Using Kerberos Credential Cache

Atscale provides support for Kerberos Credential Cache file with the CDP platform. Consider the following:

- ▲ You can use either Kerberos Credential Cache or Keytab file, but not both at the same time.
- ▲ When communication between AtScale and Hadoop cluster is based on Credential Cache file, no keytab or password is required for AtScale service account principal.
- ▲ AtScale service account principal password is only a requirement for Tableau client connection based on Kerberos Credentials. In that case AtScale acts as a SASL Server and needs to obtain a private key using the password provided.



Note: For more information on setting up Kerberos with a Keytab file, see Configuring Kerberos.

Before You Begin

Make sure all of the following conditions are met:

- ◆ CDP is added as a data warehouse; for details, see Adding Hadoop Data Warehouses.
- ▲ You can log in to the AtScale host as the atscale user.
- ▲ The Kerberos Credential Cache file is created and maintained on the AtScale host; for high-availability installation, it should be available on both Engine nodes.



Note: AtScale only tests and supports Credential Cache based on a 3-part Kerberos principal.

▲ The Kerberos Credential Cache file is readable by the ATSCALE_USER (by default atscale).

Procedure

1. Check that the Kerberos Credential Cache file is available.

In the examples below, assuming the file is: /home/atscaler/kerberos/krb5cc_atscaler

- 2. As atscale user, confirm the Credential Cache file is valid using the following command: klist -c /home/atscaler/kerberos/krb5cc_atscaler -fea
- 3. In case Kerberos was already set up with a Keytab file, remove the keytab entry from the kerberos section of the atscale.yaml file.
- 4. Add the following entries to the kerberos section of the atscale.yaml file:

1

- 1. Set enabled to true.
- 2. In the cache section, set enabled to true.
- 3. In the cache section, set file to the path to the Kerberos Credential Cache file.
- 4. Set principal to the Kerberos principal string assigned to AtScale by your system administrator. This would be the principal for which the Kerberos Cache file is created.

Here is an example:

kerberos:
enabled: true
cache:
enabled: true
file: "/home/atscaler/kerberos/krb5cc_atscaler"
principal: "atscale/instanceIdentifier@REALM"

5. Run the configurator.sh tool with the --apply option to apply the new configuration:

su - atscale cd /opt/atscale/versions/<package_version> ./bin/configurator.sh --apply

- 6. Log in to the Design Center, go to Settings > Engine, and set KERBEROS.SERVICE.PASSWORD to the password of AtScale service account principal. AtScale Engine restart is needed after setting the password. For high-availability cluster, AtScale Engine needs to be restarted on both nodes.
- 7. Complete the Kerberos setup as described in the Next Steps section.