

Configuring Apache Ranger Authentication with UNIX, LDAP, or AD

Date published: 2019-11-01

Date modified:



Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

| | |
|---|---------------|
| Configuring Ranger Authentication with UNIX, LDAP, AD, or PAM..... | 4 |
| Configure Ranger authentication for UNIX..... | 4 |
| Configure Ranger authentication for AD..... | 6 |
| Configure Ranger authentication for LDAP..... | 8 |
| Configure Ranger authentication for PAM..... | 10 |
| Ranger AD Integration..... | 12 |
| Ranger UI authentication..... | 16 |
| Ranger UI authorization..... | 19 |

Configuring Ranger Authentication with UNIX, LDAP, AD, or PAM

This section describes how to configure the authentication method that determines who is allowed to log in to the Ranger web UI. The options are local UNIX, LDAP, AD, or PAM.



Note: In CDP Public Cloud, identity management is provided by FreeIPA, and configured using the Management Console. Therefore for CDP Public Cloud you should leave the Admin Authentication Method set to the UNIX authentication settings. For more information on FreeIPA, see [Managing FreeIPA in the Identify Management documentation](#).

The screenshot shows the Cloudera Manager interface for configuring Ranger-1. The left sidebar contains navigation links: Clusters, Hosts, Diagnostics, Audits, Charts, Backup, and Administration. The main panel is titled 'Cluster 1' and shows the configuration for 'RANGER-1'. The 'Configuration' tab is active, displaying the 'authentication unix' configuration. The 'Filters' section on the left shows a list of filters categorized by SCOPE, CATEGORY, and STATUS. The main configuration area on the right includes the following settings:

- Admin Authentication Method:** Set to UNIX (selected). Other options include LDAP, ACTIVE_DIRECTORY, PAM, and NONE.
- Admin UNIX Auth Remote Login:** Set to Ranger Admin Default Group.
- Admin UNIX Auth Service Hostname:** Set to {{RANGER_USERSYNC_HOST}}.
- Unix Auth Service Hostname:** Set to 5151.
- Admin Unix Auth Service Port:** Set to 5151.

At the bottom right, there is a '25 Per Page' dropdown menu.

Related Information

[Cloudera Management Console](#)

[CDP Cloud Management Console: Managing user access and authorization](#)

[Managing FreeIPA](#)

Configure Ranger authentication for UNIX

How to configure Ranger to use UNIX for user authentication.

About this task



Note: In CDP Public Cloud, identity management is provided by FreeIPA, and configured using the Management Console. Therefore for CDP Public Cloud you should leave the Admin Authentication Method set to the UNIX authentication settings. For more information on FreeIPA, see [Managing FreeIPA](#) in the [Identify Management](#) documentation.

Procedure

1. In Cloudera Manager, select Ranger, then click the Configuration tab.
2. To display the UNIX authentication settings, type "authentication unix" in the Search box.

The screenshot shows the Cloudera Manager interface for Cluster 1. The left sidebar contains navigation links: Clusters, Hosts, Diagnostics, Audits, Charts, Backup, and Administration. The main content area is titled 'RANGER-1' and shows the 'Configuration' tab. A search bar at the top of the configuration area contains the text 'authentication unix'. Below the search bar, there are filters for SCOPE, CATEGORY, and STATUS. The configuration settings are displayed in a table-like format:

| Configuration Property | Description | Default Value | Example Value | Required |
|------------------------------|--|---------------|---------------|------------------------|
| Admin Authentication Method | The Ranger authentication method. | UNIX | UNIX | Yes, to authentication |
| Admin UNIX Auth Remote Login | Flag to enable/disable remote login. Only used if the Authentication method is UNIX. | TRUE | TRUE | No. |

3. Configure the following settings for UNIX authentication, then click Save Changes.

Table 1: UNIX Authentication Settings

| Configuration Property | Description | Default Value | Example Value | Required |
|-----------------------------|--|---------------|---------------|------------------------|
| Admin Authentication Method | The Ranger authentication method. | UNIX | UNIX | Yes, to authentication |
| Allow remote Login | Flag to enable/disable remote login. Only used if the Authentication method is UNIX. | TRUE | TRUE | No. |

| Configuration Property | Description | Default Value | Example Value | Required |
|----------------------------------|--|---------------|-----------------------|------------------|
| ranger.unixauth.service.hostname | The FQDN of the host where the UNIX authentication service is running. Only used if the Authentication method is UNIX. {{RANGER_USERSYNC_HOST}} is a placeholder value that is replaced with the host where Ranger Usersync is installed in the cluster. | localhost | myunixhost.domain.com | Yes, if selected |
| ranger.unixauth.service.port | The port number where the ranger-usersync module is running the UNIX Authentication Service. | 5151 | 5151 | Yes, if selected |

Related Information
[Cloudera Management Console](#)

Configure Ranger authentication for AD

How to configure Ranger to use Active Directory (AD) for user authentication.

About this task

Note: In CDP Public Cloud, identity management is provided by FreeIPA, and configured using the Management Console. Therefore for CDP Public Cloud you should leave the Admin Authentication Method set to the UNIX authentication settings. For more information on FreeIPA, see Managing FreeIPA in the Identify Management documentation.

