

Configuring Apache Ranger Authentication with UNIX, LDAP, or AD

Date published:

Date modified:

The Cloudera logo, featuring the word "CLOUDERA" in a bold, orange, sans-serif font. The letter "E" is stylized with a horizontal bar through its center.

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
 Configure Ranger Usersync for Deleted Users and Groups.....	 20

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 'RANGER-1' configuration page. The 'Configuration' tab is selected, and the search filter is 'authentication unix'. The 'Filters' section on the left shows counts for SCOPE, CATEGORY, and STATUS. The main configuration area includes the following settings:

- Admin Authentication Method:** ranger.authentication.method is set to **UNIX** (selected). Other options are LDAP, ACTIVE_DIRECTORY, PAM, and NONE.
- Admin UNIX Auth Remote Login:** ranger.unixauth.remote.login.enabled is checked. The default group is 'Ranger Admin Default Group'.
- Admin UNIX Auth Service Hostname:** ranger.unixauth.service.hostname is set to `{{RANGER_USERSYNC_HOST}}`. The default group is 'Ranger Admin Default Group'.
- Unix Auth Service Hostname:** ranger.usersync.port is set to **5151**. The default group is 'Ranger Usersync Default Group'.
- Admin Unix Auth Service Port:** ranger.unixauth.service.port is set to **5151**. The default group is 'Ranger Admin Default Group'.

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

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 configuring Ranger-1. The search bar at the top contains the text "authentication unix". The left sidebar shows the navigation menu with "Clusters" selected. The main content area displays the configuration for "RANGER-1" under the "Configuration" tab. The search results show filters for SCOPE, CATEGORY, and STATUS. The configuration details for "Admin Authentication Method" are shown, with "UNIX" selected. Other settings include "Admin UNIX Auth Remote Login", "Admin UNIX Auth Service Hostname", "Unix Auth Service Hostname", and "Admin Unix Auth Service Port".

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

Aug 13, 12:07 PM PDT

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Backup

Administration

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_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.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

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 "Clusters" selected. The main panel displays the configuration for Ranger-1, including filters for SCOPE, CATEGORY, and STATUS. The configuration settings for authentication are shown, including Admin Authentication Method (LDAP), 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.

- 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.

