CDP Public Cloud Management Console

Fine-grained access control for ADLS Gen2

Date published: 2019-08-22
Date modified:

https://docs.cloudera.com/

Legal Notice

Contents

Introduction to RAZ on Azure environments

Shared Data Experience (SDX) in CDP Public Cloud provides Ranger Authorization Server (RAZ) service for fine grained access control and auditing of various services and workloads running in Enterprise Data Cloud. To use RAZ server capabilities, you must first enable RAZ in an Azure environment in CDP Public Cloud.

CDP Public Cloud defaults to using cloud storage which might be challenging while managing data access across teams and individual users. The Ranger Authorization Service (RAZ) resolves this challenge by enabling ADLS Gen2 users to use fine-grained access policies and audit capabilities available in Apache Ranger similar to those used with HDFS files in an on-premises or IaaS deployment.

Prior to the introduction of RAZ, controlling access to ADLS Gen2 could be enforced at coarse-grained group level (using IDBroker mappings). This required rearchitecting the implementation of important file-centric activities as well as admin-level access to both the Azure subscription and CDP account.

In HDP and CDH deployments, files and directories are protected with a combination of HDFS Access Control Lists (ACLs) (in CDH, HDP) and Ranger HDFS policies (in HDP). Similarly, in an Azure CDP Public Cloud environment with RAZ for ADLS Gen2 enabled, Ranger's rich access control policies can be applied to CDP's access to ADLS Gen2 containers, directories, and files and can be controlled with admin-level access to CDP alone.

Important: It is recommended that you do not setup IDBroker mapping for workload users in a RAZ-enabled Azure environment.

Supported use cases for RAZ in Azure environments

Many of the use cases that RAZ for Azure enables are cases where access control on files or directories is needed. Some examples include:

- Per-user home directories.
- Data engineering (Spark) efforts that require access to cloud storage objects and directories.
- Data warehouse queries (Hive/Impala) that use external tables.
- Access to Ranger's rich access control policies such as date-based access revocation, user/group/role-based controls, along with corresponding audit.
- Tag-based access control using the classification propagation feature that originates from directories.

The core RAZ for Azure for Data Lakes and several Data Hub templates are available for production use. The following Data Hub cluster types are supported:

- Data Engineering
- Data Engineering HA
- Data Engineering Spark3
- Operational Database with SQL

Specifically, Hive, Spark, HBase, and Oozie are supported.

RAZ is fully integrated with the following CDP data services:

- Cloudera Data Flow (CDF)
- Cloudera Data Engineering (CDE)
- Cloudera Machine Learning (CML)
- Cloudera Operational Database (COD)

You can backup and restore the metadata maintained in the Data Lake services of RAZ-enabled environments. For more information, see Data Lake Backup and Restore.

Important: Integrations with some components are under technical preview or has limited availability. Contact your account team before you use RAZ for your production use cases.

Limitations to use RAZ in Azure environments

The following limitations and known issues have been identified and are under development:

- Currently, there is no automated way to enable RAZ in an existing CDP environment that does not have RAZ enabled.
- RAZ integration is under technical preview for the following CDP services:
  - Cloudera Data Warehouse (CDW)
  - Integration with Data Hub Hue's File Browser
- Solr, Kudu, and NiFi are not supported by RAZ.

Prepare to register RAZ-enabled Azure environment

Before you register a RAZ-enabled Azure environment in CDP Public Cloud, you must ensure that the cloud provider prerequisites are in place.

The RAZ service consists of RAZ client and RAZ server. The RAZ client is integrated into the HDFS driver. The Azure environment in CDP Public Cloud can use the RAZ client and RAZ server capabilities after you register the RAZ-enabled Azure environment.

The Azure prerequisites for a RAZ-enabled Azure environment are described in the Azure requirements. When meeting these prerequisites, ensure that you do the following:

- Pre-create a resource group on Azure.

  Using resource groups created by CDP with a RAZ-enabled environment is not supported. See Resource groups.
- Create a designated Ranger RAZ managed identity as described in the Minimum setup for cloud storage and in Creating Ranger RAZ managed identity for RAZ-enabled Azure environment on page 5. You can optionally create a custom policy for the Ranger RAZ managed identity.

Creating Ranger RAZ managed identity for RAZ-enabled Azure environment

In addition to creating the required managed identities, you should create an additional managed identity named Ranger RAZ for RAZ-enabled Azure environment. You can also optionally create a custom role that can be used instead of Storage Blob Data Owner.

