CCP Setting Up Knox SSO 2.0.1

Installing and Setting Up Knox SSO

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

Contents

Knox Overview

Apache Knox is a REST API and Application Gateway for the Apache Hadoop Ecosystem. Knox acts as a reverse proxy for all UIs and the REST application. You can use Knox for its proxying and authentication services.

Knox provides several security benefits:

- All requests go through Knox so same-origin browser restrictions are not a concern.
- Knox, in combination with a firewall, can restrict traffic to always go through Knox. This greatly reduces the security attack surface area of the UIs and REST application.
- Knox provides access to other common Apache Hadoop services.
- Knox provides a single sign on experience between the UIs and REST application.
- All requests can be protected and secured.

Knox Security

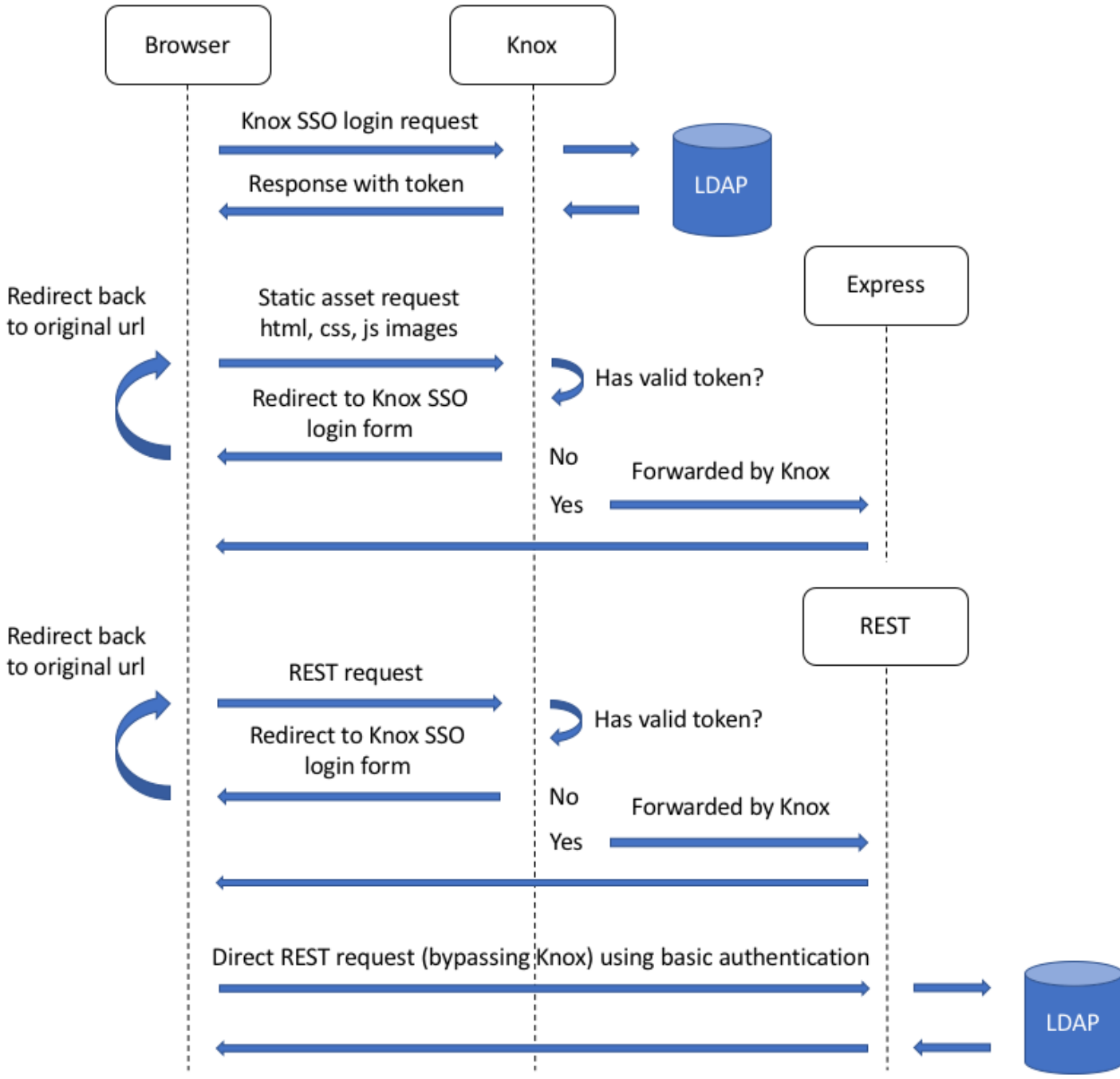
With Knox enabled, Knox now handles authentication when accessing the UIs and REST together. Basic authentication is still an option for making requests directly to the REST application. Any request to the UIs must go through Knox first and contain the proper security token.