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 has 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'. These sections include 'Shards for Solr Collection of Ranger Audits', 'Maximum Shards for Solr Collection of Ranger Audits', 'Replicas for Solr Collection of Ranger Audits', 'Admin UNIX Auth Remote Login', 'Admin UNIX Auth Service Hostname', 'Admin LDAP Auth URL', 'Admin LDAP Auth Bind User', 'Admin LDAP Auth Bind User Password', 'Admin LDAP Auth User DN Pattern', and 'Admin LDAP Auth User Search Filter'. At the bottom of the page, there is a status bar indicating '1 Edited Value' and a 'Reason for change: Modified Admin Authentication Method'. A '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

```

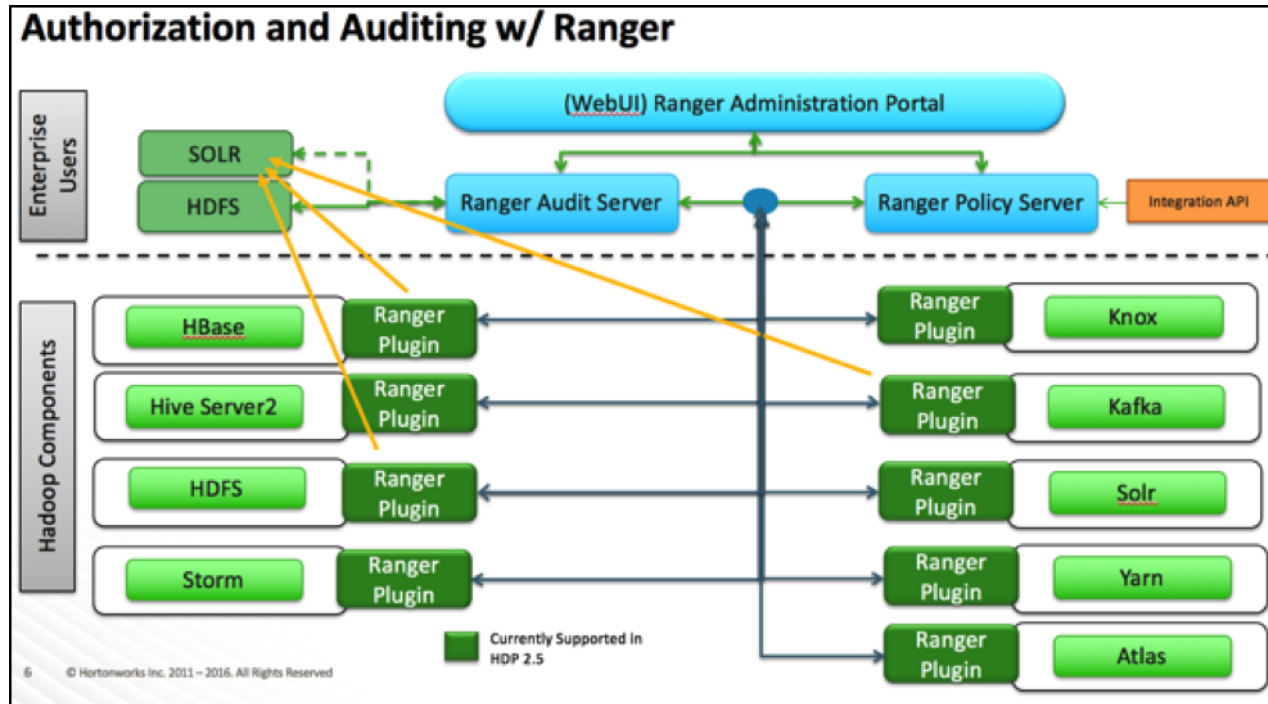
```
account sufficient pam_sss.so
```

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:

CLUSTER
Manager

Search

Clusters

- Hosts
- Diagnostics
- Audits
- Charts
- Backup
- Administration

CDEP Deployment from 2019-Aug-05 11:11

Parcels

Recent Commands

Support

admin

Cluster 1

HDFS-1 Actions

Aug 14, 11:38 AM PDT

Status Instances **Configuration** Commands File Browser Charts Library Cache Statistics Audits NameNode Web UI Quick Links

Search

Role Groups History and Rollback

Filters Clear All

SCOPE

HDFS-1 (Service-Wide)	51
Balancer	0
DataNode	1
Gateway	0
HttpFS	7
JournalNode	0
NFS Gateway	0
NameNode	2
SecondaryNameNode	0
Failover Controller	0

CATEGORY Clear

Advanced	95
Checkpointing	2
Cloudera Navigator	4
Erasure Coding	4
High Availability	5
Logs	37
Main	44
Monitoring	100
Performance	20
Ports and Addresses	26

Superuser Group HDFS-1 (Service-Wide)
dfs.permissions.superusergroup
supergroup

Kerberos Principal HDFS-1 (Service-Wide)
hdfs
Kerberos principal short name used by all roles of this service.

HDFS User to Impersonate HDFS-1 (Service-Wide)

Hue's Kerberos Principal Short Name HDFS-1 (Service-Wide)
hue.kerberos.principal.shortname

DataNode Data Transfer Protection HDFS-1 (Service-Wide)
dfs.data.transfer.protection
☒ Authentication
☐ Integrity

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.clouderz

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 : ☐ 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

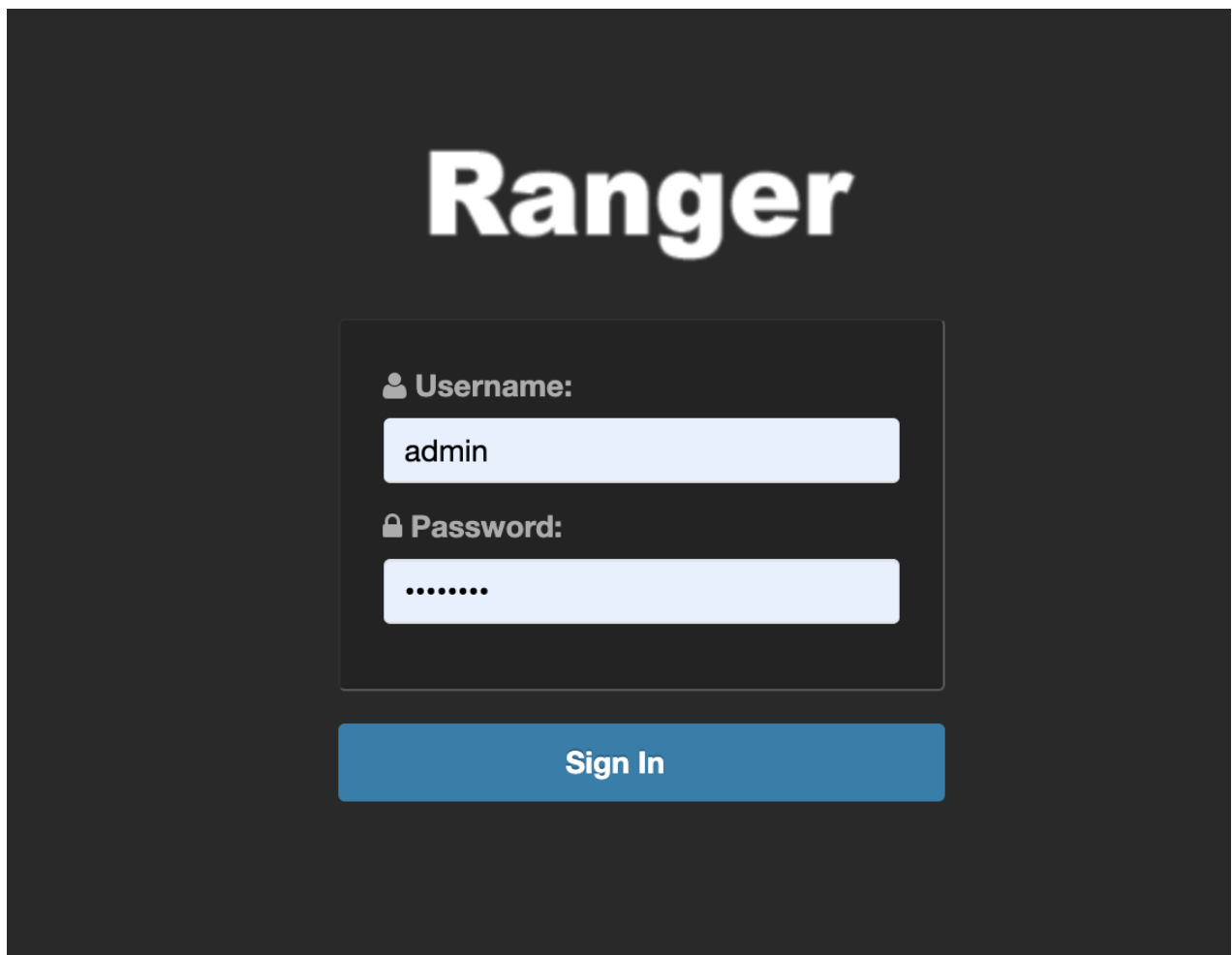
Rangers AD Integration has 2 levels:

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:

The image shows the Ranger UI authentication login screen. It has a dark gray background. At the top center, the word "Ranger" is written in a large, white, sans-serif font. Below it, there is a white rectangular box containing the login fields. Inside this box, the label "Username:" is followed by a text input field containing the text "admin". Below that, the label "Password:" is followed by a text input field filled with dots. At the bottom of the white box, there is a blue rectangular button with the text "Sign In" in white.