About this task

You can create the required managed identities as described in Minimal setup for cloud storage, and then create the following managed identity to use RAZ in Azure environment.

Managed identity	Managed identity is used for	Roles to assign to the managed identity
Ranger RAZ	Storage Account	• Storage Blob Data Owner or equivalent Creating custom role to use in RAZ-enabled Azure environment on page 6 • Storage Blob Delegator

Procedure

1. Perform the following steps to create the *Ranger RAZ* managed identity using Azure Portal:
   a) On Azure Portal, navigate to Managed Identities.
   b) Click +New.
   c) Select the Resource group used for CDP.
   d) Select your environment's Region.
   e) Specify managed identity Name. For example, Ranger RAZ.
   f) Provide tags if required by your organization.
   g) Click Review + create.
2. Perform the following steps to assign the two roles to the *Ranger RAZ* managed identity on the scope of the storage account created for CDP:
   a) In your Azure Portal, navigate to the Storage accounts *[***your storage account***]* Access Control (IAM) page.
   b) Click +Add Add role assignment .
   c) In the Add role assignment section, choose the following options:
      1. Select Storage Blob Data Owner as Role.
      2. Select User assigned managed identity as Assign access to.
      3. Select the Ranger RAZ managed identity that you created earlier.
      4. Click Save.
   d) To assign the Storage Blob Delegator role to *Ranger RAZ* managed identity, repeat steps a through c.

Creating custom role to use in RAZ-enabled Azure environment

Your Azure administrator can optionally create a custom role in the Azure subscription that can be used instead of Storage Blob Data Owner in a RAZ-enabled Azure environment.

Procedure

The Azure administrator can optionally create a custom role with required permissions to use instead of Storage Blob Data Owner. This role can be used to register a RAZ-enabled Azure environment and to create Data Hubs and Operational Databases using the following policy definition:

```
{
   {
        "properties": {
            "roleName": "Cloudera CDP Storage Authorization",
            "description": "Provide privileges that Cloudera CDP requires f
or storage access",
            "assignableScopes": [
            "/subscriptions/abce3e07-b32d-4b41-8c78-2bcaffe4ea27"
            ],
            "permissions": [
                {
                    "actions": ["Microsoft.Storage/storageAccounts/blobSer
vices/generateUserDelegationKey/action"],
                    "notActions": [],
                    "dataActions": ["Microsoft.Storage/storageAccounts/blobS
ervices/containers/blobs/manageOwnership/action",
                    "Microsoft.Storage/storageAccounts/blobServices/contai
ners/blobs/modifyPermissions/action",
                    "Microsoft.Storage/storageAccounts/blobServices/contai
ners/blobs/read",
                    "Microsoft.Storage/storageAccounts/blobServices/contai
ners/blobs/write",
```

```
                    "Microsoft.Storage/storageAccounts/blobServices/conta
iners/blobs/delete",
                    "Microsoft.Storage/storageAccounts/blobServices/contain
ers/blobs/move/action"
                            ],
                    "notDataActions": []
                }
            ]
        }
    }
```

Registering a RAZ-enabled Azure environment

You can use the CDP web interface or CDP CLI to register a RAZ-enabled Azure environment.

You can enable RAZ on the latest available version of Cloudera Runtime. The minimum Cloudera Runtime version supporting RAZ for Azure environments is 7.2.11.

When you register an Azure environment, enable the Fine-grained access control on ADLS Gen2 option, and then provide the managed identity that you created earlier.

After you implement RAZ by registering the RAZ-enabled Azure environment, the following RAZ authorization steps are completed by the RAZ server automatically:

1. Coordinates with IDBroker to generate and cache the user delegation token.
2. Updates the cached user delegation token periodically.
3. Authorizes the collated information from the RAZ client. When an action is performed on a given cloud storage or path, the RAZ client collates the information and sends it to the RAZ server for further processing.

The RAZ server generates the responses based on the requests.

The following table lists the request and the response generated by the RAZ server for the request:

Request	Response
Allowed	RAZ server responds with a DSAS token. HDFS driver uses this token information to access cloud storage or path. For more information about the request, login to Ranger Admin UI and check the access audit reports.
Denied	RAZ server returns **Access denied** response.
Not Determined	RAZ server responds with a DSAS token only if the RAZ service is configured to fallback. Otherwise, the RAZ server returns an **Access denied** response.
Server failed	If RAZ failed to process a request, the **RAZ server failed to process the request** error appears.

