Installation 2.0.0

Installing Streams Messaging Manager

Date published: 2019-09-20
Date modified: 2019-09-20

CLOUDERA

https://docs.cloudera.com/

Legal Notice

Contents

Installation Overview

Streams Messaging Manager installation steps

You are encouraged to review this overview of Streams Messaging Manager (SMM) installation steps to get a thorough understanding of the requirements before you begin the installation process.

Before you begin

See the *Hortonworks Support Matrix* for information on the requirements for DP Platform and the SMM application.

Procedure

1. Get your software.
   - Set up a local repository.
   - Create the repository configuration file.

   Note:

   If you are installing SMM as a new component on an existing Ambari 2.7.5 managed cluster with HDP 3.1.5 and/or HDF 3.5.x, then file a support case in the Cloudera portal to get the correct version of SMM.
2. Installing SMM Application on DataPlane Platform.
   a. Set up DataPlane Platform.
      - Install or upgrade to the latest version of DataPlane Platform.
      - Configure DPS.

   b. Install the SMM application.
3. Prepare your cluster for use with SMM.
   a. Install or upgrade Ambari.
   b. Install or upgrade HDF or HDP.
   c. Set up security on your cluster.
      - (Required) Set up Ambari with AD authentication.
      - (Required) Configure Knox SSO topology.
      - (Recommended) Install Ranger and set up permissions.
      - (Recommended) Set up Kerberos for your cluster.

   d. Install the SMM REST Agent.
      - Install a database for SMM.
      - Get the DPS Knox Cert key.
      - Download and install the SMM management pack.
      - Update base URLs.
      - Add the REST Server as an Ambari Service.
      - Configure TLS for SMM.
4. Integrate your cluster and DataPlane Platform.
   a. Assign SMM users the Kafka DevOps role.
   b. Generate and upload your TLS public key.
   c. Set up Knox SSO for DataPlane Platform.
   d. Add the HDP or HDF cluster and register it with DataPlane Platform.
   e. Enable SMM Service for your target cluster.

Related Information

Hortonworks Support Matrix

HDF / HDP target cluster service requirements

These are the component services required for your SMM REST Server Agent target cluster.

Component	Purpose	Comment
SMM Rest Server Agent	Provides REST endpoints that power the SMM DP Platform Application to manage and monitor.	Installed using a separate Ambari Management Pack.
Apache Kafka	The Kafka cluster that you are managing with SMM.	Installed using HDF or HDP.
Apache ZooKeeper	ZooKeeper contains information about Kafka metadata.	
Knox	Provides SSO services from the DP Platform Application in DP Platform, to the SMM REST Server on the HDP or HDF cluster. The logged in user in DP Platform using Knox SSO connects to SMM REST Services.	Installed using HDP or HDF.
AMS	Ambari Metrics Server is a time Series and Graph database built on top of HBase. It houses all the time series Kafka Metrics that power SMM.	Installed using HDP or HDF.
AD/LDAP	Identity Provider Store that houses user and group information for users that access the system. DataPlane Platform and HDP or HDF must use the same LDAP instance.	

Obtaining necessary SMM software

SMM installation artifacts

Prior to starting installation, you must download the Streams Messaging Manager (SMM) software artifacts from the Cloudera Archive. Access instructions are provided as part of the subscription fulfillment process.

Before you begin

Make sure that you have an active subscription agreement and have your license key file ready along with the required authentication credentials (username and password).

Procedure

1. If you only have your license key, you need to obtain authentication credentials (username and password) by using the Generate Credentials function on the CDP Private Cloud Base download page.

   Skip this step if you have your username and password ready.
2. Go to the *SMM download locations* page and identify the download artifacts for your target system.
3. Use your authentication credentials to download the artifacts.

Related Information

SMM download locations

Set Up a Local Repository

Setting up a local repository involves moving the tarball to the selected mirror server and extracting the tarball to create the repository. You can use the same local repository for DP Platform, the SMM application, and the SMM REST Server, or you can create unique local repositories for each.

