

Configuring Apache Ranger Authentication with UNIX, LDAP, or AD

Date published: 2019-11-01

Date modified:



Legal Notice

© Cloudera Inc. 2025. 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
Ranger Usersync.....	20
Ranger user management.....	25
Known issue: Ranger group mapping.....	26

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 displays the configuration for 'RANGER-1' under the 'Configuration' tab. The search bar shows 'authentication unix'. The configuration is organized into sections: SCOPE, CATEGORY, STATUS, and Admin Authentication. The Admin Authentication section shows the Method set to UNIX. Other sections include Admin UNIX Auth Remote Login, Admin UNIX Auth Service Hostname, Unix Auth Service Hostname, and Admin Unix Auth Service Port.

SCOPE	Count
RANGER-1 (Service-Wide)	0
Ranger Admin	4
Ranger Tagsync	0
Ranger Usersync	1

CATEGORY	Count
Advanced	0
Logs	0
Main	4
Monitoring	0
Performance	0
Ports and Addresses	1
Resource Management	0
Security	0
Stacks Collection	0

STATUS	Count
Error	0
Warning	0
Edited	0
Non-default	0
Has Overrides	0

Admin Authentication
 Method: ☒ UNIX
 ranger.authentication.method

Admin UNIX Auth Remote Login
 Ranger Admin Default Group
 ranger.unixauth.remote.login.enabled

Admin UNIX Auth Service Hostname
 Ranger Admin Default Group
 ranger.unixauth.service.hostname: {{RANGER_USERSYNC_HOST}}

Unix Auth Service Hostname
 Ranger Usersync Default Group
 ranger.usersync.port: 5151

Admin Unix Auth Service Port
 Ranger Admin Default Group
 ranger.unixauth.service.port: 5151

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 has tabs for Status, Instances, Configuration (selected), Commands, Charts Library, Audits, Ranger Admin Web UI, and Quick Links. A search bar at the top of the configuration page 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:

Property	Value	Group
Admin Authentication Method	UNIX	Ranger Admin Default Group
Admin UNIX Auth Remote Login	<input checked="" type="checkbox"/>	Ranger Admin Default Group
Admin UNIX Auth Service Hostname	{{(RANGER_USERSYNC_HOST)}}	Ranger Admin Default Group
Unix Auth Service Hostname	5151	Ranger Usersync Default Group
Admin Unix Auth Service Port	5151	Ranger Admin Default Group

At the bottom right, there is a pagination control showing '25 Per Page'.

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. 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.

Cluster 1

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Backup

Administration

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

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 Admin Default Group

Method

ranger.authentication.method

UNIX

LDAP

ACTIVE_DIRECTORY

PAM

NONE

Admin UNIX Auth Remote Login

Ranger Admin Default Group

ranger.unixauth.remote.login.enabled

Admin UNIX Auth Service Hostname

Ranger Admin Default Group

Hostname

ranger.unixauth.service.hostname

{{RANGER_USERSYNC_HOST}}

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 Admin Default Group

ranger.ldap.user.dn.pattern

Admin LDAP Auth User Search Filter

Ranger Admin Default Group

ranger.ldap.user.searchfilter

Admin LDAP Auth Group Search Base

Ranger Admin Default Group

ranger.ldap.group.searchbase

CDEP Deployment from 2019-Aug-05 11:11

Parcels

Recent Commands

Support

- 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	dc=example,dc=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.	N/A	
Admin AD Auth User Search Filter ranger.ldap.ad.user.searchfilter	The search filter used for Bind Authentication.	N/A	

* 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 theReferralException 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 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 authentication. The left sidebar contains a search bar and a list of navigation items: Clusters, Hosts, Diagnostics, Audits, Charts, Backup, and Administration. The main panel displays the 'authentication' configuration page for 'RANGER-1'. The 'Admin Authentication Method' is set to 'LDAP'. The 'Admin LDAP Auth Group Search Base' is set to '((CN=Hdp_users)(CN=Hdp_admins))'. The 'Admin LDAP Auth Group Search Filter' is set to '(&(CN=Hdp_users)(CN=Hdp_admins))'. The 'Admin LDAP Auth URL' is set to 'ldap://localhost:389 or ldaps://localhost:636'.