Procedure

1. Select Cloudera Manager Ranger Configuration, type authentication in Search. Ranger authentication property settings display. You may need to scroll down to see the AD settings.

Cluster 1

✓ RANGER-1 [Actions](#) Aug 13, 12:07 PM PDT

Status Instances **Configuration** Commands Charts Library Audits Ranger Admin Web UI [Quick Links](#)

authentication [Role Groups](#) [History and Rollback](#) [Show All Descriptions](#)

Filters

- SCOPE**
 - RANGER-1 (Service-Wide) 0
 - Ranger Admin 19
 - Ranger Tagsync 1
 - Ranger Usersync 2
- CATEGORY**
 - Advanced 0
 - Logs 0
 - Main 21
 - Monitoring 0
 - Performance 0
 - Ports and Addresses 1
 - Resource Management 0
 - Security 0
 - Stacks Collection 0
- STATUS**
 - Error 0
 - Warning 0
 - Edited 2
 - Non-default 2
 - Has Overrides 0

Admin Authentication Method
ranger.authentication.method

Ranger Admin Default Group [?](#)

☐ UNIX

☐ LDAP

☒ ACTIVE_DIRECTORY

☐ PAM

☐ NONE

Admin UNIX Auth Remote Login
ranger.unixauth.remote.login.enabled

☐ Ranger Admin Default Group [?](#)

Admin UNIX Auth Service Hostname
ranger.unixauth.service.hostname

Ranger Admin Default Group

[?](#)

Host where unix authentication service is running. Only used if Authentication method is UNIX. {{RANGER_USERSYNC_HOST}} is a placeholder value which will be replaced with the host where Ranger Usersync will be installed in the current cluster.

Admin LDAP Auth User DN Pattern
ranger.ldap.user.dn.pattern

Ranger Admin Default Group [?](#)

Admin LDAP Auth User Search Filter
ranger.ldap.user.searchfilter

Ranger Admin Default Group [?](#)

Admin LDAP Auth Group Search Base
ranger.ldap.group.searchbase

Ranger Admin Default Group [?](#)

CDEP Deployment from 2019-Aug-05 11:11

[Parcels](#) [Recent Commands](#) [Support](#)

2. Configure the following settings for AD authentication, then click Save Changes.

| Property | Description | Default value | Sample values |
|---|---|---------------|---------------------------------------|
| Admin Authentication Method | The Ranger authentication method. | UNIX | ACTIVE_DIRECTORY |
| Admin AD Auth Base DN ranger.ldap.ad.base.dn | The Distinguished Name (DN) of the starting point for directory server searches. | N/A | dc=example,dc=com |
| Admin AD Auth Bind DN ranger.ldap.ad.bind.dn | The full Distinguished Name (DN), including Common Name (CN) of an LDAP user account that has privileges to search for users. | N/A | cn=adadmin,cn=Users,dc=example,dc=com |
| Admin AD Auth Bind Password ranger.ldap.ad.bind.password | Password for the bind.dn. | N/A | Secret123! |
| Admin AD Auth Domain Name ranger.ldap.ad.domain | The domain name of the AD Authentication service. | N/A | example.com |

| Property | Description | Default value | Sample values |
|--|---|---------------|----------------------------|
| Admin AD Auth Referral ranger.ldap.ad.referral* | See below. | ignore | follow ignore throw |
| Admin AD Auth URL ranger.ldap.ad.url | The AD server URL, for example: ldap://<AD-Servername>Port | N/A | ldap://<AD-Servername>Port |
| Admin AD Auth User Search Filter ranger.ldap.ad.user.searchfilter | AD user search filter. | N/A | |

* There are three possible values for ranger.ldap.ad.referral:

- follow
- throw
- ignore

The recommended setting is: follow.

When searching a directory, the server might return several search results, along with a few continuation references that show where to obtain further results. These results and references might be interleaved at the protocol level.

When ranger.ldap.ad.referral is set to follow:

The AD service provider processes all of the normal entries first, and then follows the continuation references.

When ranger.ldap.ad.referral is set to throw:

All of the normal entries are returned in the enumeration first, before the `ReferralException` is thrown.

By contrast, a referral error response is processed immediately when this property is set to follow or throw.

When ranger.ldap.ad.referral is set to ignore:

The server should return referral entries as ordinary entries (or plain text). This might return partial results for the search. In the case of AD, a `PartialResultException` is returned when referrals are encountered while search results are processed.

Related Information

[Cloudera Management Console](#)

Configure Ranger authentication for LDAP

How to configure Ranger to use LDAP for user authentication.

About this task



Note: In CDP Public Cloud, identity management is provided by FreeIPA, and configured using the Management Console. Therefore for CDP Public Cloud you should leave the Admin Authentication Method set to the UNIX authentication settings. For more information on FreeIPA, see [Managing FreeIPA](#) in the Identify Management documentation.

Procedure

1. In Cloudera Manager, select Ranger, then click the Configuration tab.

- To display the authentication settings, type "authentication" in the Search box. You may need to scroll down to see all of the LDAP settings.