Before you begin

Ensure that you have downloaded the required tarballs from the customer portal, following the instructions provided as part of the product procurement process.

Procedure

1. Copy the SMM Application and SMM REST Server (Cluster Agent) tarballs to the web server directory and expand (uncompress) the archive file:
   a) Navigate to the web server directory you previously created.
   cd /var/www/html/

   All content in this directory is served by the web server.
   b) Move the tarballs to the current directory and expand each of the repository tarballs that you downloaded.

   Replace <*file-name*> with the actual name of the RPM tarball that you are expanding.

   tar zxvf <file-name>.tar.gz

   During expansion of the tarball, subdirectories are created in /var/www/html/, such as DSS/centos7SMM/centos7. These directories contain the repositories.

   Expanding the app tarball takes several seconds.

2. Confirm that you can browse to the newly created local repositories by using the base URLs: http://<*webserver-host-name*>/<*repo-name*>/<*OS*>/<*service-version-X*>
   - <webserver-host-name>

     This is the FQDN of the web server host.
   - <repo-name>

     This is composed of the abbreviated name of the repository.

     For the SMM, the repository name is SMM-APP.
   - <OS>

     This is the operating system version.
   - <service-version-X>

     This is the version number of the downloaded repository with an appended unique number.

   Base URL Examples

   Base URL:

   ```
   http://webserver.com:port/DSS/centos7/1.1.0.0-X
   ```

   Base URL for the SMM Application:

   ```
   http://webserver.com:port/SMM-APP/centos7/2.0.0.0-x
   ```

   Base URL for the SMM REST Server (Cluster Agent):

   ```
   http://webserver.com/SMM/centos7/2.0.0.0-x/
   ```

   Be sure to record these Base URLs, because you need them when installing the application on the host, and installing the associated agent on the clusters.

   Be sure to record these Base URLs, because you need them when installing the application on the host.
3. If you have multiple repositories configured in your environment, deploy the following plugin on all the nodes in your cluster.

   ```
   yum install yum-plugin-priorities
   ```
4. Edit the /etc/yum/pluginconf.d/priorities.conf file to add the following values:

   ```
   [main]
   enabled=1
   gpgcheck=0
   ```

Results

The repositories are now prepared for installation.

What to do next

Create the configuration file for the repository.

Create the Repository Configuration File

A repository configuration file must be created for the Streams Messaging Manager Service on the DP Platform host. The file is required to identify the path to the repository data, establish whether a GPG signature check should be

performed on the repository packages, etc. A unique repository configuration file is required for DP Platform and the SMM application. No configuration files is required for the SMM Rest Server.

Procedure

1. Navigate to the repository directory.
   cd /etc/yum.repos.d/
2. Create a repository file.
   vi dss-app.repo
   vi smm-app.repo

   Alternatively, you can copy an existing repository file to edit.
3. Add the following content in the repository file:
   #VERSION_NUMBER=<downloaded-version#> [<service-name-abbreviation>]

   This is composed of the service name abbreviation and version number (includes the build number). Example: SMM-APP-2.0.0.0-x

   ```
   name=<service-name-abbreviation> Version - <service-name-abbreviation>
   ```

   ```
   baseurl=http://<webserver-host-name>/<directory-containing-repo>
   ```

   <webserver-host-name> is the FQDN of the web server host that contains the repository. This is the same base URL that you used in the task to prepare the repositories.

   <directory-containing-repo> is the path expanded from the tarball.