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 content area is titled 'Cluster 1' and shows the 'Configuration' tab for 'RANGER-1'. A search box at the top of the configuration area contains the word 'authentication'. Below the search box, there are filters for SCOPE, CATEGORY, and STATUS. The SCOPE filter shows 'RANGER-1 (Service-Wide)' with a count of 0, 'Ranger Admin' with 19, 'Ranger Tagsync' with 1, and 'Ranger Usersync' with 2. The CATEGORY filter shows various categories like Advanced, Logs, Main, Monitoring, Performance, Ports and Addresses, Resource Management, Security, and Stacks Collection, all with counts. The STATUS filter shows Error (0), Warning (0), Edited (2), Non-default (2), and Has Overrides (0). 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.reshi` and `d.alora` so make sure to enter a matching value for 'Username' in the login 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.

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 'authentication' configuration. The configuration is divided into two main sections: Filters and Admin Authentication. The Filters section includes SCOPE, CATEGORY, and STATUS filters. The Admin Authentication section includes fields for Method (LDAP selected), 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.

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

	User Name	Email Address	Role	User Source	Groups	Visibility
☐	admin		Admin	Internal	--	Visible
☐	rangerusersync		Admin	Internal	--	Visible
☐	rangertagsync		Admin	Internal	--	Visible
☐	hive		User	External	hive	Visible
☐	cloudera-scm		User	External	wheel cloudera-scm	Visible
☐	https		User	External	https	Visible
☐	superset		User	External	superset	Visible
☐	atlas		User	External	hadoop atlas	Visible
☐	ranger		User	External	hadoop ranger	Visible
☐	kudu		User	External	kudu	Visible
☐	kms		User	External	kms	Visible
☐	accumulo		User	External	accumulo	Visible
☐	polkitd		User	External	polkitd	Visible
☐	nfsnobody		User	External	nfsnobody	Visible
☐	spark		User	External	spark	Visible
☐	flume		User	External	flume	Visible
☐	solr		User	External	solr	Visible
☐	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.

Configure Ranger Usersync for Deleted Users and Groups

How to configure Ranger Usersync for users and groups that have been deleted from the sync source.

About this task

You can configure Ranger Usersync to update Ranger when users and groups have been deleted from the sync source (UNIX, LDAP, AD or PAM). This ensures that users and groups – and their associated access permissions – do not remain in Ranger when they are deleted from sync source.

Procedure