Using CDP UI to register RAZ-enabled Azure environment

Once you've met the Azure cloud provider requirements, register your Azure environment in CDP.

Before you begin

This assumes that you have already fulfilled the environment prerequisites described in Azure requirements.

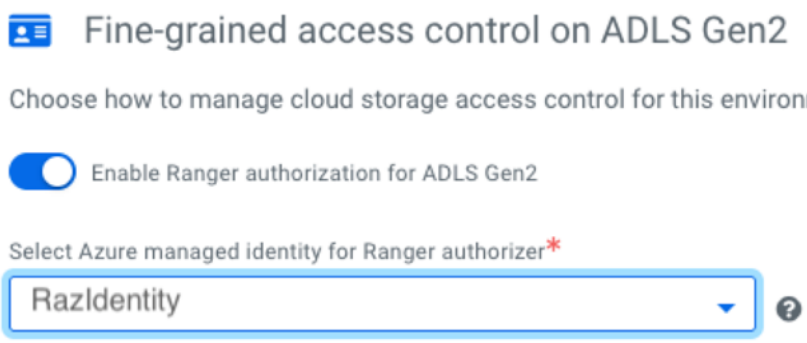
Required role: EnvironmentCreator

Procedure

1. Log in to the CDP web interface.

2. Navigate to the Management Console Environments Register environment page.
3. On the Register Environment page, provide the following information:
   a) Enter an Environment Name.
   b) Select a provisioning credential.
4. Click Next.
5. On the Data Access and Data Lake Scaling page, provide the following information:
   a) Enter a Data Lake Cluster Name.
   b) Make sure to select Runtime 7.2.11 or a higher version from the Data Lake version drop-down menu.
   c) In the Data Access and Audit section, provide your data storage location and managed identities created for minimal setup for cloud storage.
   d) In the Fine-grained access control on ADLS Gen2 section, click on the toggle button to enable Ranger authorization for ADLS Gen2 and select the managed identity created for RAZ.

      The following image shows the Fine-grained access control on ADLS Gen2 section where you can enable the Ranger authorization for ADLS and choose an Azure managed identity for Ranger authorizer:



6. Click Next.
7. On the Region, Networking and Security page, provide the following information:
   a) Select the region.
   b) Select an existing resource group. Creating new resource groups is not supported.
   c) Select the network, security groups, and provide an SSH key. If required, add tags.
8. Click Next.
9. On the Storage page, provide your logs storage location and managed identities created for minimal setup for cloud storage.
10. Click Register Environment to trigger environment registration.

Using CDP CLI to register RAZ-enabled Azure environment

You can use the CDP CLI to register a RAZ-enabled Azure environment. You must download and install beta CDP CLI, and then use CDP CLI commands to register a RAZ-enabled Azure environment.

Procedure

1. To install beta CDP CLI, see Installing Beta CDP CLI.
2. To register a RAZ-enabled Azure environment, use the --ranger-cloud-access-authorizer-role *[***RAZ_IDENTITY***]* CDP CLI command.

   If you have CDP CLI templates to create an Azure environment, modify them by adding the additional parameter required for RAZ.

   The additional option is highlighted in the following sample snippet:

```
cdp environments create-azure-environment \
--environment-name [***ENVIRONMENT_NAME***] \
```

```
--credential-name [***CREDENTIAL_NAME***] \
--region [***REGION***] \
--security-access cidr=[***YOUR_CIDR***] \
--public-key [***SSH_PUBLIC_KEY***] \
--log-storage [***LOG_STORAGE_CONFIGURATION***]\
--use-public-ip
--resource-group-name [***EXISTING_RESOURCE_GROUP***]

cdp environments set-id-broker-mappings \
--environment-name [***ENVIRONMENT_NAME***] \
--data-access-role [***DATA_ACCESS_IDENTITY***]\
--ranger-audit-role [***RANGER_AUDIT_IDENTITY***] \
--ranger-cloud-access-authorizer-role [***RAZ_IDENTITY***] \
--set-empty-mappings

cdp datalake create-azure-datalake \
--datalake-name [***DATALAKE_NAME***] \
--environment-name [***ENVIRONMENT_NAME***] \
--cloud-provider-configuration [***STORAGE_LOCATION_BASE_CONFIGURATION***]
 \
--enable-ranger-raz
```

Note: You can obtain CDP CLI commands for environment creation from CDP CLI help on CDP web interface. For more information, see Obtain CLI commands for registering an environment.

