Cloudera Flow Management 1

Securing Cloudera Flow Management

Date of Publish: 2019-04-15

https://docs.hortonworks.com/

Contents

Enabling TLS 3

Enable TLS for NiFi 3
Enable TLS for NiFi Registry 4
Using External Certificates 5
Using Custom Certificate DN Support 6

Authentication Strategies 7

Get Client Certificates for Authentication 7
Configure Kerberos Authentication 8
Configure LDAP Authentication 8
LDAP Login Identity Provider Configuration 8
LDAP User Sync Configuration 10

Security Configuration Templates 12

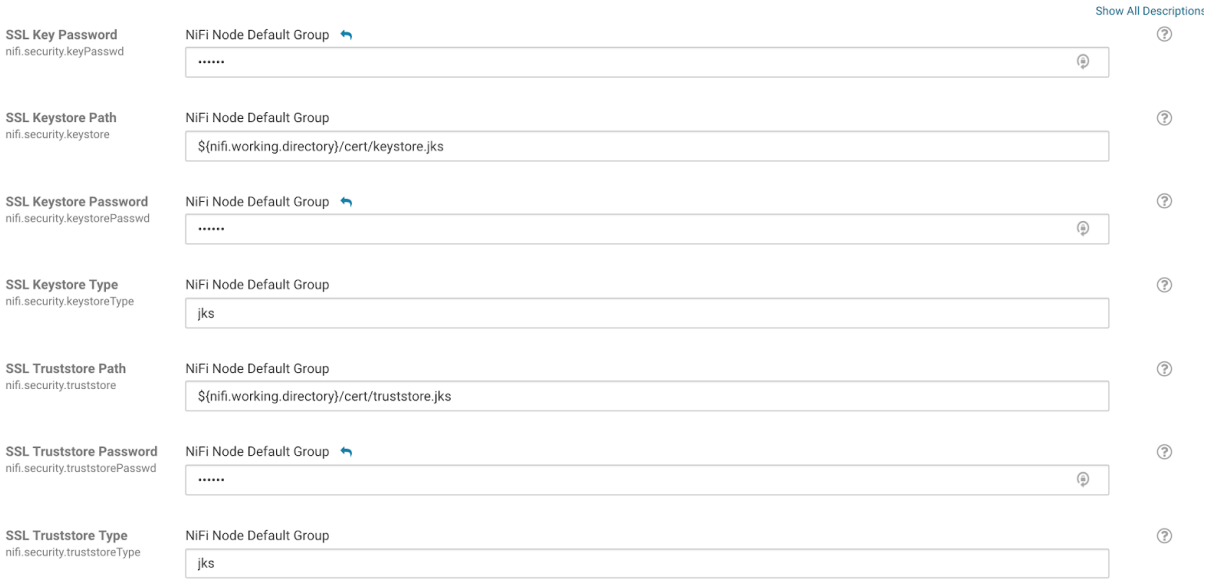
NiFi User Sync LDAP Properties 12
NiFi Registry LDAP TLS Property Configuration 15