The screenshot shows the Cloudera Manager interface for configuring Ranger-1. The search bar at the top contains the word "authentication". The left sidebar shows the navigation menu with "Administration" selected. The main panel displays the configuration for "RANGER-1" with the "Configuration" tab active. The search results show filters for SCOPE, CATEGORY, and STATUS. The configuration details for "Admin Authentication Method" are shown, with "LDAP" selected. Other settings like "Admin UNIX Auth Remote Login", "Admin UNIX Auth Service Hostname", "Admin LDAP Auth User DN Pattern", "Admin LDAP Auth User Search Filter", "Admin LDAP Auth Group Search Base", and "Admin LDAP Auth Group Search Filter" are also visible.

- Configure the following settings for LDAP authentication, then click Save Changes.

| Property | Required ? | Description | Default value | Sample values |
|---|------------|-----------------------------------|---------------|---|
| Admin Authentication Method | Required | The Ranger authentication method. | UNIX | LDAP |
| Admin LDAP Auth Group Search Base ranger.ldap.group.searchbase | Optional | The LDAP group search base. | N/A | ((CN=Hdp_users)(CN=Hdp_admins)) |
| Admin LDAP Auth Group Search Filter ranger.ldap.group.searchfilter | Optional | The LDAP group search filter. | N/A | |
| Admin LDAP Auth URL ranger.ldap.url | Required | The LDAP server URL | N/A | ldap://localhost:389 or ldaps://localhost:636 |

| Property | Required ? | Description | Default value | Sample values |
|---|------------|--|---------------|-------------------------------------|
| Admin LDAP Auth Bind User ranger.ldap.bind.dn | Required | Full distinguished name (DN), including common name (CN), of an LDAP user account that has privileges to search for users. This user is used for searching the users. This could be a read-only LDAP user. | N/A | cn=admin,dc=example,dc=com |
| Admin LDAP Auth Bind User Password ranger.ldap.bind.password | Required | Password for the account that can search for users. | N/A | Secret123! |
| Admin LDAP Auth User Search Filter ranger.ldap.user.searchfilter | Required | The LDAP user search filter. | N/A | |
| Admin LDAP Auth Base DN ranger.ldap.base.dn | Required | The Distinguished Name (DN) of the starting point for directory server searches. | N/A | dc=example,dc=com |
| Admin LDAP Auth Group Role Attribute ranger.ldap.group.roleattribute | Optional | The LDAP group role attribute. | N/A | cn |
| Admin LDAP Auth Referral ranger.ldap.referral* | Required | See below. | ignore | follow ignore throw |
| Admin LDAP Auth User DN Pattern ranger.ldap.user.dnpattern | Required | The LDAP user DN. | N/A | uid={0},ou=users,dc=xasecure,dc=net |

* There are three possible values for ranger.ldap.ad.referral: follow, throw, and ignore. The recommended setting is follow.

When searching a directory, the server might return several search results, along with a few continuation references that show where to obtain further results. These results and references might be interleaved at the protocol level.

- When this property is set to follow, the AD service provider processes all of the normal entries first, and then follows the continuation references.
- When this property is set to throw, all of the normal entries are returned in the enumeration first, before the ReferralException is thrown. By contrast, a "referral" error response is processed immediately when this property is set to follow or throw.
- When this property is set to ignore, it indicates that the server should return referral entries as ordinary entries (or plain text). This might return partial results for the search. In the case of AD, a PartialResultException is returned when referrals are encountered while search results are processed.

Related Information

[Cloudera Management Console](#)

Configure Ranger authentication for PAM

How to configure Ranger to use PAM for user authentication.

About this task



Note: In CDP Public Cloud, identity management is provided by FreeIPA, and configured using the Management Console. Therefore for CDP Public Cloud you should leave the Admin Authentication Method set to the UNIX authentication settings. For more information on FreeIPA, see [Managing FreeIPA](#) in the [Identify Management](#) documentation.

Procedure

1. In Cloudera Manager, select Ranger, then click the Configuration tab.
2. Under Admin Authentication Method, select PAM, then click Save Changes.

3. Create the following two PAM files:

- `/etc/pam.d/ranger-admin` with the following content:

```
#%PAM-1.0
auth sufficient pam_unix.so
auth sufficient pam_sss.so
account sufficient pam_unix.so
account sufficient pam_sss.so
```

- `/etc/pam.d/ranger-remote` with the following content:

```
#%PAM-1.0
auth sufficient pam_unix.so
auth sufficient pam_sss.so
account sufficient pam_unix.so
```