Cluster templates available in RAZ-enabled Azure environment

After your Azure environment is running, use the usual steps to create Data Hub clusters to use in a RAZ-enabled Azure environment. You can create custom variants of these templates in a RAZ-enabled Azure environment.

The following cluster templates have been tested and can be used in a RAZ-enabled Azure environment:

- Data Engineering
- Data Engineering HA
- Data Engineering Spark3
- Data Mart
- Operational Database with SQL

Configuring Data Mart for RAZ-enabled Azure environment

The Data Mart template provides a ready to use, fully capable, standalone deployment of Impala. To use a Data Mart cluster in a RAZ-enabled Azure environment, you need to configure additional Data Mart configuration steps in the Data Mart for Azure cluster definition.

Procedure

1. Log in to the Cloudera Manager for the Data Mart.

2. Select Impala Configuration , and then set the value of the Impala Daemon Data Cache Per Directory Capacity property to 10 GB.

   This property must be set to avoid the following Impala Daemon start failure:

   ```
   F0615 07:11:40.206655 62270 impalad-main.cc:73] Insufficient space for /
   hadoopfs/fs1/impala/datacache.
   Required 130.00 GB. Only 29.53 GB is available
   . Impalad exiting.
   ```

3. Create a Ranger ALDS policy in the cm_adls service with the following properties:

   Note that the following property values are sample values. You can enter the values as required for your environment.

   - Storage Account *= mpdsasv2san
   - Storage Account Container * = data
   - Relative Path * = /
   - Recursive = ON
   - User = impala
   - Permissions = read, add, create, write, delete, list, move, superuser

   This policy must be created to avoid the following failure:

   ```
   E0615 07:58:02.019865 71092 impala-server.cc:383] Could not read the root
    directory at abfs://data@mpdsasv2san.dfs.core.windows.net/mp-dsasv2-dm.
    Error was:
   Failed to acquire a SAS token for list on / due to org.apache.hadoop.se
   curity.AccessControlException: org.apache.ranger.raz.intg.RangerRazExcep
   tion: request failed: status=403
   ```

4. Restart the Impala service in Cloudera Manager, then verify that the Ranger Azure authorization is working as expected.

Ranger policies for RAZ-enabled Azure environment

Ranger enables you to configure resource-based services for Hadoop components and add access policies to those services. Ranger includes a set of preloaded resource-based services and policies which you can use in a RAZ-enabled Azure environment.

For more information, see Preloaded resource-based services and policies

Troubleshooting for RAZ-enabled Azure environment

This section includes FAQs, and discusses some common errors that might occur while using a RAZ-enabled Azure environment and the steps to resolve the issues.

How do I view logs and RAZ configuration in a RAZ-enabled Azure environment?

You can use the following methods to view logs and RAZ configuration in a RAZ-enabled Azure environment:

- To view RAZ server logs, perform the following steps:
  1. Identify the host on which the RAZ service is installed in Cloudera Manager.
  2. SSH to log into the RAZ server.
  3. Locate the ranger-raz-*[***host-name***]*-*-rangerraz.log file in the /var/log/ranger/raz/ directory.
- To view the RAZ client logs, go to the respective component logs.

  RAZ authorization is triggered when a CDP Public Cloud service accesses the ADLS storage through the HDFS client layer. The logs related to these calls are stored by the respective service or component logs.

  The following table lists some services and the RAZ client log location:

Service	RAZ client log location
HiveServer2	/var/log/hive/ folder. The associated HS2 and HMS logs in this directory provide the details about the Apache RAZ client calls.
YARN MapReduce Hive on Tez Spark	After the job run, you can locate the RAZ client logs in the corresponding application log. The Resource Manager creates the application log. You can access the logs through Resource Manager or use YARN command line tools.

- To view RAZ server configuration, perform the following steps:
  1. Identify the host on which the RAZ service is installed in Cloudera Manager.
  2. SSH to log into the RAZ server.
  3. Run the ps -ef | grep rangerraz | awk '{split($0, array,"classpath"); print array[2]}' | cut -d: -f1 command to identify the RAZ_CONF_DIR directory.
  4. Run the cat *[***RAZ_CONF_DIR***]*/ranger-raz-site.xml command to view the RAZ server configuration details.

How do I enable the debug level for RAZ server and RAZ client?

When you enable the DEBUG level for RAZ server and RAZ client, a detailed verbose log is generated. Alternatively, you can only enable debug on a package level, so that only the package logs show detailed verbose logs.