   ```
   gpgcheck=1
   ```

   ```
   gpgkey=http://<webserver-host-name>/<directory-containing-repo>/RPM-GPG-KEY/RPM-GPG-KEY-Jenkins
   ```

   ```
   enabled=1
   ```

   ```
   priority=1
   ```

Example

Example Repository File

```
#VERSION_NUMBER=1.0.0.0-59
[DSS-APP-1.0.0.0-59]
name=DSS-APP Version - DSS-APP-1.0.0.0-59
baseurl=http://<your_webserver>:port/DSS-APP/centos7/1.0.0.0
gpgcheck=1
gpgkey=http://<your_webserver>:port/DSS-APP/centos7/1.0.0.0/RPM-GPG-KEY/RPM-GPG-KEY-Jenkins
enabled=1
priority=1
```

```
#VERSION_NUMBER=2.0.0.0-x
[SMM-APP-2.0.0.0-x]
name=SMM-APP Version - 2.0.0.0-x
baseurl=http://<your_webserver>:port/SMM-APP/centos7/2.0.0.0
gpgcheck=1
gpgkey=http://<your_webserver>:port/SMM-APP/centos7/2.0.0.0/RPM-GPG-KEY/RPM-GPG-KEY-Jenkins
```

```
enabled=1
priority=1
```

Installing Your SMM Application on DP Platform

Set up DP Platform

Before you can install Streams Messaging Manager, you must first install or upgrade to DataPlane Platform 1.2.x, and configure it according to the instructions provided in the DP Platform installation documentation.

Procedure

1. Install or upgrade to DP Platform 1.2.x.
2. Configure DP Platform.

Related Information

Installing DP Platform
Managing Clusters in DP Platform
Managing Users and Groups

Install the SMM Application

To install the Streams Messaging Manager application, you log into the DP Platform host, install your SMM application RPMs, and then load your Docker image and initialize your environment.

Before you begin

You have successfully installed DP Platform and DP Platform is running.

Procedure

1. Log in as root to the host on which you set up the DP Platform repositories.

   ```
   sudo su
   ```

2. Install the RPMs for your service application.

   ```
   yum install smm-app
   ```

   A folder is created that contains the Docker image tarball files and a configuration script.

   If the `yum` command fails, then the local repository was not set up correctly. Check the repository file /etc/yum.repos.d/smm-app.repo on the host.

3. Navigate to the directory containing the installation scripts for the service, for example:
   cd /usr/smm-app/current/streams-messaging-manager/bin

4. Load the Docker images and initialize the environment.

```
./smmdeploy.sh init
```

Loading the images might take a while.

Note:

If you run into errors while deploying, you must destroy the deployment using ./smmdeploy.sh destroy command and re-install the app. To check the logs of the container, you can use the command ./smmdep loy.sh logs.

5. Verify that the container you installed is running.
./smmdeploy.sh ps

Prepare Your Cluster for Use with SMM

Install or Upgrade Ambari, HDF, and HDP

Get started with the SMM installation by preparing your target cluster. Your cluster must be managed by Ambari 2.7.x. It can be an HDF 3.3.x, 3.4.0 or 3.4.1.1 cluster or an HDP 3.1 or 3.1.1 cluster. Additionally, an HDP 3.1 or 3.1.1 cluster with HDF 3.3.x , 3.4.0 or 3.4.1.1 services installed is also supported.

Procedure

1. Install or upgrade to Ambari 2.7.x.
2. Install or upgrade your HDF 3.3.x, 3.4.0 or 3.4.1.1 or HDP 3.1.0 or 3.1.1 cluster. You can also install HDF services on an HDP cluster.

   Review the *Target cluster service requirements* information to understand which services are required for SMM 1.2.0.

Related Information

Installing Ambari
Upgrading Ambari
Installing HDP
Upgrading HDP
Installing HDF
Upgrading HDF

Security Setup

Mandatory security configuration

Procedure

1. Set up Ambari with AD authentication.
2. Configure Knox SSO topology for Ambari.

Related Information

Configuring Ambari Authentication with LDAP/AD
Configuring Knox SSO between DP Platform and Your Cluster

Recommended security configuration

Procedure

1. Set up Kerberos for your cluster.
2. Install Ranger and set up permissions.
   For information, see *Updating Ranger Users*.
3. Set up TLS.