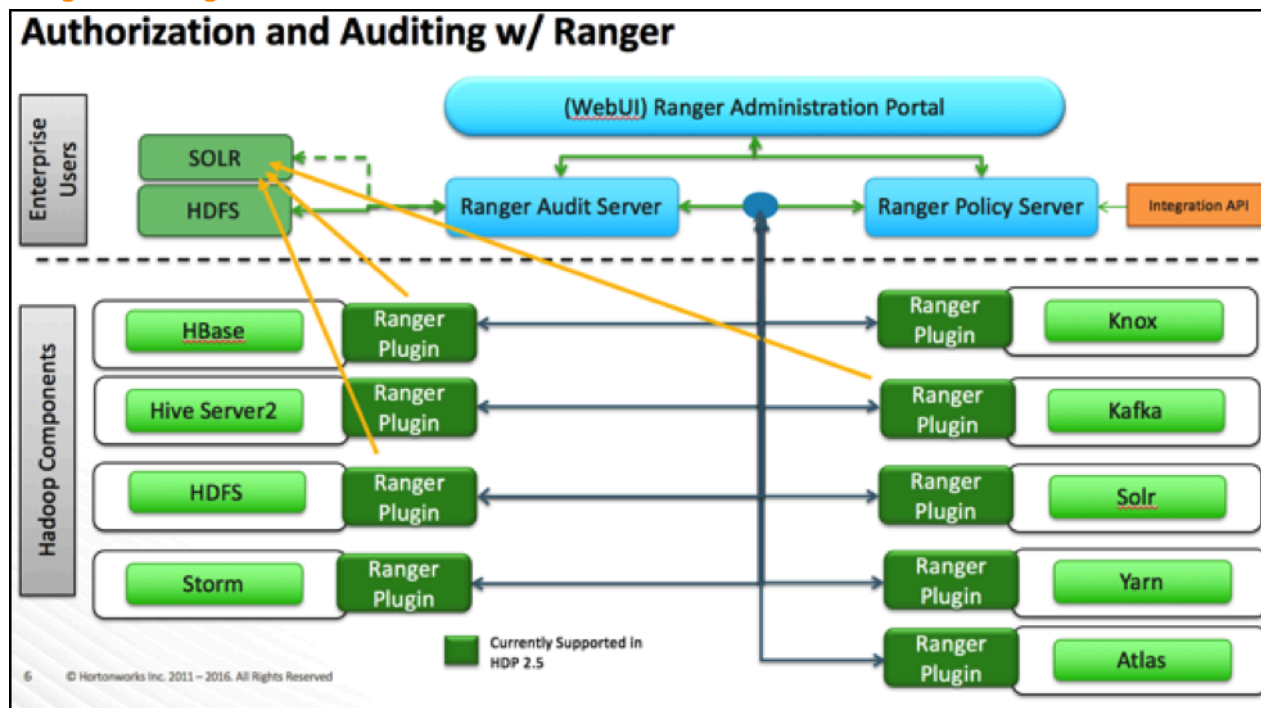
```
account sufficient pam_sss.so
```

4. Confirm that the /etc/shadow file has 444 permissions.
5. Select Actions > Restart to restart Ranger.

Ranger AD Integration

A conceptual overview of Ranger-AD integration architecture.

Ranger AD Integration: Architecture Overview



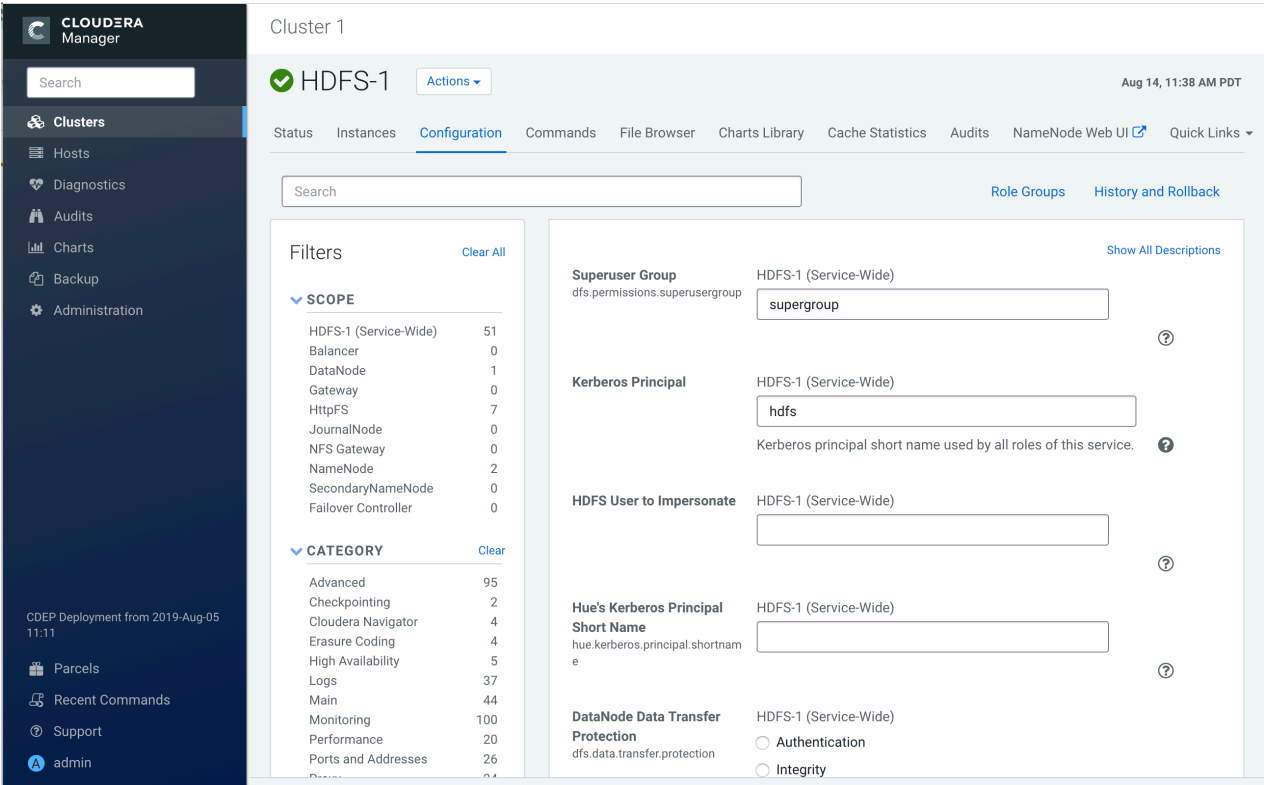
When a Ranger plugin for a component (such as HBase or HDFS) is activated, Ranger is in full control of any access. There is two-way communication between the Ranger plugin and the Ranger (Admin) Policy Server (RPS):