If a valid token is not found, Knox will redirect to the Knox SSO login form. Once a valid token is found, Knox will then redirect to the original url and the request will be forwarded on. Accessing the REST application through Knox also follows this pattern. The UIs make REST requests this way with Knox enabled since they no longer depend on Express to proxy requests. The context path now determines which type of request it is rather than the host and port.

REST still requires authentication so a filter is provided that can validate a Knox token using token properties and a Knox public key. The REST application also supports Basic authentication. Since both Knox and the REST application should use the same authentication mechanism, LDAP authentication is required for the REST application.

Roles are mapped directly to LDAP groups when Knox is enabled for REST. LDAP group names are converted to upper case and prepended with ROLE_. For example, if a user's groups in LDAP were user and admin, the corresponding roles in REST with Knox enabled would be ROLE_USER and ROLE_ADMIN.

The following diagram illustrates the flow of data for the various types of requests when Knox is enabled:



Note how the flow diagrams for Static asset requests and Rest requests (through Knox) are identical.

Installing Knox

You can install Knox for Cloudera Cybersecurity Platform (CCP) with Ambari. The Knox service option is available through the Add Service wizard after CCP is installed.

Procedure

1. Login to Ambari at http://$AMBARI_HOST:8080.
2. In the left navigation menu, click **Actions**, then select **Add Service**.
3. On the **Add Service Wizard** page, select **Knox**, then click **Next**.
4. You are prompted to Assign Masters. Make a note of the Knox Gateway host(s) for use in subsequent installation steps. Click **Next**.
5. Enter a password in the **Knox Master Secret** field, then click **Next**.
6. Confirm the Ambari recommended changes for your dependent configuration, then click **OK**.
7. Click **Deploy**.

Setting Up Knox SSO

You can set up Knox to handle authentication when you access the user interfaces and REST APIs. After you set up Knox, basic authentication is still an option for making requests directly to the REST application, but any request to the user interfaces must go through Knox first and contain the proper security token.

Before you begin

- Ensure that you have enabled LDAP on the Metron **Security** page in Ambari. Knox and Metron must be configured to use the same LDAP.
- Ensure that you have installed the Metron client component on all Knox gateway hosts.

Procedure

1. Navigate to **Ambari > Hosts > $METRON_HOST**.
2. At the bottom of the **Components** section, in the dropdown menu next to the clients, select Install clients, then click Confirm Add.
3. Select **Metron Client**, then click **Next**.

   This will install the Metron client.
4. Retrieve the Knox public key by running the following command on the Knox gateway host:

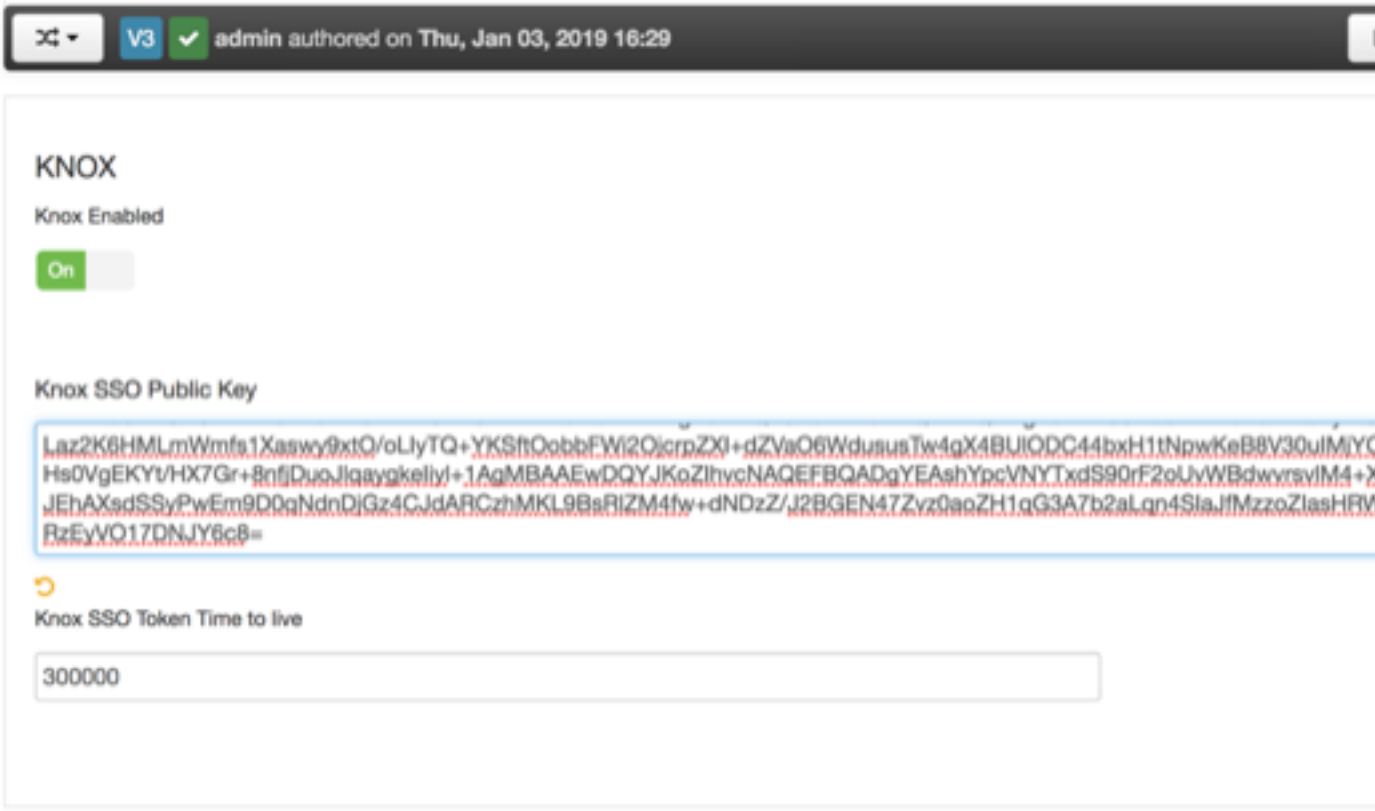
   ```
   openssl s_client -connect node1:8443 < /dev/null | openssl x509 | grep -v
    'CERTIFICATE' | paste -sd "" -
   ```