Enabling TLS

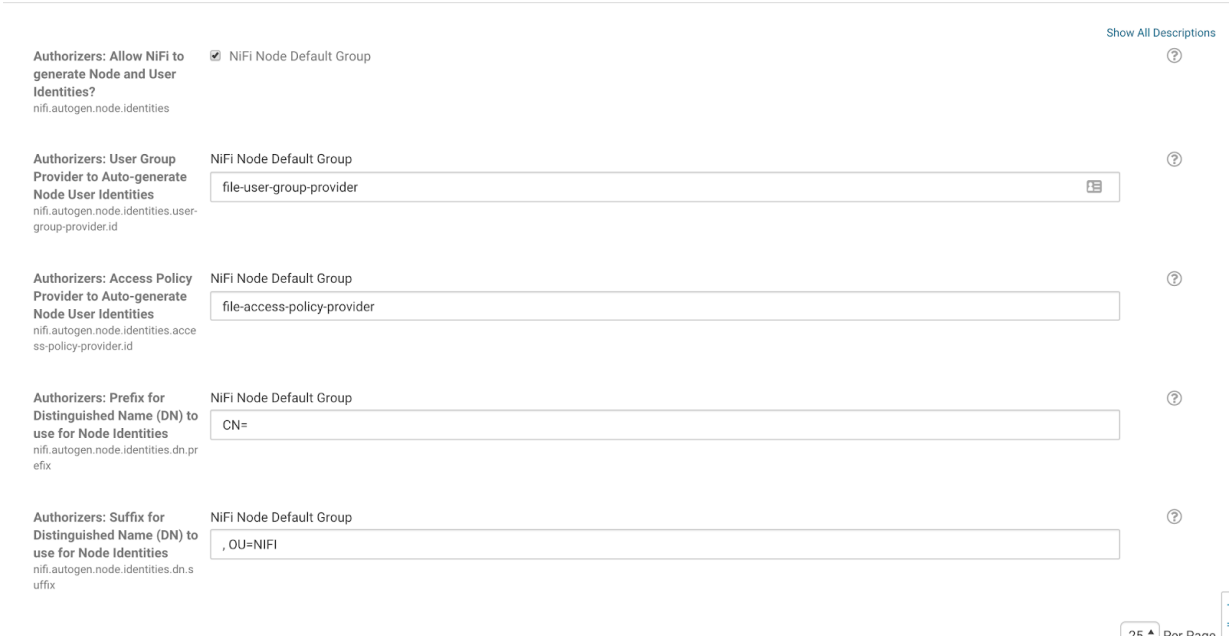
Enable TLS for NiFi

Procedure

1. Ensure that the **NiFi Toolkit CA Service** radio button is selected.
2. In the **Enable TLS/SSL for NiFi Node** field, check the **NiFi Node Default Group** box.
3. In the **Initial Admin Identity** field, specify the information you will use to identify the initial admin user. For example, client certificate distinguished name (dn), Kerberos user, or LDAP user.
4. In the **NiFi CA Force Regenerate** field, check the **NiFi Node Default Group** box.
5. Review and update the location of the keystores and truststores, as needed.



6. Confirm that NiFi is allowed to auto-generate node identities. Set the prefix and suffix to values used in NiFi CA. (NOTE, ensure suffix that starts with comma has a space. Known issue exist for NiFi CA where space isn't allowed after comma). Also ensure that it is aligned with a defined user group provider (by default this is the default file-user-group-provider)
   - You must ensure that any suffix starting with a comma includes a trailing space.
   - Verify that the suffix is aligned with a defined user group provider. By default, file-user-group-provideris specified.



What to do next

- If you are using Client Certificates for authentication and user authorization, restart the service and log in with the Initial Admin Certificate. If you need to create a client certificate see *Get Client Certificates for Authentication*.
- If you are integrating with Kerberos or LDAP, continue with further configuration defined below.