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

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

Property	Description	Default value	Sample values
Admin LDAP Auth Bind User ranger.ldap.bind.dn	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	Password for the account that can search for users.	N/A	Secret123!
Admin LDAP Auth User Search Filter ranger.ldap.user.searchfilter	The LDAP user search filter.	N/A	
Admin LDAP Auth Base DN ranger.ldap.base.dn	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	The LDAP group role attribute.	N/A	cn
Admin LDAP Auth Referral ranger.ldap.referral*	See below.	ignore	follow ignore throw
Admin LDAP Auth User DN Pattern ranger.ldap.user.dnpattern	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.

The screenshot shows the Cloudera Manager interface for configuring Ranger. The left sidebar contains the navigation menu with 'Administration' selected. The main panel displays the 'Admin Authentication Method' configuration. The 'Admin Authentication Method' section is highlighted, showing radio buttons for UNIX, LDAP, ACTIVE_DIRECTORY, PAM (selected), and NONE. Below this, there are several other configuration sections, each with a dropdown menu set to 'Ranger Admin Default Group'. At the bottom, a status bar indicates '1 Edited Value' and 'Reason for change: Modified Admin Authentication Method'. A blue 'Save Changes (CTRL+S)' button is located at the bottom right.

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
```

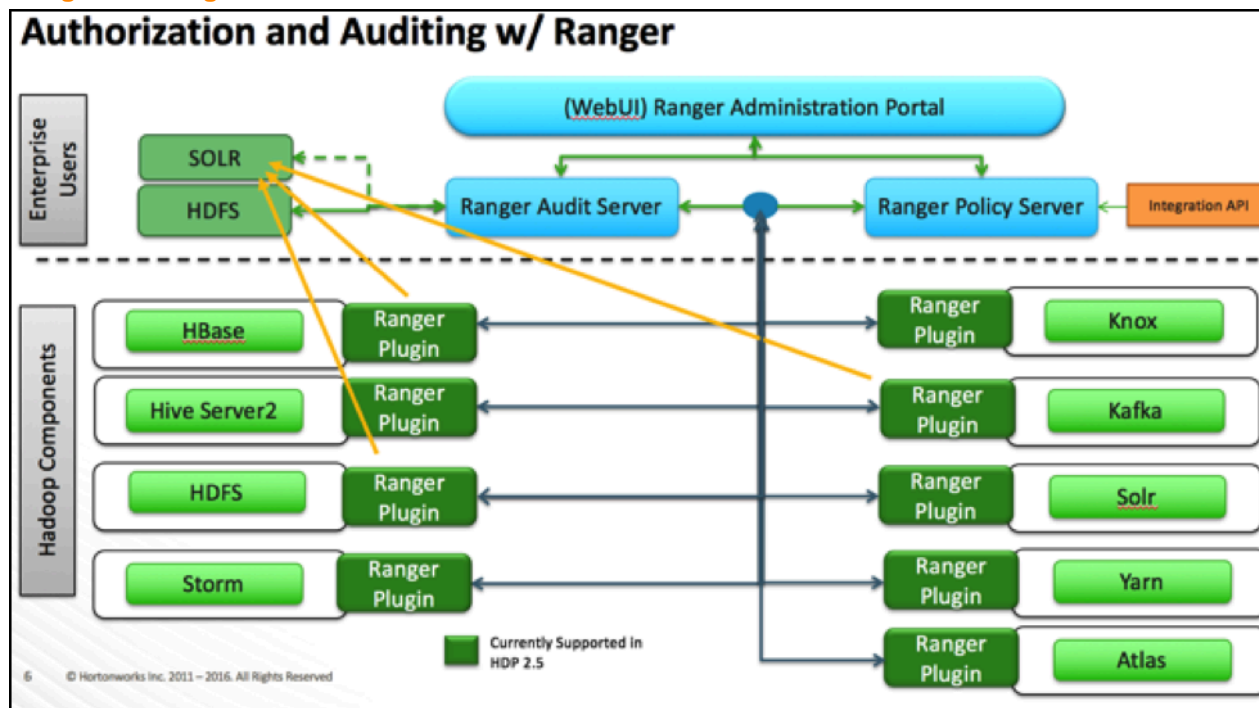
```
account sufficient pam_sss.so
```

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

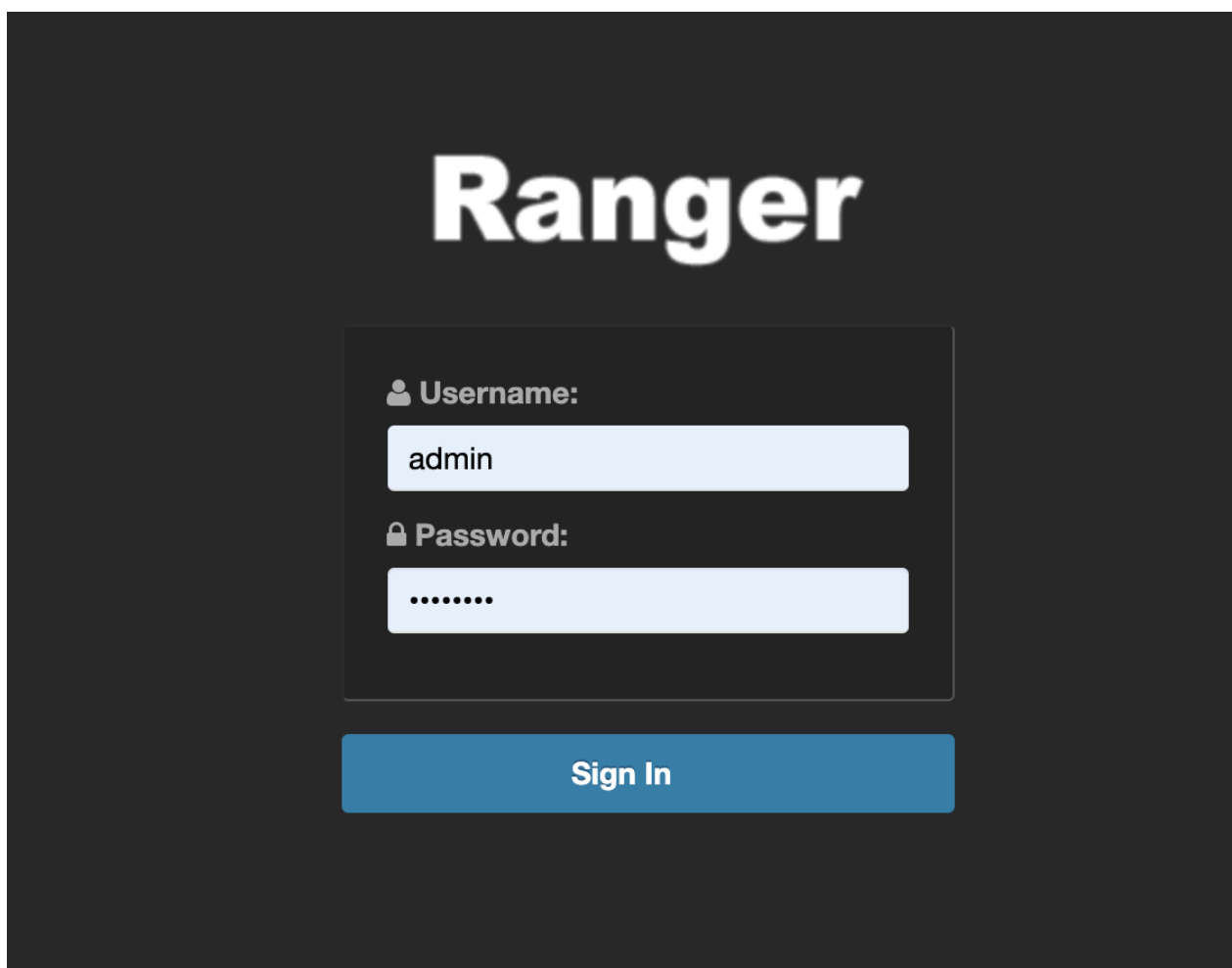
Rangers AD Integration has 2 levels:

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 screenshot shows the Cloudera Manager interface for the 'RANGER-1' cluster. The left sidebar contains navigation links: Clusters, Hosts, Diagnostics, Audits, Charts, Backup, and Administration. The main panel is titled 'Cluster 1' and shows the 'RANGER-1' configuration page. The 'Configuration' tab is selected, and the search box contains 'authentication'. The left sidebar also shows a list of filters under 'SCOPE', 'CATEGORY', and 'STATUS'. The main configuration area displays several settings for authentication:

- Admin Authentication Method:** ranger.authentication.method. Options: ☐ UNIX, ☐ LDAP, ☒ ACTIVE_DIRECTORY, ☐ PAM, ☐ NONE.