1. In Cloudera Manager, select Ranger > Configuration, then use the Search box to search for Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml. Use the Add (+) icons to add the following properties, then click Save Changes.

Name	Value	Description
ranger.usersync.deletes.enabled	true	Enables deleted users and groups synchronization. The default setting is false (disabled).

Name	Value	Description
ranger.usersync.deletes.frequency	10	Sets the frequency of delete synchronization. The default setting is 10, or once every 10 Usersync cycles. Delete synchronization consumes cluster resources, so a lower (more frequent) setting may affect performance.

CLOUDERA
Manager

- Clusters
- Hosts
- Diagnostics
- Audits
- Charts
- Replication
- Administration
- Private Cloud New

- Parcels
- Running Commands
- Support
- admin

7.4.2

Cluster 1

RANGER-1
Actions
Jun 4, 8:57 PM UTC

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

Filters (1)
Role Groups
History & Rollback

Filters (1) Clear All

SCOPE

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

CATEGORY

Advanced 1
Database 0
Logs 0
Main 0
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
Include Overrides 0

Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml

Name

ranger.usersync.deletes.enabled

Value

true

Description

☐ Final

Name

ranger.usersync.deletes.frequency

Value

10

Description

☐ Final

Show All Descriptions

View as XML

1 - 1 of 1

1 Edited Value

Reason for change:

Modified Ranger Usersync Advanced Configuration Snippet (Safety Valve) for c

Save Changes(CTRL+S)

2. Click the Ranger Restart icon.

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Private Cloud New

Parcels

Running Commands

Cluster 1

RANGER-1

Actions

Stale Configuration: Restart

Command needed

Charts Library

Jun 4, 8:58 PM UTC

Status

Instances

Configuration

Audits

Ranger Admin Web UI

Quick Links

Q ranger-ugsync-site.xml

Filters (1)

Role Groups

History & Rollback

Filters (1)

Clear All

SCOPE

Clear

RANGER-1 (Service-Wide)

0

Ranger Admin

0

Ranger Tagsync

0

Ranger Usersync

1

CATEGORY

Advanced

1

Database

0

Logs

0

Main

0

Monitoring

0

Performance

0

Ports and Addresses

0

Resource Management

0

Security

0

Stacks Collection

0

STATUS

Error

0

Warning

0

Edited

0

Non-Default

1

Ranger Usersync Advanced Configuration Snippet (Safety Valve) for conf/ranger-ugsync-site.xml

conf/ranger-ugsync-site.xml_role_safety_valve

Ranger Usersync Default Group

Show All Descriptions

View as XML

Name

ranger.usersync.deletes.enabled

Value

true

Description

Final

Name

ranger.usersync.deletes.frequen

Value

10

Description

Final

3. On the Stale Configurations page, click Restart Stale Services.

Cluster 1

Stale Configurations

File: conf/ranger-ugsync-site.xml RANGER-1(1) [Show](#)