Related Information

Configuring Authentication with Kerberos
Installing Apache Ranger
Providing Authorization with Apache Ranger
Updating Ranger Users

Install the SMM REST admin server

Configure your SMM database

About this task

You can use the following databases with SMM:

- Postgres
- MySQL
- Oracle
- MariaDB

Procedure

1. To configure a MySQL database:

```
create database streamsmsgmgr;
CREATE USER 'streamsmsgmgr'@'localhost' IDENTIFIED BY 'streamsmsgmgr';
GRANT ALL PRIVILEGES ON streamsmsgmgr.* TO 'streamsmsgmgr'@'localhost' WIT
H GRANT OPTION;
CREATE USER 'streamsmsgmgr'@'%' IDENTIFIED BY 'streamsmsgmgr';
GRANT ALL PRIVILEGES ON streamsmsgmgr.* TO 'streamsmsgmgr'@'%' WITH GRANT
 OPTION;
```

2. To configure a Postgres database:

```
# Log in database
sudo su postgres
psql

# Setup databases and users
create database streamsmsgmgr;
CREATE USER streamsmsgmgr WITH PASSWORD streamsmsgmgr;
GRANT ALL PRIVILEGES ON DATABASE "streamsmsgmgr" to streamsmsgmgr;
```

Install the SMM management pack

A management pack (mpack) bundles service definitions, stack definitions, and stack add-on service definitions so they do not need to be included with the Ambari core functionality and can be updated in between major releases.

Before you begin

You have obtained the management pack and public repository locations from the Hortonworks . Customer Portal following the instructions provided as part of the subscription fulfillment process.

Procedure

1. Back up your Ambari resources folder:

```
cp -r /var/lib/ambari-server/resources /var/lib/ambari-server/resources.
backup
```

2. Copy the bundle to /tmp on the node where you installed Ambari.
3. Install the SMM management pack.

```
ambari-server install-mpack
--mpack=tmp/smm-ambari-mpack-2.0.0.0-<version>.tar.gz
--verbose
```

4. Restart the Ambari Server:

```
ambari-server restart
```

5. Once Ambari server is restarted, update public repo URL, Go to Stack and Versions Section on Ambari, click Versions -> Manage Versions, Click HDP or HDF version link. Update SMM link with its public repo link.

Update the SMM Base URL

Adding the base URL tells Ambari where to look for the SMM repository. The base URL will be included in the customer support portal, where you get the repository. This step is necessary because you are using an existing Ambari instance that is already managing an HDP or HDF cluster.

About this task

Update the base URL with the base URL you created for the SMM REST Server (Cluster Agent) management pack when you created the local repo. For example:

```
http://webserver.com/SMM/centos7/2.0.0.0-x/
```

Procedure

1. From the Ambari menu, click the admin drop-down on the top right of your Ambari Dashboard. Then select Manage Ambari.
2. From the Clusters view on the left, clickVersions. Then select the HDP versions or HDF versions link, depending on your cluster.
3. Add the SMM Base URL appropriate for your operating system.
4. Click Save.

Add the SMM REST Server as a Service

Once you have installed the SMM management pack and updated the Base URL in Ambari, you are ready to add the SMM Rest Server as a service in your Ambari-managed HDF or HDP cluster.

Procedure

1. From the Ambari UI, launch the Add Service Wizard.
2. In Step 1, Choose Services, select Streams Messaging Manager.
3. In Step 2, Assign Masters, add the host on which you want to install the SMM REST Server.
4. In Step 4, Customize Services, select the Streams Messaging Manager tab and add the configuration information for the SMM REST Server.
5. Click through the rest of the Add Service Wizard and click OK.

Results

You can verify the SMM installation by launching the following:

- http://{your hostname}:8585/swagger
- http://{your hostname}:8585/api/v1/admin/brokers

In both cases the default user name is admin and the default password is Horton!#works.