- Admin UNIX Auth Remote Login:** ranger.unixauth.remote.login.enabled. Value: ☐ Ranger Admin Default Group.
- Admin UNIX Auth Service Hostname:** ranger.unixauth.service.hostname. Value: . Description: 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. Value: .
- Admin LDAP Auth User Search Filter:** ranger ldap.user.searchfilter. Value: .
- Admin LDAP Auth Group Search Base:** ranger ldap.group.searchbase. Value: .

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.res` and `d.alora` so make sure to enter a matching value for 'Username' in the logon dialogue.

With `ACTIVE_DIRECTORY` it is not possible to limit the scope of users that can access the Ranger UI any further by refining the value of the `ranger.ldap.ad.user.searchfilter` property even further to :

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

This does NOT work with the `ACTIVE_DIRECTORY` option.

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.

Cluster 1

✓ RANGER-1 [Actions](#)

Aug 13, 12:20 PM PDT

Status Instances **Configuration** Commands Charts Library Audits Ranger Admin Web UI Quick Links

authentication [Role Groups](#) [History and Rollback](#)

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

{{RANGER_USERSYNC_HOST}}

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.idap.user.dnpattern

Ranger Admin Default Group

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

Ranger Admin Default Group

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

Ranger Admin Default Group

Admin LDAP Auth Group Search Filter
ranger.idap.group.searchfilter

Ranger Admin Default Group

There is one catch: the `ranger.idap.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.idap.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:

Ranger Access Manager Audit Security Zone Settings admin

Users/Groups/Roles > User Edit

User Detail

Basic Info Change Password

User Name * rangerusersync ⓘ

First Name * rangerusersync ⓘ

Last Name ⓘ

Email Address ⓘ

Select Role * ✓ Admin User Auditor ⓘ

Group Please select ⓘ

Save Cancel

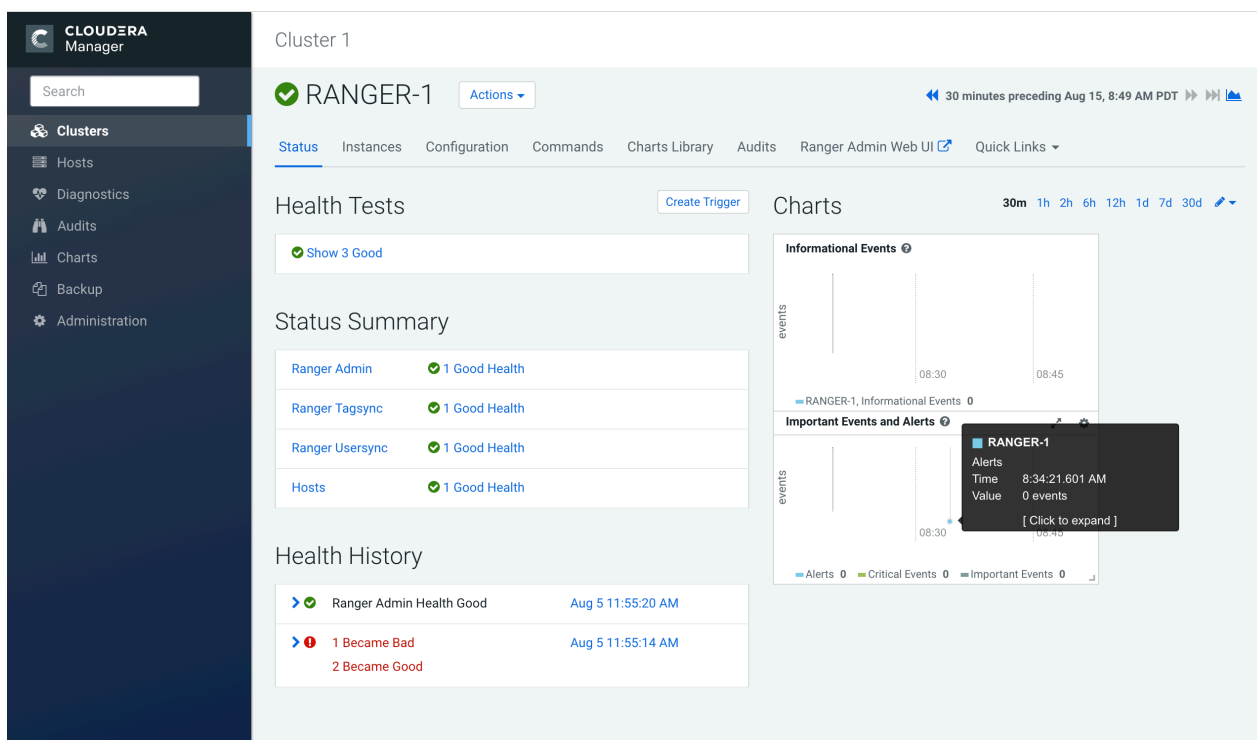
Only users with the Admin role can edit Ranger policies.

Ranger Usersync

Reference information on Ranger usersync, when configuring Ranger AD integration.

A vital part of the Ranger architecture is the ability to get users and groups from the corporate AD to use in policy definitions.

Ranger usersync runs as separate daemon:



It can also be refreshed using the Actions drop-down.