1. **Plugins to RPS:** Ranger plugins regularly call the RPS to see if new policies were defined in the Ranger Administration Portal (RAP). Generally it takes approximately 30 seconds for a policy to be updated.
2. **RPS to components:** The RPS queries the component for meta objects that live on the component to base policies upon (this provides the autocomplete and drop-down list when defining policies).

The first communication channel (Plugin to RPS) is essential for the plugin to function, whereas the second (RPS to components) is optional. It would still be possible to define and enforce policies without the second channel, but you would not have autocomplete during policy definition.

Configuration details on both communication channels are configured in both Cloudera Manager and in the Ranger Administration Portal.

Example for HDFS plugin on a kerberized cluster:



The Kerberos principal short name for the HDFS service,"hdfs", is the one that is involved the second communication channel (RPS to components) for getting metadata from HDFS (such as HDFS folders) across. The settings on the HDFS configuration must match those set in Ranger (by selecting Access > Manager > Resource Based Policies, then selecting the Edit icon for the HDFS service:

Ranger Access Manager Audit Security Zone Settings admin

Service Manager Edit Service

Select Tag Service: cm_tag

Config Properties :

Username * hdfs

Password *

Namenode URL * hdfs://dhoyle-8-5-1.vpc.cloudera

Authorization Enabled Yes

Authentication Type * Kerberos

hadoop.security.auth_to_local

dfs.datanode.kerberos.principal

dfs.namenode.kerberos.principal

dfs.secondary.namenode.kerberos.principal

RPC Protection Type Authentication

Common Name for Certificate

Add New Configurations

| Name | Value |
|----------------------------|-------|
| tag.download.auth.users | hdfs |
| policy.download.auth.users | hdfs |

+

Test Connection

Save Cancel Delete

To verify the second communication channel (RPS to components) click Test Connection for the applicable service (as shown above for the HDFS service). A confirmation message appears if the connection works successfully.

To verify if the paramount first communication channel (Plugins to RPS) works, select Audit > Plugins in Ranger:

| Ranger Access Manager Audit Security Zone Settings admin | | | | | | |
|--|--------------|-----------------|--------------|--------------|--------------------|---------------------------|
| Access Admin Login Sessions Plugins Plugin Status User Sync | | | | | | |
| Search for your plugins... | | | | | | |
| Entries : 1 to 23 of 23 Last Updated Time : 08/14/2019 03:01:02 PM | | | | | | |
| Export Date (Eastern Daylight Time) | Service Name | Plugin Id | Plugin IP | Cluster Name | Http Response Code | Status |
| 08/13/2019 11:49:39 AM | cm_hive | hiveServer2@... | 10.65.30.5 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:49:27 AM | cm_hive | impala@... | 10.65.30.5 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:49:22 AM | cm_hive | impala@... | 10.65.30.5 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:49:17 AM | cm_hive | impala@... | 10.65.49.144 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:49:17 AM | cm_hive | impala@... | 10.65.50.67 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:46:39 AM | cm_hive | hiveServer2@... | 10.65.30.5 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:46:27 AM | cm_hive | impala@... | 10.65.30.5 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:46:22 AM | cm_hive | impala@... | 10.65.30.5 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:46:17 AM | cm_hive | impala@... | 10.65.49.144 | Cluster 1 | 200 | Policies synced to plugin |
| 08/13/2019 11:46:17 AM | cm_hive | impala@... | 10.65.50.67 | Cluster 1 | 200 | Policies synced to plugin |
| 08/05/2019 02:51:20 PM | cm_atlas | atlas@... | 10.65.30.5 | Cluster 1 | 200 | Policies synced to plugin |

Ranger AD Integration: Ranger Audit

Ranger plugins furthermore send their audit event (whether access was granted or not and based on which policy) directly to the configured sink for audits, which can be HDFS, Solr or both. This is indicated by the yellow arrows in the architectural graph.

The audit access tab on the RAP (Audit > Access) is only populated if Solr is used as the sink.