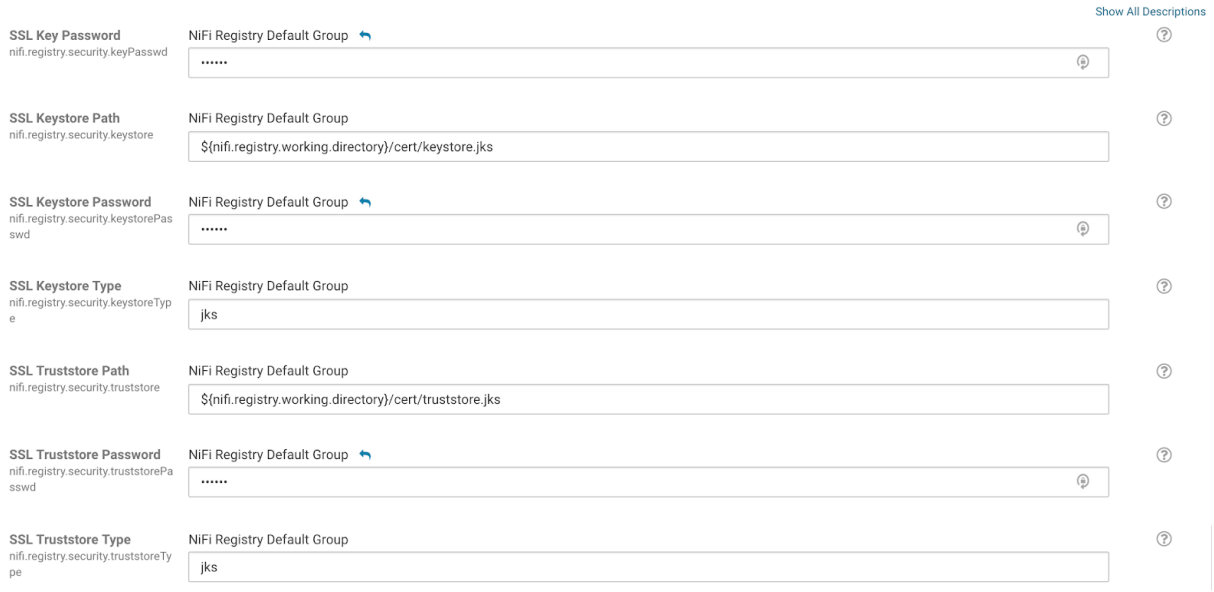
Related Information

Get Client Certificates for Authentication

Enable TLS for NiFi Registry

Procedure

1. Ensure that the **NiFi Toolkit CA Service** radio button is selected.
2. In the **Enable TLS/SSL for NiFi Registry** field, check the **NiFi Registry Default Group** box.
3. In the **Initial Admin Identity** field, specify the information you will use to identify the initial admin user. For example, client certificate distinguished name (dn), Kerberos user, or LDAP user.
4. In the **NiFi Registry CA Force Regenerate** field, check the **NiFi Node Default Group** box.
5. Review and update the location of the keystores and truststores, as needed.



What to do next

- If you are using Client Certificates for authentication and user authorization, restart the service and log in with the Initial Admin Certificate. If you need to create a client certificate see *Get Client Certificates for Authentication*.
- If you are integrating with Kerberos or LDAP, continue with further configuration defined below.

Related Information

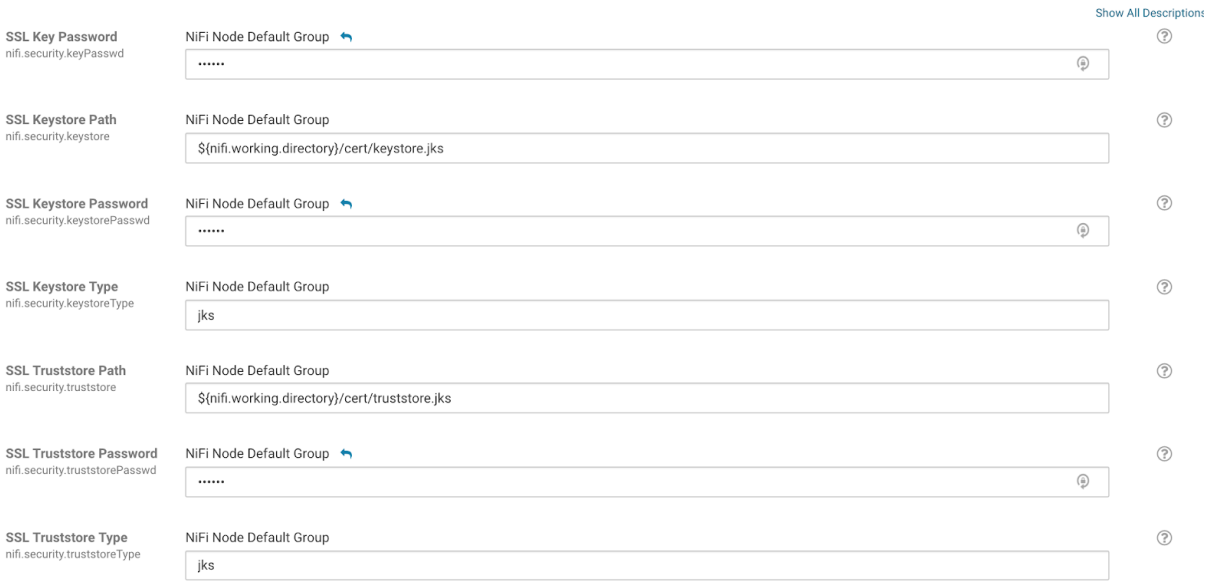
Get Client Certificates for Authentication

Using External Certificates

You can use an external CA or external self-signed certificates by updating some of the configuration values in Cloudera Manager.

Procedure

1. In the **NiFi Toolkit CA Service** field, deselect the Toolkit CA Service by setting the radio button to **None**.
2. In the **Enable TLS/SSL** field, enable TLS by clicking the **NiFi Node Default Group** box.
3. Update keystore and truststore information for provided certificates.



4. Review Auto-generate Node Identities settings to ensure prefix and suffix match those in certificates.

   For auto-generate to work successfully externally created certificates should identify, within the common name, the fully qualified hostname for each agent running a nifi node e.g. CN=hostname.local, OU=NIFI.

Using Custom Certificate DN Support

If you cannot use the auto-generate feature for Node Identities, given the structure for the DN in the certificates for nodes, you can use the authorizers.xml safety valve to identify node nodes by DN.