Configure Knox for SMM integration

Procedure

1. From the Ambari UI Advanced streams-messaging-manager-sso-config, verify that Authentication.provider.url is accurate.

   The format of the URL is as follows:

   ```
   https://<hostname>:8443/gateway/knoxsso/api/v1/websso
   ```

   For example,

   ```
   https://dw-weekly.field.cloudera.com:8443/gateway/knoxsso/api/v1/websso
   ```

2. Generate your public.key.pem.

   a. From Knox | Configs | Advanced knoxsso-toplogy, add the following:

   ```
   <name>main.ldapRealm.userDnTemplate</name>
   <value>CN=admin1,CN=Users,DC=HWQE,DC=HORTONWORKS,DC=COM</value>

   <name>main.ldapRealm.contextFactory.url</name>
   <value>ldap://ad-nano.qe.hortonworks.com:389</value>
   <name>knoxsso.redirect.whitelist.regex</name>
   <value>.*;^/.*$;https?://localhost*$;^http.*$</value>
   ```

   Note: This is an example. You must replace the key values with the values from your environment.

   b. Save this change and restart Knox.

   c. Export the Knox certificate.

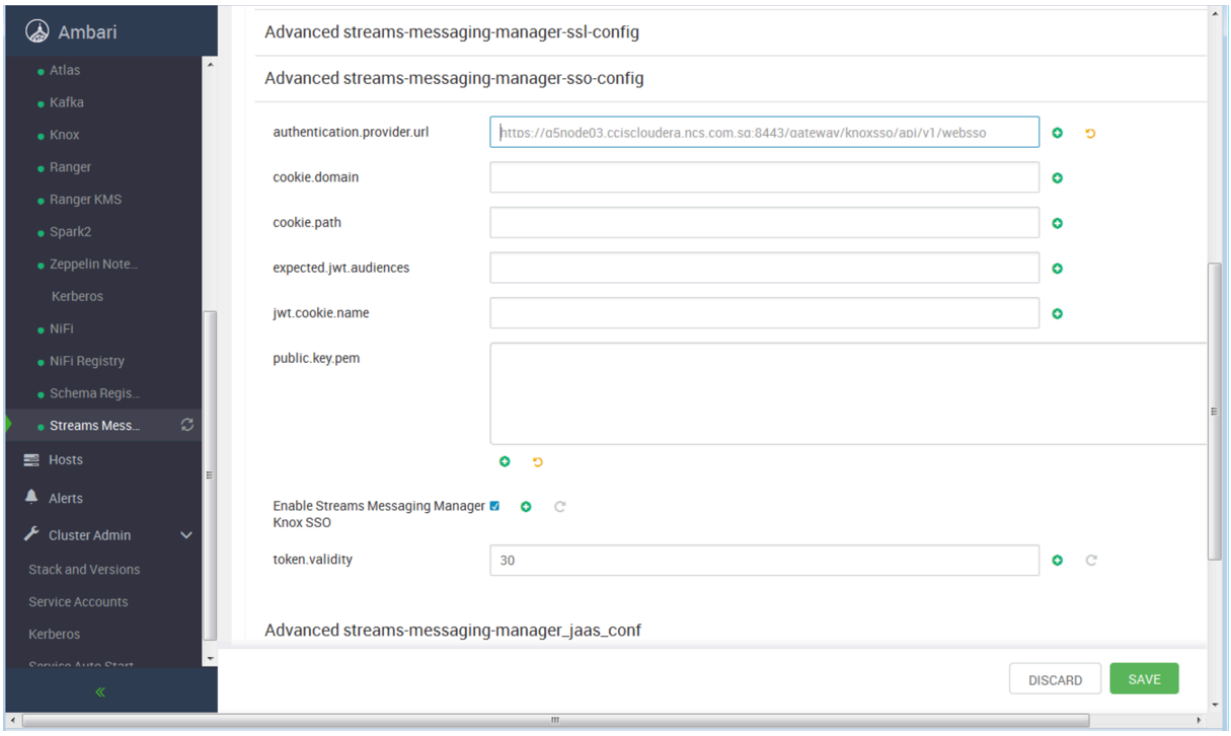
   ```
   cd /usr/hdp/current/knox-server/bin
   ./knoxcli.sh export-cert --type PEM
   [root@dw-weekly bin]# ./knoxcli.sh export-cert --type PEM
   Certificate gateway-identity has been successfully exported to: /usr/
   hdp/<HDP_version>/knox-server/data/security/keystores/gateway-identit
   y.pem
   ```