The screenshot shows the Cloudera Manager interface for Cluster 1, specifically the Ranger-1 configuration page. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Backup, and Administration. The main content area is divided into several sections:

- Health Tests:** Shows a status of 'Show 3 Good'.
- Status Summary:** A table listing components and their health:

Component	Status
Ranger Admin	1 Good
Ranger Tagsync	1 Good
Ranger Usersync	1 Good
Hosts	1 Good
- Health History:** A log of health events:

Event	Timestamp
Ranger Admin Health Good	Aug 5 11:55:20 AM
1 Became Bad	Aug 5 11:55:14 AM
2 Became Good	
- Charts:** Displays 'Informational Events' and 'Important Events and Alerts' over time.

The 'Actions' dropdown menu is open, showing options: Start, Restart, Setup Ranger Admin Component, Setup Ranger Plugin Service, Stop, Add Role Instances, Rename, Enter Maintenance Mode, Refresh Ranger Usersync (highlighted), and Refresh Ranger Tagsync.

Ranger Usersync Configuration

Usersync has a lot of moving parts and can have very different outcomes. Two main sets of properties govern the way users and groups are synchronized.

Without Enable Group Search First, the primary access pattern is user-based, and groups are only searched/added based on the users it finds first. In contrast, with Enable Group Search First enabled, the primary access pattern is group-based (in turn based on the group search filter) and users are only searched/added based on the group memberships it finds first.

CLOUDERA

Manager

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Backup

Administration

Cluster 1

RANGER-1

Actions

Status

Instances

Configuration

Commands

Charts Library

Audits

Ranger Admin Web UI

Quick Links

Enable Group Search First

Role Groups

History and Rollback

Filters

Clear All

SCOPE

Clear

RANGER-1 (Service-Wide)

0

Ranger Admin

0

Ranger Tagsync

0

Ranger Usersync

2

CATEGORY

Advanced

0

Logs

0

Main

2

Monitoring

0

Performance

0

Ports and Addresses

0

Resource Management

0

Security

0

Stacks Collection

0

STATUS

Error

0

Warning

0

Edited

1

Non-default

1

Has Overrides

0

Usersync Enable User Search

Ranger Usersync Default Group

ranger.usersync.user.searchenab

led

?

Usersync Enable Group Search First

Ranger Usersync Default Group

ranger.usersync.group.search.fir

st.enabled

?

25

Per Page

22

Cluster 1

✓ RANGER-1 Actions

Aug 15, 10:19 AM PDT

Status Instances **Configuration** Commands Charts Library Audits Ranger Admin Web UI Quick Links