```

... .. @@ -197,6 +197,14 @@
197 197 <property>
198 198 <name>ranger.usersync.kerberos.principal</name>
199 199 <value>rangerusersync/_HOST@ROOT.HWX.SITE</value>
200 200 </property>
201 201 + <property>
202 202 + <name>ranger.usersync.deletes.enabled</name>
203 203 + <value>true</value>
204 204 + </property>
205 205 + <property>
206 206 + <name>ranger.usersync.deletes.frequency</name>
207 207 + <value>10</value>
208 208 + </property>
209 209 </configuration>
210 210

```

File: conf/rangeradmin.properties RANGER-1(1) [Show](#)

```

... .. @@ -1,5 +1,9 @@
1 1 dhoyl717-1.dhoyl717.root.hwx.site:ranger.externalurl=
2 2 dhoyl717-1.dhoyl717.root.hwx.site:ranger.service.http.port=6080
3 3 dhoyl717-1.dhoyl717.root.hwx.site:ranger.service.https.attrib.ssl.enabled=fa
4 4 dhoyl717-1.dhoyl717.root.hwx.site:ranger.service.https.port=6182
5 5 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.externalurl=
6 6 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.service.http.port=6080
7 7 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.service.https.attrib.ssl.enabled=fa
8 8 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.service.https.port=6182
9 9

```

File: conf/rangeradmin.properties RANGER-1(2) [Show](#)