| Ranger Access Manager Audit Security Zone Settings admin | | | | | | | | | | |
|---|----------------|------------------------|---------------|-------|---------------------|-----------------------------|-------------|---------|-----------------|-----------------|
| Access Admin Login Sessions Plugins Plugin Status User Sync | | | | | | | | | | |
| START DATE: 08/14/2019 | | | | | | | | | | |
| Exclude Service Users : <input type="checkbox"/> Entries : 1 to 25 of 101696 Last Updated Time : 08/14/2019 03:15:10 PM | | | | | | | | | | |
| Policy ID | Policy Version | Event Time | Application | User | Service Name / Type | Resource Name / Type | Access Type | Result | Access Enforcer | Agent Host Name |
| 5 | 1 | 08/14/2019 03:15:02 PM | hbaseRegional | atlas | cm_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 10.65.30.5 |
| 15 | 1 | 08/14/2019 03:15:02 PM | kafka | kafka | cm_kafka kafka | kafka-cluster cluster | kafka_admin | Allowed | ranger-acl | 10.65.30.5 |
| 15 | 1 | 08/14/2019 03:15:02 PM | kafka | kafka | cm_kafka kafka | kafka-cluster cluster | kafka_admin | Allowed | ranger-acl | 10.65.30.5 |
| 15 | 1 | 08/14/2019 03:15:00 PM | kafka | kafka | cm_kafka kafka | kafka-cluster cluster | kafka_admin | Allowed | ranger-acl | 10.65.30.5 |
| 20 | 1 | 08/14/2019 03:15:00 PM | kafka | atlas | cm_kafka kafka | ATLAS_SPARK_... topic | consume | Allowed | ranger-acl | 10.65.30.5 |
| 15 | 1 | 08/14/2019 03:15:00 PM | kafka | kafka | cm_kafka kafka | kafka-cluster cluster | kafka_admin | Allowed | ranger-acl | 10.65.30.5 |
| 18 | 1 | 08/14/2019 03:15:00 PM | kafka | atlas | cm_kafka kafka | ATLAS_HOOK topic | consume | Allowed | ranger-acl | 10.65.30.5 |
| 15 | 1 | 08/14/2019 03:14:58 PM | kafka | kafka | cm_kafka kafka | kafka-cluster cluster | kafka_admin | Allowed | ranger-acl | 10.65.30.5 |
| 15 | 1 | 08/14/2019 03:14:58 PM | kafka | kafka | cm_kafka kafka | kafka-cluster cluster | kafka_admin | Allowed | ranger-acl | 10.65.30.5 |
| 5 | 1 | 08/14/2019 03:14:57 PM | hbaseRegional | atlas | cm_hbase hbase | atlas_janus/m column-family | get | Allowed | ranger-acl | 10.65.30.5 |

This screen points out an important Ranger feature. When the plugin is enabled AND no specific policy is in place for access to some object, the plugin will fall back to enforcing the standard component-level Access Control Lists (ACLs). For HDFS that would be the user : rwx / group : rwx / other : rwx ACLs on folders and files.

Once this defaulting to component ACLs happens, the audit events list a " - " in the Policy ID column instead of a policy number. If a Ranger policy was in control of allowing/denying access, the policy number is shown.

Ranger AD Integration: Overview

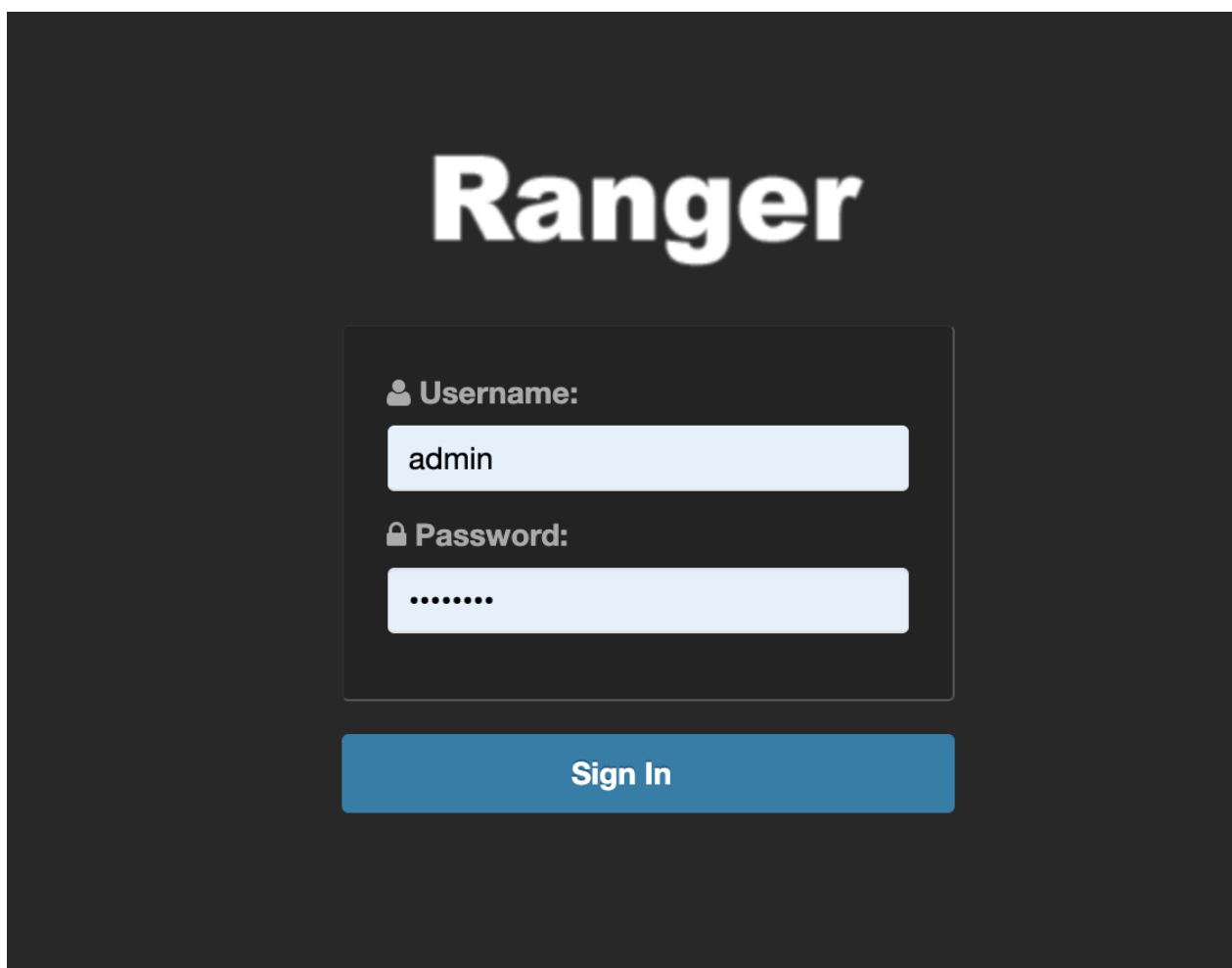
Rangers AD Integration has 2 levels:

1. Ranger UI authentication (which users can log in to Ranger itself).
2. Ranger user/group sync (which users/groups to define policies for)

Ranger UI authentication

Reference information on Ranger UI authentication, when configuring Ranger AD integration.

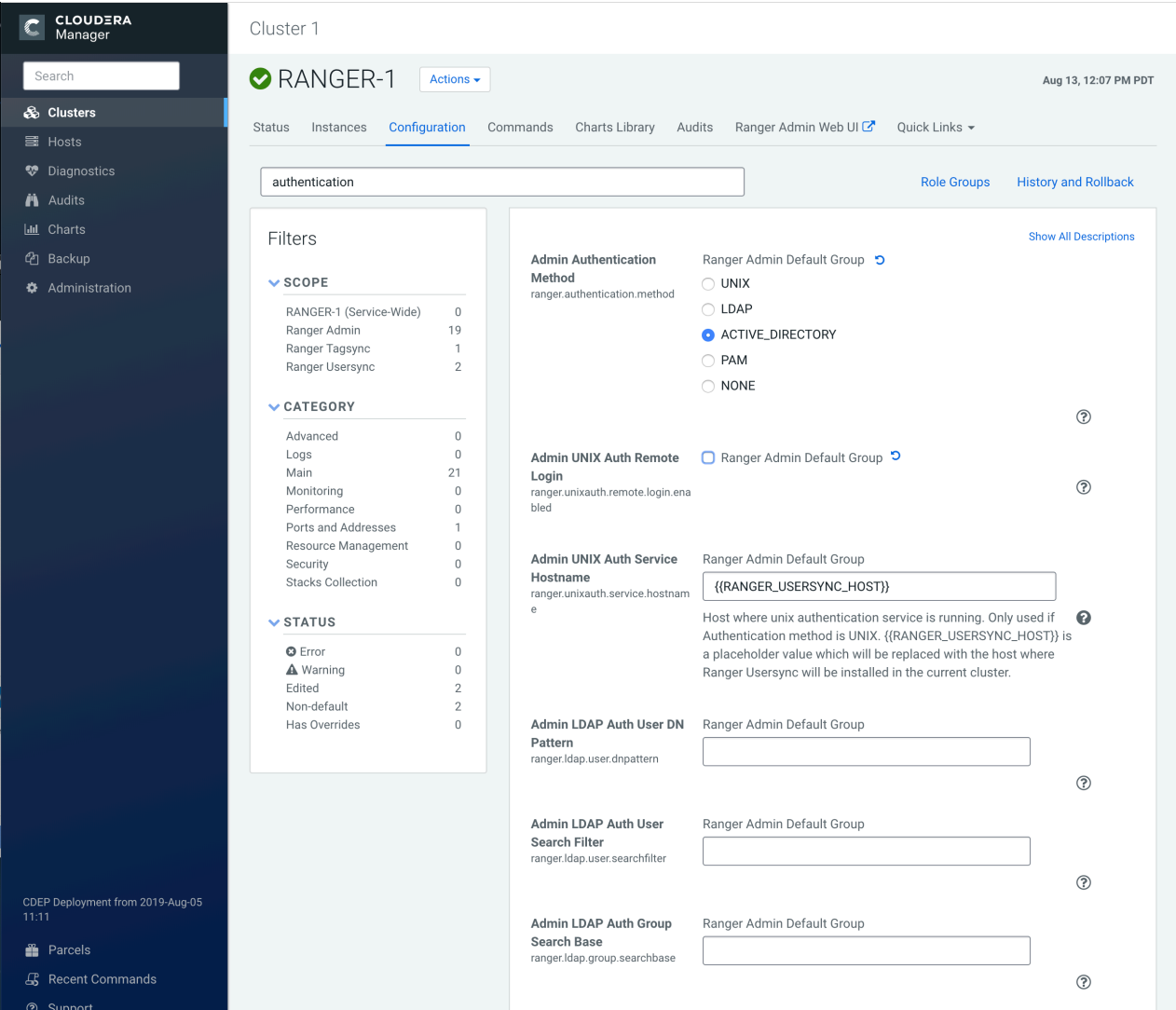
This is an extra AD level filter option on top of Kerberos authentication that maps to:



For AD there are two options for defining who can access the Ranger UI: LDAP or ACTIVE_DIRECTORY. There is not a huge amount of difference between them, but they are separate sets of properties.