Usersync Search Role Groups History and Rollback

Filters Clear All

SCOPE Clear

RANGER-1 (Service-Wide)	0
Ranger Admin	0
Ranger Tagsync	0
Ranger Usersync	13

CATEGORY

Advanced	0
Logs	0
Main	13
Monitoring	0
Performance	0
Ports and Addresses	0
Resource Management	0
Security	0
Stacks Collection	0

STATUS

Error	0
Warning	0
Edited	4
Non-default	4
Has Overrides	0

Usersync Bind User
ranger.usersync.idap.binddn

Ranger Usersync Default Group

Usersync Bind User Password
ranger.usersync.idap.bindpassword

Ranger Usersync Default Group

Usersync Search Base
ranger.usersync.idap.searchBase

Ranger Usersync Default Group

OU=CorpUsers,DC=field,DC=hortonworks,DC=com

Usersync User Search Base
ranger.usersync.idap.user.searchbase

Ranger Usersync Default Group

Usersync User Search Scope
ranger.usersync.idap.user.searchscope

Ranger Usersync Default Group

☒ sub
☐ base
☐ one

Usersync User Search Filter
ranger.usersync.idap.user.searchfilter

Ranger Usersync Default Group

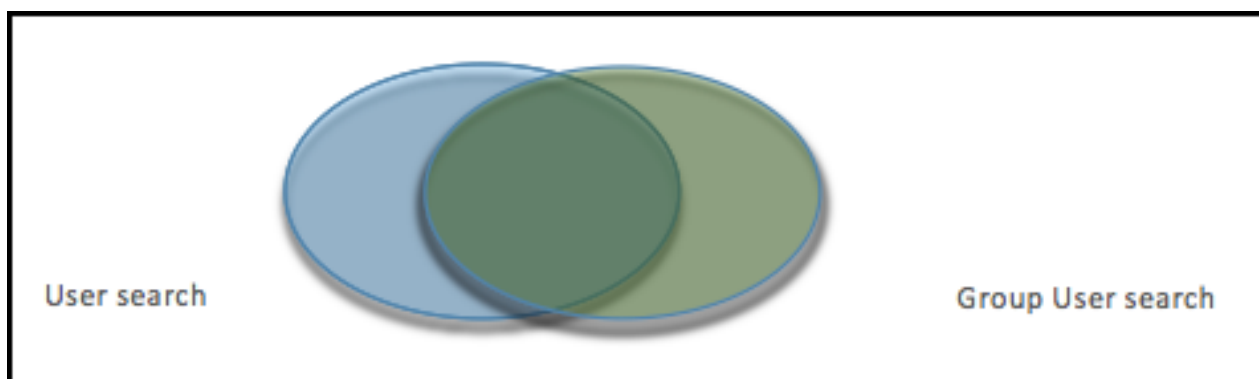
((memberOf=CN=Hdp_admins,OU=Company,OU=User

Value of 'User Search Base':
OU=CorpUsers,DC=field,DC=hortonworks,DC=com

Value of 'User Search Filter':
((memberOf=CN=Hdp_admins,OU=Company,OU=User Accounts,OU=CorpUsers,DC=field,DC=hortonworks,DC=com)(memberOf=CN=Hdp_users,OU=Company,OU=User Accounts,OU=CorpUsers,DC=field,DC=hortonworks,DC=com))

Value of 'User Group Name Attribute':
sAMAccountName

Value of 'Group Search Base':
((CN=Hdp_users)(CN=Hdp_admins))



Be aware that the filters on the group level limit the returns on the user search, and vice versa. In the graph above if the left oval represents the results of all users queried by the user configuration settings, and the right oval represents all users queried by the group configuration settings, the eventual set of users that make it to Ranger usersync is the overlap between the two.

Therefore it is recommended that you set the filters on both ends exactly the same to potentially have a 100% overlap in the ovals.

In the example configuration above, the scope of the usersync would be all members of the "Hdp_admins" and "Hdp_users" groups.

The best of both worlds is to have both Enable Group Search First and Enable User Search enabled.

The logging of a run of the usersync daemon can be retrieved from `/var/log/ranger/usersync/usersync.log` on the server hosting Ranger Admin. A successful run might output logging like below:

```

08 Dec 2016 19:40:05 INFO UserGroupSync [UnixUserSyncThread] - Begin: Initial load of user/group from source==>sink
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - LDAPUserGroupBuilder updateSink started
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Performing Group search first
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Adding Hdp_users to user
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Adding Hdp_users to user
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - No. of members in the group Hdp_users = 2
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Adding Hdp_admins to user
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Adding Hdp_admins to user
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Adding Hdp_admins to user
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - No. of members in the group Hdp_admins = 3
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - LDAPUserGroupBuilder.getGroups() completed with group count: 2
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - user search is enabled and hence computing user membership.
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Updating username far
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Updating username far
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Updating username far
08 Dec 2016 19:40:05 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Updating username far
08 Dec 2016 19:40:06 INFO LdapUserGroupBuilder [UnixUserSyncThread] - Updating username far
08 Dec 2016 19:40:06 INFO LdapUserGroupBuilder [UnixUserSyncThread] - LDAPUserGroupBuilder.getUsers() completed with user count: 5
08 Dec 2016 19:40:06 INFO UserGroupSync [UnixUserSyncThread] - End: Initial load of user/group from source==>sink
08 Dec 2016 19:40:06 INFO UserGroupSync [UnixUserSyncThread] - Done Initializing user/group source and sink

```

From that log it clearly shows that the groups are synced first and that all users belonging to those groups are then retrieved according to its own settings, after which the user parts are enriched/overwritten by the returns from the user queries.

Beware:

If you don't enable Enable User Search, that enrichment does NOT happen. Logging for such a run looks like this:

```
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LdapServerGroupBuilder initialization completed with -- ldapurl: ldap://adn1.field.hortonworks.com:389, ldapbinddn: DnsUserSearchField.Hortonworks.Com, ldapbindpw: *****, ldapauthentication: simple, ldapsearchbase: dn=*, searchscope: always, userSearchBase: [O=AdmAccount,OU=Corporate,DC=field,DC=hortonworks,DC=com], usernameAttribute: sAMAccountName, userSearchAttributes: ([sAMAccountName], userGroupAttributesSet: null, pageResultSize: true, pageResultSize: 500, groupSearchEnabled: true, groupSearchBase: [O=AdmAccount,OU=Corporate,DC=field,DC=hortonworks,DC=com], groupSearchScope: 2, groupObjectClass: group, groupSearchFilter: (&(Hdwp.users)(CN=HdpAdmin)), extendedGroupSearchFilter: (&(ObjectClass=user)(CN=HdpUsers)(CN=HdpAdmin)), extendedAdmUserSearchFilter: (&(ObjectClass=user)(CN=HdpUsers)(CN=HdpAdmin))), groupMemberAttribute: groupName, groupMemberAttribute: n
00 Dec 2016 18:24:29 INFO UserGroupSync [DnsUserSyncThread] - Begin: Initial load of user/group from source=sink
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LDAPServerGroupBuilder updatesink started
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - Performing Group search first
00 Dec 2016 18:24:29 INFO PolicyLdapServerGroupBuilder [DnsUserSyncThread] - Using principal = ranguensysync/rjk-hq25-m-60BFIELD.HORTONWORKS.COM and keytab = /etc/security/keytabs/ranguensysync.service.keytab
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - Adding HdpUsers to user
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - Adding HdpUsers to user
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - No. of members in the group Hdp.Users = 2
00 Dec 2016 18:24:29 INFO PolicyLdapServerGroupBuilder [DnsUserSyncThread] - Using principal = ranguensysync/rjk-hq25-m-60BFIELD.HORTONWORKS.COM and keytab = /etc/security/keytabs/ranguensysync.service.keytab
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - Adding HdpAdmins to user
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - Adding HdpAdmins to user
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - Adding HdpAdmins to user
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - Adding HdpAdmins to user
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - No. of members in the group Hdp.admins = 3
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LDAPServerGroupBuilder.getGroups() completed with group count: 2
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - User search is disabled and hence using the group member attribute for username.
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LongIdentifier:
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LongIdentifier:
00 Dec 2016 18:24:29 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LongIdentifier:
00 Dec 2016 18:24:30 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LongIdentifier:
00 Dec 2016 18:24:30 INFO LdapServerGroupBuilder [DnsUserSyncThread] - LongIdentifier:
00 Dec 2016 18:24:30 INFO UserGroupSync [DnsUserSyncThread] - End: Initial load of user/group from source=sink
00 Dec 2016 18:24:30 INFO UserGroupSync [DnsUserSyncThread] - Done Initializing user/group source and sink
```

The result in the Ranger UI are other user names (LongUserName) derived from "member" group attributes full DN. You get the long name "James Kirk" in the Ranger userlist instead of "j.kirk". Ranger does not treat those as one and the same user. Policies that are defined for user "k.reshi" will not map to the user "Kvothe Reshi", and vice versa. To prevent any confusion it is probably best to delete the long username versions from the Rangers user list.

**Important:**

On the first page of Rangers user list there are many system users. Most of them were put there by the Ranger installer and during the plugins installs:

The screenshot shows the Ranger web interface with the 'Users' tab selected. The 'User List' section displays a table of system users. The table has columns for User Name, Email Address, Role, User Source, Groups, and Visibility. The users listed are: admin, rangerusersync, rangertagsync, hive, cloudera-scm, https, superset, atlas, ranger, kudu, kms, accumulo, polkitd, nfsnobody, spark, flume, solr, jenkins, hbase, zookeeper, oozie, zeppelin, impala, gluster, and systest. Each user has a checkbox in the first column and a 'Visible' status in the last column. The 'Role' column shows 'Admin' for the first three users and 'User' for the others. The 'User Source' column shows 'Internal' for the first three and 'External' for the others. The 'Groups' column shows the groups associated with each user.

	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
<input type="checkbox"/>	hbase		User	External	hbase	Visible
<input type="checkbox"/>	zookeeper		User	External	zookeeper	Visible
<input type="checkbox"/>	oozie		User	External	oozie	Visible
<input type="checkbox"/>	zeppelin		User	External	zeppelin	Visible
<input type="checkbox"/>	impala		User	External	hive impala	Visible
<input type="checkbox"/>	gluster		User	External	gluster	Visible
<input type="checkbox"/>	systest		User	External	wheel systest	Visible

Do NOT remove these system users!

There are basic access policies based on those system users designed to keep a Ranger-governed component working after Ranger is given all control over that component's authorizations. Without those policies/users many components may not function as expected.

Ranger user management

Reference information on Ranger user management, when configuring Ranger AD integration.

To delete a user, select the check box for the user in the User Name list, then click the red Delete button. Ranger removes the user from all policies.

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"/>	hdfs		User	External	hadoop hdfs	Visible
<input type="checkbox"/>	rangerlookup		User	External	--	Visible
<input type="checkbox"/>	livy		User	External	livy	Visible
<input type="checkbox"/>	chrony		User	External	chrony	Visible
<input type="checkbox"/>	druid		User	External	hadoop druid	Visible
<input type="checkbox"/>	kafka		User	External	kafka	Visible
<input type="checkbox"/>	knoxui		User	External	knoxui	Visible
<input type="checkbox"/>	yarn		User	External	hadoop yarn	Visible
<input type="checkbox"/>	hue		User	External	hue	Visible
<input type="checkbox"/>	sqoop		User	External	sqoop	Visible
<input type="checkbox"/>	centos		User	External	systemd-journal wheel adm centos	Visible
<input type="checkbox"/>	storm		User	External	--	Visible
<input type="checkbox"/>	knox		User	External	hadoop knox	Visible
<input type="checkbox"/>	mapred		User	External	hadoop mapred	Visible
<input type="checkbox"/>	nifi		User	External	--	Visible
<input type="checkbox"/>	tez		User	External	tez	Visible
<input type="checkbox"/>	auditor1		Auditor	Internal	--	Visible
<input type="checkbox"/>	new-user1		Admin	Internal	--	Visible
<input checked="" type="checkbox"/>	asmith		Admin	Internal	public	Visible

« ‹ 1 2 › »

Known issue: Ranger group mapping

For Ranger AD integration, there is an issue with Ranger not being able to map a user on a group 'Hdp_admins' to a policy that allows/denies access to the group 'Hdp_admins'. The issue is the upper case characters that might be in a AD group name definition.

Most HDP components get the group information for a user via the SSSD daemon. When asked for the groups the user 'd.threpe' belongs to we get:

```
[centos@rjk-hdp25-m-01 ~]$ groups d.threpe
d.threpe : domain_users hdp_admins hadoop
```

So 'hdp_admins' all in lower case. Ranger does not treat this as the same value as 'Hdp_admins' which came via the group sync and was applied to some policies.

There is no way to make the group sync write or retrieve the group names all in lower case since there is no AD attribute that rewrites it in lowercase.

This issue can be worked around fortunately (till it gets solved). The solution is to define a local group in Ranger as a shadow group of a real group from AD, but then all in lower case:

<input type="checkbox"/>	systemd-bus-proxy	External
<input type="checkbox"/>	slider	External
<input type="checkbox"/>	sssd	External
<input type="checkbox"/>	Hdp_users	External
<input type="checkbox"/>	Hdp_admins	External
<input type="checkbox"/>	hdp_admins	Internal
<input type="checkbox"/>	hdp_users	Internal

If we now create policies and use that lower case ‘shadow’ group literal the result is that policies are correctly mapped to the AD groups again:

List of Policies : HDP_...atlas

Policy ID	Policy Name	Status	Audit Logging	Groups
9	all - taxonomy	Enabled	Enabled	Hdp_admins hdp_users hdp_admins
10	all - operation	Enabled	Enabled	Hdp_admins hdp_admins hdp_users
11	all - type	Enabled	Enabled	Hdp_admins hdp_admins hdp_users
12	all - entity	Enabled	Enabled	Hdp_admins hdp_users
13	all - term	Enabled	Enabled	Hdp_admins hdp_users hdp_admins

*The ‘Hdp_admins’ entry does not have to be there, it is shown for clarification only. ‘hdp_admins’ is necessary to make it work.