Cloudera Manager 7.8.1

Release Notes

Date published: 2020-11-30
Date modified: 2022-11-18

https://docs.cloudera.com/

Legal Notice

Contents

Cloudera Manager 7.8.1 Release Notes

Known issues, fixed issues and new features for Cloudera Manager 7.8.1.

What's New in Cloudera Manager 7.8.1

New features and changed behavior for Cloudera Manager 7.8.1

Cloudera Manager now supports Active Directory objects with additional attributes

Cloudera Manager now supports Active Directory objects with additional attributes other than just accountExpires and objectClass for every new account creation. You can use these additional attributes of an object to identify or search for objects in the Active Directory network using LDAP queries.

You can now start using some of the sample attributes such as employeeType, Usertype, Manager, passwordNeverExpires, etc.

Routing email alerts to different email addresses

You can now configure the alert rules in Cloudera Manager to send email alerts to various email addresses based on rules you provide for users, hosts, services, roles, and alert rules. See Alert email routing.

What's new in Installation and Upgrade for CDP Private Cloud Data Services 1.4.1

New Procedure for decommissioning ECS hosts

See Decommissioning ECS hosts.

A custom, external Docker Repository is now available for Embedded Container Service (ECS) clusters

During installation of an ECS cluster, you can select an option to use an external, custom Docker Repository that you manage in your environment. See Docker repository access.

Pre-installation validation added to ECS Installation

The following items are validated before installing the Control Plane: Jobs, service accounts, cluster role bindings, whether the KUBECONFIG file has administrator privileges, that the base cluster has the truststore setup JKS format, and tests the vault.

Hosts are now inspected before creating an ECS cluster

The following items are now inspected:

- GPU
- Supported Operating System
- Storage
- CPU
- Required ports are available

Warnings are displayed in the Host Inspector during ECS installation if any of the inspections return unsatisfactory results.

Fixed Issues in Cloudera Manager 7.8.1

Fixed issues in Cloudera Manager 7.8.1

Cloudera Bug: OPSAPS-64580: Control Plane installation is failing because of failure in Install Longhorn UI step

Fixed an issue where, 0ccasionally, the Install Longhorn UI step failed due to a race condition.

OPSAPS-65365 Do not use the $ character while in the password for the custom Docker Repository for ECS installations.

Ensure that the $ character is not part of the Docker Repository password.

Fixed issues for Installation and upgrade for CDP Private Cloud Data Services 1.4.1

Cloudera Bug: OPSAPS-64580: Control Plane installation is failing because of failure in Install Longhorn UI step

Fixed an issue where, occasionally, the Install Longhorn UI step failed due to a race condition.

Cloudera Bug: OPSX-2926: Mismatch in expected number of docker images in copy script

Previously, the total number of images were calculated incorrectly.

As a result, the copy docker images script thinks that not all images were processed whereas all images actually were processed. As a result, the folder where the images were temporarily placed would not be deleted.

Subsequently running the same script on the same machine, but to a second destination, the docker repository will reuse the same temp folder and skip all those docker images, and as a result, the required docker images will not be present in the second docker repository.

Cloudera Bug: OPSX-3031: Don't reset the index counter when handling packages

During the docker image copying process, some of the indices (49/200, 50/200, etc) were off. This is cosmetic.

Cloudera Bug: OPSX-3068: Pods fail to start in Embedded Container Service (ECS) clusters.

Fixed a timing issue that caused the pods to fail to start.

Cloudera Bug: OPSX-3530:Copying images to the external Docker registry failed on OpenShift Container Platform (OCP) deployments.

Known Issues in Cloudera Manager 7.8.1

Known issues in Cloudera Manager 7.8.1

Known Issues for Installation and Upgrade of CDP Private Cloud Data Services 1.4.1

OPSAPS-67152: Cloudera Manager does not allow you to update some configuration parameters.

Cloudera Manager does not allow you to set to "0" for the dfs_access_time_precision and dfs_name node_accesstime_precision configuration parameters.

You will not be able to update dfs_access_time_precision and dfs_namenode_accesstime_precision to "0". If you try to enter "0" in these configuration input fields, then the field gets cleared off and results in a validation error: This field is required.

To fix this issue, perform the workaround steps as mentioned in the KB article.

If you need any guidance during this process, contact Cloudera support.

Cloudera bug: OPSAPS-59764: Memory leak in the Cloudera Manager agent while downloading the parcels.

When using the M2Crpyto library in the Cloudera Manager agent to download parcels causes a memory leak.

The Cloudera Manager server requires parcels to install a cluster. If any of the URLs of parcels are modified, then the server provides information to all the Cloudera Manager agent processes that are installed on each cluster host.