ACTIVE_DIRECTORY

In Cloudera Manager, select Ranger, then click the Configuration tab. To display the authentication settings, type "authentication" in the Search box. You may need to scroll down to see the AD settings.



The ranger.ldap.ad.base.dn property determines the base of any search, so users not on this OU tree path can not be authenticated.

The ranger.ldap.ad.user.searchfilter property is a dynamic filter that maps the user name in the Ranger web UI login screen to sAMAccountName. For example, the AD sAMAccountName property has example values like k.reshi and d.alora so make sure to enter a matching value for 'Username' in the logon dialogue.

LDAP

The LDAP properties allow for more fine tuning.

In Cloudera Manager, select Ranger, then click the Configuration tab. To display the authentication settings, type "authentication" in the Search box. You may need to scroll down to see all of the LDAP settings.

There is one catch: the `ranger.ldap.user.dnpattern` is evaluated first. Consider the following example value:

`CN={0},OU=London,OU=Company,OU=User Accounts,OU=CorpUsers,DC=field,DC=hortonworks,DC=com`

This would work, but has two side effects:

- Users would have to log on with their 'long username' (like 'Kvotthe Reshi / Denna Alora'), which would also mean that policies would have to be updated using that long name instead of the `k.reshi` short name variant.
- Traversing AD by DN patterns does not allow for applying group filters at all. In the syntax above, only users directly in `OU=London` would be able to log on.

This adverse behavior can be avoided by intentionally putting a DN pattern (`DC=intentionally,DC=wrong`) in the `ranger.ldap.user.dnpattern` property, AND a valid filter in User Search Filter:

`(&(objectclass=user)(memberOf=CN=Hdp_admins,OU=Company,OU=User Accounts,OU=CorpUsers,DC=field,DC=hortonworks,DC=com)(sAMAccountName={0}))`

This works because the filter is only applied after the DN pattern query on AD does not return anything. If it does, the User Search Filter is not applied.

Ranger has a very simple approach to the internal user list that is kept in a relational schema. This list contains all users that were synced with AD ever, and all those users can potentially log in to the Ranger UI. But only Admin users can really do any policy-related things in the Ranger UI (see next section).

Be aware that all of this is only about authentication to Ranger. Someone from the 'Hdp_admins' group would still not have a Ranger admin role.

Related Information

[Configure Ranger authentication for LDAP](#)

Ranger UI authorization

Reference information on Ranger UI authorization, when configuring Ranger AD integration.

To configure the users, groups, and roles that can access the Ranger portal or its services, select Settings > Users/Groups/Roles in the top menu.

Ranger Access Manager Audit Security Zone Settings **admin**

Users/Groups/Roles

Users Groups Roles

User List

Search for your users...

Add New User Set Visibility

| <input type="checkbox"/> | User Name | Email Address | Role | User Source | Groups | Visibility |
|--------------------------|----------------|---------------|-------|-------------|--------------------|------------|
| <input type="checkbox"/> | admin | | Admin | Internal | -- | Visible |
| <input type="checkbox"/> | rangerusersync | | Admin | Internal | -- | Visible |
| <input type="checkbox"/> | rangertagsync | | Admin | Internal | -- | Visible |
| <input type="checkbox"/> | hive | | User | External | hive | Visible |
| <input type="checkbox"/> | cloudera-scm | | User | External | wheel cloudera-scm | Visible |
| <input type="checkbox"/> | https | | User | External | https | Visible |
| <input type="checkbox"/> | superset | | User | External | superset | Visible |
| <input type="checkbox"/> | atlas | | User | External | hadoop atlas | Visible |
| <input type="checkbox"/> | ranger | | User | External | hadoop ranger | Visible |
| <input type="checkbox"/> | kudu | | User | External | kudu | Visible |
| <input type="checkbox"/> | kms | | User | External | kms | Visible |
| <input type="checkbox"/> | accumulo | | User | External | accumulo | Visible |
| <input type="checkbox"/> | polkitd | | User | External | polkitd | Visible |
| <input type="checkbox"/> | nfsnobody | | User | External | nfsnobody | Visible |
| <input type="checkbox"/> | spark | | User | External | spark | Visible |
| <input type="checkbox"/> | flume | | User | External | flume | Visible |
| <input type="checkbox"/> | solr | | User | External | solr | Visible |
| <input type="checkbox"/> | jenkins | | User | External | jenkins | Visible |

A user can be a User, Admin, or Auditor:

The screenshot shows the Ranger web interface for editing a user. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', 'Settings', and a user profile 'admin'. The breadcrumb trail is 'Users/Groups/Roles > User Edit'. The 'User Detail' section has two tabs: 'Basic Info' (selected) and 'Change Password'. The 'Basic Info' tab contains the following fields:

- User Name *: rangerusersync
- First Name *: rangerusersync
- Last Name: (empty)
- Email Address: (empty)
- Select Role *: A dropdown menu is open, showing 'Admin' (selected), 'User', and 'Auditor'.
- Group: please select

At the bottom of the form are 'Save' and 'Cancel' buttons.

Only users with the Admin role can edit Ranger policies.