dlog-storage-class ontap-iscsi --disk-storage-class ontap-iscsi --consul-storage-class ontap-iscsi --hana-storage-class ontap-iscsi --diagnostic-storage-class ontap-iscsi --pv-storage-class ontap-iscsi --vsystem-disable-load-nfs-modules
     ```
     This command starts the SAP Data Hub installation and sets the storage classes of each component to `ontap-iscsi` as well as the default storage class.
   
   For details about possible command-line parameters, see the [SAP Data Hub 2.7 installation documentation](https://www.sap.com).
4. Specify the following parameters:
   - S-User and password
   - Host name for certificates: for example, `datahub.nkslocal.com`
   - Password: `Abcpoiuz01!`
   - Tenant name: `default`
- **Vora admin user**: voraadm
- **Vora checkpoint store**: Depending on your setup, either **Yes** or **No**
  
  If you’re using the Vora checkpoint store, and you’re using StorageGRID as the object store, specify the following additional parameters:
  
  - Type of checkpoint store: s3
  - Access key: 07UQ5IF1P156S82Z3Q3B
  - Secret: 9oH+cX805IM8LyjK1hMdQZ/pSfi2Mxzguap3P3UX
  - S3 host: [https://s3.nkslocal.com:32182/](https://s3.nkslocal.com:32182/)
  - Region: us-east-1
  - S3 bucket: datahub/

5. After the installation is complete, expose the following services (these examples use NodePort):
  
  - `vsystem`
  ```bash
  kubectl expose service -n nkslocal vsystem --type=NodePort --name=my-vsystem-nodeport
  ```
  
  - `vora-tx-coordinator-ext`
  ```bash
  kubectl expose service -n nkslocal vora-tx-coordinator-ext --type=NodePort --name=my-vora-tx-coordinator-ext
  ```
  
  - `vora-textanalysis`
  ```bash
  kubectl expose service -n nkslocal vora-textanalysis --type=NodePort --name=my-vora-textanalysis
  ```

5.2 Install SAP Data Hub Using the SL Plug-in

Log in to the NKS master node and start the installation process by completing the following steps:

1. Change the directory to your SAP Data Hub installation source.

2. Change into the subdirectory `slplugin/workdir` and execute the following command:

   ```bash
   ./setup.sh
   ```

3. Specify the following actions and settings:
   
   - Next action: `n` (for next)
   - Set the Kubernetes namespace: `nkslocal`
   - Accept the license agreement: `y`
   - Select advanced installation: `2`
   - Select not to use saved container images: `1`
   - S-User name
   - S-User password
   - Choose existing technical user: `1`
   - Container registry: `registry.nkslocal.com:32120`
   - Do not use an image pull secret: `1`

**Note**: In this example, the Docker registry was configured without the need for a user and a password.

   - Certificate domain: `datahub.nkslocal.com`
   - Password: Abcpoiuz01!
   - Tenant name: `default`
   - Username: voraadm
− Use the same password: 1
− Do not configure proxy settings: 2

4. Choose whether to enable a checkpoint store.
If you’re using the Vora checkpoint store, and you’re using StorageGRID as the object store, specify the following additional parameters:
− Type of checkpoint store: s3
− Access key: O7UQ5IF1P1568Z3Q3B
− Secret: 9oH+cX8O5IM8LyjKlhMdQZ/pSfiZMxzguap3P3UX
− S3 host: https://s3.nkslocal.com:32182/
− Region: us-east-1
− S3 bucket: datahub/

5. Type 2 to configure storage classes.
6. Specify ontap-iscsi for the default storage class.
7. Confirm ontap-iscsi for all the following storage classes:
   − System Management
   − Dlog
   − Disk
   − Consul
   − SAP HANA
   − SAP Data Hub Diagnostics

8. Specify the following:
   − Do not configure Docker container log path: 1
   − Use default registry for SAP Data Hub Modeler: 2
   − Disable loading NFS modules: 2
   − Disable network policies: 2
   − Helm timeout: 1800
   − Pod wait timeout: 500
   − No additional installation parameters

9. Start the deployment: Type n (for next).
10. After the installation is finished, expose the following services (these examples NodePort):
    − vsystem
      ```bash
kubectl expose service -n nkslocal vsystem --type=NodePort --name=my-vsystem-nodeport
```
    − vora-tx-coordinator-ext
      ```bash
      kubectl expose service -n nkslocal vora-tx-coordinator-ext --type=NodePort --name=my-vora-tx-coordinator-ext
      ```
    − vora-textanalysis
      ```bash
      kubectl expose service -n nkslocal vora-textanalysis --type=NodePort --name=my-vora-textanalysis
      ```

5.3 Troubleshooting
After uninstalling and purging an existing SAP Data Hub installation, make sure that all the persistent volumes have been deleted.
kubectl get pv | grep <SAP Data Hub namespace>

If the vsystem-application-runtime-storage persistent volume has not been deleted, remove it by running the following command:

kubectl delete pv nkslocal-vsystem-application-runtime-storage

**Appendix A: helm.yaml**

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: helm
  namespace: kube-system

---

apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRoleBinding
metadata:
  name: helm
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
  - kind: ServiceAccount
    name: helm
    namespace: kube-system
```

**Appendix B: storage-class-basic_iscsi_ext4.yaml**

```yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-iscsi
provisioner: netapp.io/trident
parameters:
  backendType: ontap-san
  fsType: "ext4"
```

**Where to Find Additional Information**

To learn more about the information that is described in this document, review the following websites:

- NetApp Kubernetes Service (NKS) documentation
- NetApp Trident documentation
- NetApp product documentation

**Version History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>February 2020</td>
<td>Initial version.</td>
</tr>
</tbody>
</table>
Refer to the [Interoperability Matrix Tool (IMT)](http://www.netapp.com/TM) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

**Copyright Information**

Copyright © 2020 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

**THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

**Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at [http://www.netapp.com/TM](http://www.netapp.com/TM) are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4817-0220