   They Knox public key will be similar to the following:

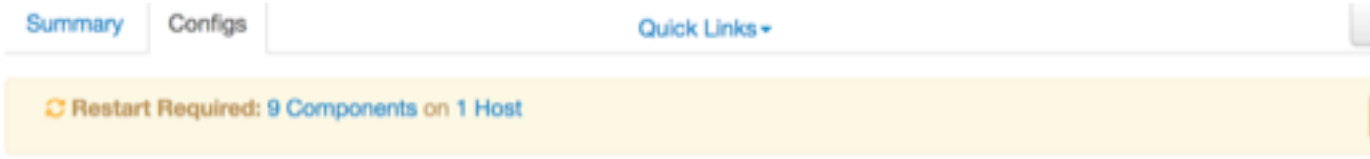
   ```
   MIICMjCCAZugAwIBAgIJAPvF9X/
   Tm9+4MA0GCSqGSIb3DQEBBQUAMFsxCzAJBgNVBAYTAlVTMQ0wCwYDVQQIEwRUZXN0MQ0wCwYDVQQHEwRUZXN0
    8wDQYDVQQKEwZIYWRvb3AxDTALBgNVBAsTBFRlc3QxDjAMBgNVBAMTBW5vZGUxMB4XDTE5MDEwMzIyMDExN1
    MCVVMxDTALBgNVBAgTBFRlc3QxDTALBgNVBAcTBFRlc3QxDzANBgNVBAoTBkhhZG9vcDENMAsGA1UECxMEVG
    KoZIhvcNAQEBBQADgY0AMIGJAoGBAJVkl8kYk2tPNJ9hlO+mSbgTAlkma7LGY4X/
   LtHqNd7PP161p9Hhty2HRpfZ5rUE2rIdlHpESSoo3Ifg38JrN745/yrw
    EGI0A5KhqOnNKw6Hk8mhoyoc8DDBVd3+nsGIJ5263rapOtyPWgxuj2gcd14utMvZOTGkHGkpr/
   FFRjUDAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAMyL+JHBfBIg2i
    AxmkOkH30iEVen1SgNqMoD4zApnA5z
   +ZVmL6cA72eV0BXjjY0YsxnVcAR4zqWYUDjZCNsAI4TtkXzlSZAhaVKzM+Ru+e
   +L5Lo22d5U5T5SqZMrubPx1dyyKe
    FMJPbG4ZGs5XbK+GAS3LDqBYEm5ZiEZ0E3RUT0=
   ```

5. Copy the output of the command and paste it into the Ambari setting at **Metron > Configs > Security > Knox SSO Public Key**.

   Note: Make sure that LDAP is enabled at the top of the **Security** tab window.



6. Enable Knox, then click **Save**.
7. Click the **Restart** menu to restart the Metron client, Metron REST, Metron Alerts UI, and Metron Management UI.



After REST comes back up, Metron should be enabled for Knox.

What to do next

When you launch a user interface, Knox searches for a valid token. If a valid token is not found, Knox redirects to the Knox SSO login form. Once a valid token is found, Knox redirects to the original url and forwards the request. Accessing the REST application through Knox also follows this pattern.