- To configure debug for RAZ server at package level, perform the following steps:
  1. Go to the Cloudera Manager *Ranger RAZ service* Configuration tab.
  2. Search for the **Ranger Raz Server Logging Advanced Configuration Snippet (Safety Valve) property** property, and enter the following information:

     ```
     log4j.logger.org.apache.ranger.raz.[***package name***]=DEBUG
     log4j.logger.org.apache.hadoop.security=DEBUG
     log4j.appender.RFA.layout.ConversionPattern=[%p] %d{dd/MM/yyyy HH:mm:ss,
     SSS} [THREAD ID=%t] [CLASS=(%C{1}:%L)] %m%n
     ```
  3. Click Save Changes.
  4. Restart the Ranger RAZ service.
- You can configure the DEBUG level for RAZ clients.

  For example, to view the HDFS log in DEBUG level, run the HADOOP_ROOT_LOGGER=DEBUG,console hdfs *[***options***]* *[***arguments***]* command.

Is there a checklist to refer while troubleshooting RAZ-enabled Azure environments?

You can use the following brief checklist to help you to troubleshoot RAZ-enabled environments:

- Is Hierarchical NameSpace enabled for ADLS Gen2?
- Does the Ranger RAZ managed identity have the Storage Blob Delegator and Storage Blob Data Owner roles?
- Does the RAZ-enabled Azure environment use a zone-redundant storage (ZRS)?
- Are the Ranger Admin cloud policies (cm_adls) created with the correct storage account & paths based on the corresponding environment?
- Do you have sufficient permissions in Ranger Admin cloud policies (cm_adls) in the corresponding environment?
- Can the RAZ servers in Data Lake and workload clusters download Ranger policies from the Ranger Admin UI?
- Can the RAZ servers in Data Lake and workload clusters download Ranger UserStore?
- Can the RAZ servers in Data Lake and workload clusters connect to IDBroker and download the UserDelegationKey?

What are the most common errors in RAZ-enabled Azure environments?

The following table lists the most common errors, their causes, and solution to resolve the errors:

Error and error location	Cause and Solution
Failed to communicate with Ranger Admin and Error getting UserStore errors appear in RAZ Server logs.	These errors appear when the RAZ server cannot download the latest version of the user-store (user information) because the Ranger Admin service cannot reach the RAZ server host. To resolve this issue, verify whether the Ranger Admin service is up and reachable from the RAZ server host. If not, fix the connectivity issue.
AbfsTokenProvider: IdBroker initialization failed error appears in RAZ Server logs.	This error appears when the RAZ server cannot connect to IDBroker to obtain the UserDelegationKey that is used for authorizing requests in ADLS paths. To resolve this issue, verify whether IDBroker is up and reachable for the RAZ server host. If not, fix the connectivity issue.
DTAwsCredentialsProvider failed when trying to get token from idbroker, or AbfsTokenProvider: ==> AbfsTokeProvider.fetchUserDelegationKey and fetchAccessToken(): null response received from IDBroker errors appear in RAZ Server logs.	These errors appear when the RAZ server cannot connect to IDBroker to obtain the UserDelegationKey that is used for authorizing requests in S3 paths. To resolve this issue, verify whether IDBroker is up and reachable for the RAZ server host. If not, fix the connectivity issue.
Failed to communicate with all Raz URLs, Verify that the URLs are correct and corresponding services are running & accessible, and Multiple service types are not supported messages appear in RAZ client logs.	This issue appears when the RAZ server setup fails because the ranger.raz.bootstrap.servicetypes property in the ranger-raz-site.xml file has multiple service-types such as adls, s3 that are not supported. To resolve this issue, configure the ranger.raz.bootstrap.servicetypes property in the ranger-raz-site.xml file to the required cluster type, remove the other service types, and save the file. For example, enter s3 for AWS cluster type and enter adls for Azure cluster type.
Server did not process this request due to in-sufficient auth details, Failed to acquire a SAS token… AccessControlException:, HTTP Status 401 – Unauthorized appear in RAZ client logs.	These error messages appear when the RAZ server denies the authorization request because no or incomplete authentication details are available. To resolve this issue, you must ensure that the Ranger RAZ server has Kerberos or RAZ-DT & JWT authentication. You must have a valid TGT when the RAZ server supports Kerberos authentication.