```

... .. @@ -2,5 +2,10 @@
2 2 dhoyl717-1.dhoyl717.root.hwx.site:ranger.externalurl=
3 3 dhoyl717-1.dhoyl717.root.hwx.site:ranger.service.http.port=6080
4 4 dhoyl717-1.dhoyl717.root.hwx.site:ranger.service.https.attrib.ssl.enabled=fa
5 5 dhoyl717-1.dhoyl717.root.hwx.site:ranger.service.https.port=6182
6 6 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.authentication.method=PAM
7 7 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.externalurl=
8 8 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.service.http.port=6080
9 9 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.service.https.attrib.ssl.enabled=fa
10 10 +dhoyl717-2.dhoyl717.root.hwx.site:ranger.service.https.port=6182
11 11

```

[Restart Stale Services](#)

4. On the Restart Stale Services page, select the Re-deploy client configuration check box, then click Restart Now.

Restart Stale Services

1 Review Changes

2 Command Details

Review Changes

All services running with outdated configurations in the cluster and their dependencies will be restarted.

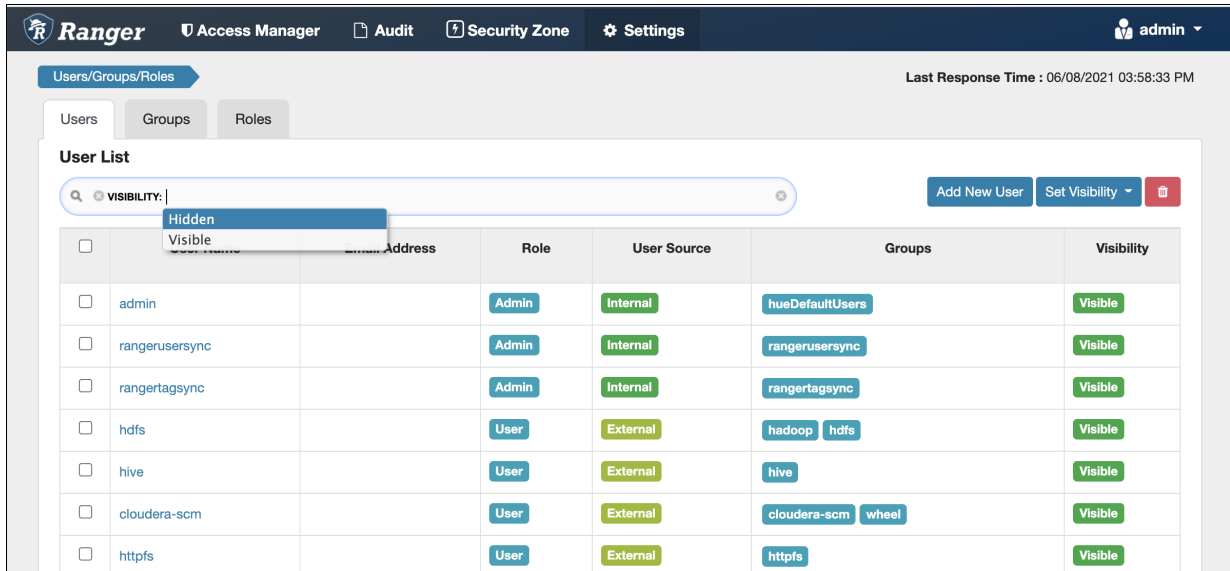
☒ Re-deploy client configuration

[Back](#) [Restart Now](#)

5. A progress indicator page appears while the services are being restarted. When the services have restarted, click Continue.

6. Users that have been deleted in sync source are not automatically deleted in Ranger – they are marked as Hidden and must be manually deleted by the Ranger Admin user, and then Ranger Usersync must be restarted.

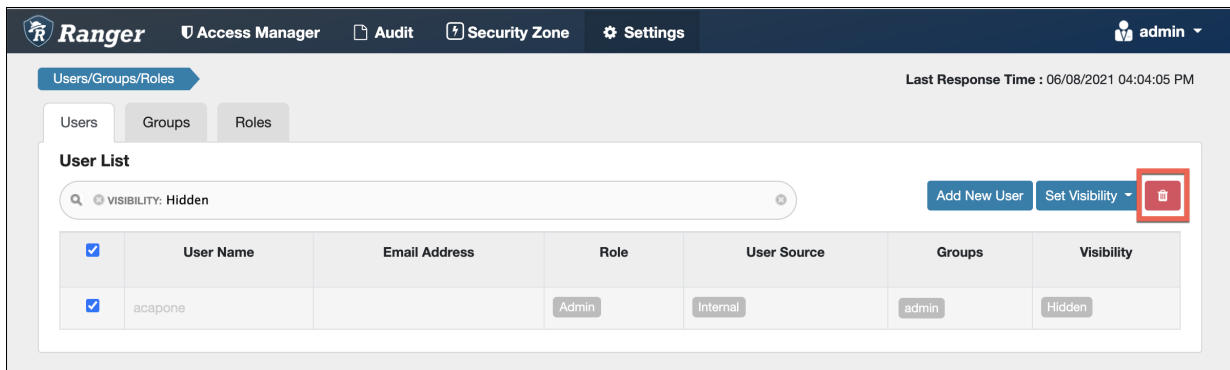
In the Ranger Admin Web UI, select Settings > Users/Groups/Roles. Click in the User List text box, then select Visibility > Hidden.



The screenshot shows the Ranger Admin Web UI. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. The 'Users/Groups/Roles' section is active, with 'Users' selected. The 'User List' is displayed with a search bar and a dropdown menu for 'VISIBILITY'. The dropdown menu is open, showing 'Hidden' and 'Visible' options. The table below lists users with columns for checkboxes, User Name, Email Address, Role, User Source, Groups, and Visibility.

	User Name	Email Address	Role	User Source	Groups	Visibility
☐	admin		Admin	Internal	hueDefaultUsers	Visible
☐	rangerusersync		Admin	Internal	rangerusersync	Visible
☐	rangertagsync		Admin	Internal	rangertagsync	Visible
☐	hdfs		User	External	hadoop hdfs	Visible
☐	hive		User	External	hive	Visible
☐	cloudera-scm		User	External	cloudera-scm wheel	Visible
☐	httpfs		User	External	httpfs	Visible

7. To delete a hidden user or group manually, select the applicable check boxes, then click the red Delete icon, as shown in the following example.



The screenshot shows the Ranger Admin Web UI. The top navigation bar is the same. The 'Users/Groups/Roles' section is active, with 'Users' selected. The 'User List' is displayed with a search bar and a dropdown menu for 'VISIBILITY'. The dropdown menu is set to 'Hidden'. The table below lists users with columns for checkboxes, User Name, Email Address, Role, User Source, Groups, and Visibility. A red box highlights the 'Delete' icon (a trash can) in the top right corner of the table.

	User Name	Email Address	Role	User Source	Groups	Visibility
☒	acapone		Admin	Internal	admin	Hidden

You can delete multiple users or groups by running a "delete" script on the command line interface.

For example:

Sample command to delete users:

```
python deleteUserGroupUtil.py -users <user file path> -admin <ranger admin user> -url <rangerhosturl> [-force] [-sslCertPath <cert path>] [-debug]
```

Sample command to delete groups:

```
python deleteUserGroupUtil.py -groups <group file path> -admin <ranger admin user> -url <rangerhosturl> [-force] [-sslCertPath <cert path>] [-debug]
```



Note: The deleteUserGroupUtil.py script installs as part of the Ranger installation on the node where Ranger Admin runs, in the following location: /opt/cloudera/parcels/CDH/lib/ranger-admin/.

8. In Cloudera Manager, select Ranger > Ranger Usersync, then select Actions > Restart this Ranger Usersync.

The screenshot shows the Cloudera Manager interface for the Ranger Usersync service. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The main content area displays the 'Ranger Usersync' configuration page for 'Cluster 1 / RANGER-1 / dhoye717-1'. The 'Actions' dropdown menu is open, showing options to start, stop, restart, enter maintenance mode, refresh, list open files, collect stack traces, heap dump, and heap histogram. The 'Health Tests' section shows 4 Good and 2 Disabled tests. The 'Health History' section shows a list of events, including '2 Became Good', '2 Became Disabled', '1 Became Good', and '1 Became Unknown'. A 'VM Heap Memory Usage' chart is visible on the right, showing memory usage over time for 'ranger_usersync...' and 'ranger_usersync...'.



Note:

- Sync source is tracked when processing Ranger users and groups for deletion. If the same user name for a separate sync source already exists in Ranger DB, that user will not be updated or marked as hidden.
- For AD/LDAP sync:
 - After marking a user or group as deleted/hidden in Ranger, the user or group status does not change automatically. The user or group must be manually deleted (or deleted using the cli "delete" script). Usersync must be restarted to reflect any changes to the same user name in the source.
 - For example, a user (Bob) from one OU (say Engineering) is deleted from the source and is marked as deleted in Ranger admin. If the same user name (Bob) is subsequently added back to the same OU, the user status will not be automatically enabled. The user must be manually deleted and Usersync must be restarted to implement the changes.
 - If an identical user name (say Bob) is deleted from one OU (say Engineering) and added to a different OU (say Finance) between the sync cycles, user Bob is marked as hidden/deleted only when the delete cycle is triggered. Until then there is a security risk that user Bob from Finance will be granted the permissions for Bob from Engineering.