The Cloudera Manager agent then starts checking for updates regularly by downloading the manifest file that is available under each of the URLs. However, if the URL is invalid or not reachable to download the parcel, then the Cloudera Manager agent shows a 404 error message

and the memory of the Cloudera Manager agent process increases due to a memory leak in the file downloader code of the agent.

To prevent this memory leak, ensure all URLs of parcels in Cloudera Manager are reachable. To achieve this, delete all unused and unreachable parcels from the Cloudera Manager parcels page.

OPSAPS-65365 Do not use the $ character in the password for the custom Docker Repository for ECS installations.

Ensure that the $ character is not part of the Docker Repository password.

OPSX-2713: PVC ECS Installation: Failed to perform First Run of services.

If an issue is encountered during the Install Control Plane step of ECS Cluster First Run, installation will be re-attempted infinitely rather than the command failing.

Since the control plane is installed and uninstalled in a continuous cycle, it is often possible to address the cause of the failure while the command is still running, at which point the next attempted installation should succeed. If this is not successful, abort the First Run command, delete the Containerized Cluster, address the cause of the failure, and retry from the beginning of the Add Cluster wizard. Any nodes that are re-used must be cleaned before re-attempting installation.

OPSX-3359: ECS Upgrade failure

You may see the following error message during the Upgrade Cluster > Reapplying all settings > kubectl-patch step:

```
kubectl rollout status deployment/rke2-ingress-nginx-controller -
n kube-system --timeout=5m
error: timed out waiting for the condition
```

If you see this error, do the following:

1. Check whether all the Kubernetes nodes are ready for scheduling. Run the following command from the ECS Server node:

   ```
   kubectl get nodes
   ```

   You will see output similar to the following:

   ```
   NAME STATUS ROLES AGE VERSION
   <node1> Ready,SchedulingDisabled control-plane,etcd,master 103
   m v1.21.11+rke2r1
   <node2> Ready <none> 101m v1.21.11+rke2r1
   <node3> Ready <none> 101m v1.21.11+rke2r1
   <node4> Ready <none> 101m v1.21.11+rke2r1
   ```

2. Run the following command from the ECS Server node for the node showing a status of Sche dulingDisabled:

   ```
   kubectl uncordon
   ```

   You will see output similar to the following:

   ```
   <node1>node/<node1> uncordoned
   ```

3. Scale down and scale up the rke2-ingress-nginx-controller pod by running the following command on the ECS Server node:

   ```
   kubectl delete pod  rke2-ingress-nginx-controller-<pod number>
    -n kube-system
   ```

4. Resume the upgrade.

OPSX-3547: ECS upgrade is taking 10+ hours to complete on 25 nodes cluster

The worst case scenario in rolling restart during upgrade takes around 24 minutes per node on clusters with 25 nodes.

During the upgrade, If you see that the stop operation on a single node takes longer than 25 minutes or starting a node takes longer than 10 minutes, you can configure Cloudera Manager to reduce the default timeouts by decreasing the value of the timeout parameters listed below to speed up the upgrade. (To change the configuration In the Cloudera Manager Admin Console, go to the ECS service, click the Configuration tab, and search for the parameter.)

The stop operation on a single node has the following steps:

- Graceful drain of the node

  This process has a default timeout of 10 minutes, controlled by the Cloudera Manager configuration parameter DRAIN_NODE_TIMEOUT.
- Non-graceful drain of the node

  This process has a default timeout of 10 minutes, controlled by the Cloudera Manager configuration parameter DRAIN_NODE_TIMEOUT.
- Wait for the workloads to spawn on other nodes in the cluster.

  This process has a default timeout of 10 minutes, controlled by the Cloudera Manager configuration parameter WAIT_TIME_FOR_NODE_READINESS.

The start operation has the following steps:

- Uncordon the node

  There is no timeout parameter for this step.
- Wait for the workloads to spawn on the node

  This process has a default timeout of 10 minutes, controlled by the Cloudera Manager configuration parameter WAIT_TIME_FOR_NODE_READINESS.

OPSX-3550 Incorrect status on CDP Private Cloud Data Services services page in the Cloudera Manager Admin Console while ECS is upgrading

The Cluster page might show that the Upgrade failed while an upgrade is in progress.

Please check the Upgrade Command for the status of the upgrade. The Cluster page will reflect the new version once the upgrade command is complete.

OPSX-735: Kerberos service should handle Cloudera Manager downtime

The Cloudera Manager Server in the base cluster must be running in order to generate Kerberos principals for Private Cloud. If there is downtime, you may observe Kerberos-related errors.

Resolve downtime on Cloudera Manager. If you encountered Kerberos errors, you can retry the operation (such as retrying creation of the Virtual Warehouse).