Error and error location	Cause and Solution
Failed to get DSAS token from Raz, HttpStatus: 403, Failed to acquire a SAS token … : Permission denied messages appear in RAZ client logs.	These errors might appear because of various reasons, the following are a few possible causes and solutions: • The required Ranger policies are not set. To verify, the administrator must check the Ranger Admin Access Audits and if required, assign the required policies. • The RAZ server might not be able to fetch the User Delegation key from IDBroker. To verify, check the Ranger RAZ server logs. To resolve this issue, generate the User Delegation Key manually. If you cannot generate DSAS manually, this indicates that a network connectivity issue exists. To proceed, you must resolve the connectivity issues. • RAZ server cannot fetch the latest Ranger admin policies/users. To verify, download the RAZ policies manually. If you cannot download RAZ policies manually, this indicates a network connectivity issue. To proceed, resolve the connectivity issues.

How do I generate a UserDelegationKey manually?

Perform the following steps to generate a UserDelegationKey manually:

Procedure

1. Identify the host on which the RAZ service is installed in Cloudera Manager.
2. SSH to log into the RAZ server.
3. Run following commands to get the required parameters:
   a. ps -ef | grep rangerraz | awk '{split($0, array,"classpath"); print array[2]}' | cut -d: -f1 to identify the RAZ_CONF_DIR directory.
   b. klist -kt [***RAZ_CONF_DIR***]/../ranger_raz.keytab to identify the RAZ_PRINCIPLE parameter. The RAZ_PRINCIPLE parameter starts with *rangerraz*.
   c. cat /etc/alternatives/hadoop-conf/core-site.xml | grep -a1 'fs.azure.ext.cab.address' | grep 'value' to identify the complete ID_BROKER_URL.
4. Update the expiry date in the sasPost.xml file to another valid date.
5. Run following commands:
   a. kinit -kt *[***RAZ_CONF_DIR***]*/../ranger_raz.keytab *[***RAZ_PRINCIPLE***]*
   b. DT=$(curl --negotiate -u : "*[***ID_BROKER_URL***]*/dt/knoxtoken/api/v1/token" | jq -r '.access_token')
   c. AT=$(curl -k -H "Authorization: Bearer $DT" '*[***ID_BROKER_URL***]*/azure-cab/cab/api/v1/credentials' | jq -r '.access_token')
   d. curl -v -i -X POST -d @sasPost.xml -H "x-ms-version: 2018-11-09" -H "Authorization: Bearer $AT" "https://*[***ACCOUNT***]*.blob.core.windows.net/?restype=service&comp=userdelegationkey"

   The UserDelegationKey is generated.
6. In case, the UserDelegationKey is not generated as expected, run the following commands to verify whether the identity mappings are available:
   a. SSH to the IDBroker host.
   b. Go to the cd /var/log/knox/idbroker/ IDBroker logs directory.
   c. Run the grep -rl “addIdentitiesToVM” * command to view the list of identities. Note that the output must not be empty.
   d. Run the grep . -rnwe ‘addIdentitiesToVM’ command to view the assumerIdentity, adminIdentity, and rangerraz identities.

How do I download RAZ policies manually?

You can perform the following steps to download the RAZ policies manually:

Procedure

1. Identify the host on which the RAZ service is installed in Cloudera Manager.
2. SSH to log into the RAZ server.
3. Run following commands to identify the required parameters:
   a. ps -ef | grep rangerraz | awk '{split($0, array,"classpath"); print array[2]}' | cut -d: -f1 to identify the RAZ_CONF_DIR directory.
   b. klist -kt *[***RAZ_CONF_DIR**]*/../ranger_raz.keytab to identify the RAZ_PRINCIPLE. The RAZ_PRINCIPLE starts with rangerraz.
   c. cat /var/run/cloudera-scm-agent/process/1546336485-ranger_raz-RANGER_RAZ_SERVER/ranger-raz-conf/ranger-raz-site.xml | grep -a1 'ranger.raz.policy.rest.url' | grep 'value' to identify the ADMIN_URL. Use the ADMIN_URL after you remove any trailing slash.
4. Run following commands to download the RAZ policies:
   a. kinit -kt [***RAZ_CONF_DIR***]/../ranger_raz.keytab *[***RAZ_PRINCIPLE***]*
   b. curl -ikv --negotiate -u : -X GET -H "Accept:application/json" -H "Content-Type:application/json" "*[***ADMIN_URL***]*/service/plugins/secure/policies/download/cm_adls

   The RAZ policies for the ADLS service are downloaded to the current directory of the logged in host or server.

Managing a RAZ-enabled Azure environment

You can manage a RAZ-enabled environment in a similar manner as any other CDP environment.

For information on how to manage and monitor CDP environments running in Azure, refer to Working with Azure environments.