3. Open gateway-identity.pem that is created in the previous step and copy the content between ----BEGIN CERTIFICATE---- and ----END CERTIFICATE---- lines.

   For example,

```
----BEGIN CERTIFICATE----
MZrfbqou3rhoqrq
12rh13fbnjkdsfnkjef
fn123nf13unf1o3uf
----END CERTIFICATE----
```

4. From the Ambari UI Advanced streams-messaging-manager-sso-config, insert the content, which you copied in the previous step, in the public.key.pem field.



Integrating your cluster with DPS

Assign users the Kafka DevOps role

Users must be assigned the Kafka DevOps role before they can access SMM from the DP Platform UI.

Procedure

1. From the DataPlane left navigation pane, go to Users.
2. Identify the user to which you want to give SMM access, and select Edit from the Actions icon on the right-hand side.
3. Add Kafka DevOps to the roles for the user and click Save.

Results

That use is now able to access SMM from the DataPlane UI.

Upload your TLS public key

If the SMM REST endpoint on your HDF or HDP cluster is TLS enabled, you must upload the TLS public key to DPS.

Procedure

1. From the command line, enter:

```
openssl s_client -showcerts -connect <cluster-name:cluster-port>
```

2. Copy the certificate, including the begin and end lines, and save to a file named SMM.pem.
3. From the DataPlane left navigation pane, click Settings.
4. Click Upload to upload your SMM.pem file

Enable SMM Service for Target Cluster Registered in DP Platform

Procedure

1. From the DataPlane UI left navigation pane, go to Services and click the SMM application.
2. Click Enable for each cluster you want to use with SMM.

Updating Ranger Users

Before you can launch SMM, you must manually add a user to Ranger, add the user to Ranger Policies for the Kafka service, and add the SMM user to the Ranger Policy for Kafka. Additionally, if the SSL is enabled for Ranger, you must add the Ranger plugin SSL CLName configuration value.

Procedure

1. Add a User to Ranger.
   a. From the Ranger UI, go to Settings, then Users/Groups, and ensure that the Users tab is selected.
   b. Click Add New User.
   c. Provide the user name. This user name is derived from the streams_messaging_manger_principal_name you set during the Ambari Kerberos configuration. For example: streamsmsgmgr-cluster-smm.
   d. For the Role, select User. For the Group, select hadoop, streamsmsgmgr, and ranger.
   e. Click Save.
2. Add user to Ranger Policy for Kafka Service.
   a. From Ranger UI, Service Manager, in the Kafka service pane, click the hyperlink (cluster-name_kafka).
   b. Add the SMM user to both policies. Select the edit policies icon, and from Allow Conditions, add the SMM user to the Select User field. Also add sreamsmsgmgr user, if it does not already exist.
3. Add SMM user to Ranger Policy for Kafka.
   a. From the Ranger UI, Services Manager, and select the Edit icon for the Kafka service.
   b. Add the streamsmsgmgr-cluster-smm user name to the following two configuration values:
      - policy.download.auth.users
      - tag.download.auth.users

4. (If SSL is enabled for Ranger) Update the Ranger plugin SSL CLName. Go to Config Properties | Ranger plugin SSL CLName. For example: Kafka Client. The CLName is the value you set up when generating your Ranger Admin SSL certificate.

Related Information

Recommended security configuration