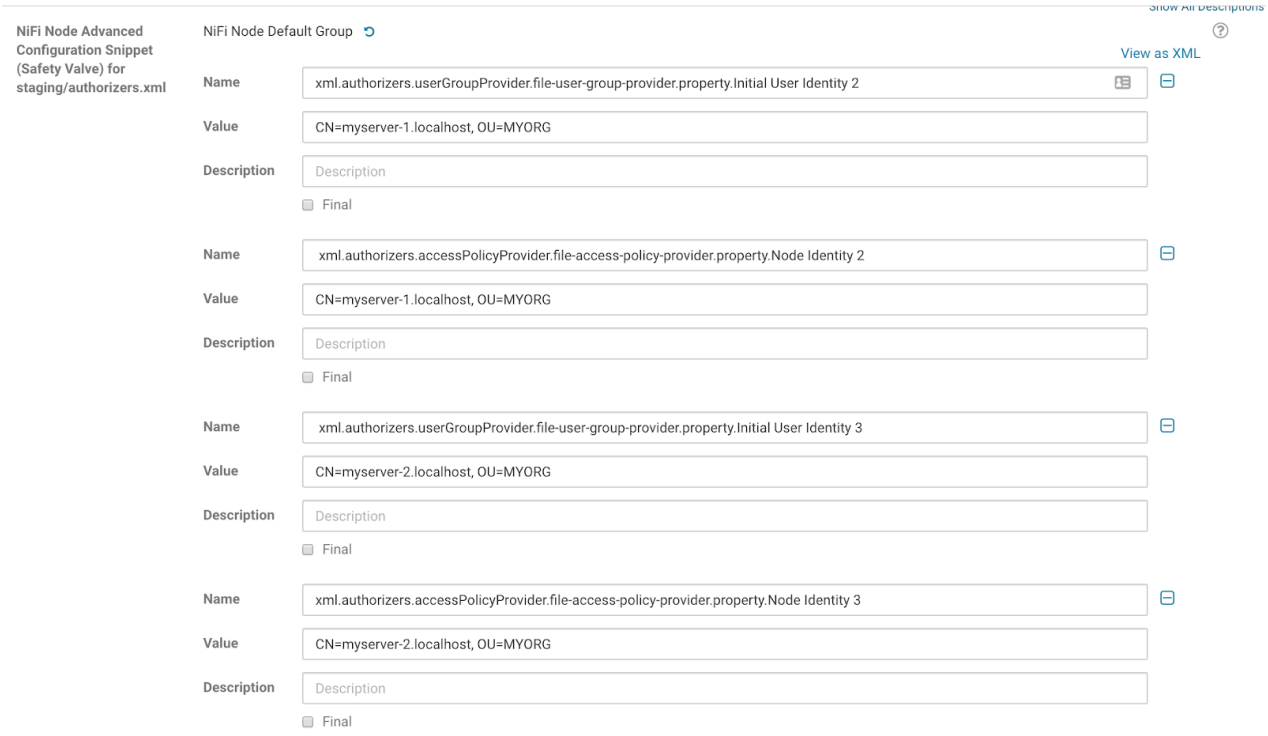
Using the authorizers.xml safety valve, enter xml properties for Node and User identities to identify nodes by DN. Both Node and User Identities should be defined starting at number 2. The below example shows configuration properties for 2 nodes using the default File User Group and default File Access Policy Provider:

```
Name: xml.authorizers.userGroupProvider.file-user-group-
provider.property.Initial User Identity 2
Value: CN=myserver-1.localhost, OU=MYORG

Name: xml.authorizers.accessPolicyProvider.file-access-policy-
provider.property.Node Identity 2
Value: CN=myserver-1.localhost, OU=MYORG

Name: xml.authorizers.userGroupProvider.file-user-group-
provider.property.Initial User Identity 3
Value: CN=myserver-2.localhost, OU=MYORG

Name: xml.authorizers.accessPolicyProvider.file-access-policy-
provider.property.Node Identity 3
Value: CN=myserver-2.localhost, OU=MYORG
```



Authentication Strategies

Get Client Certificates for Authentication

After you install NiFi CA, you can use the NiFi Toolkit to generate a client certificate for users you wish to authenticate. You can do this with NiFi Toolkit binaries running locally or located on agent machines where CFM is installed.

Example of creating a client certificate using the NiFi Toolkit in CFM parcel:

```
#ensure java home is set before execution
<parcel_home_dir>/CFM/TOOLKIT/bin/tls-toolkit.sh client
-c <nifi-ca-host-fdqn>
-t <nifi-ca-token>
-p <nifi-ca-port
-D <user-dn>
-T PKCS12
```

Once pkcs12 keystore is created, use the password information from the config.json to import the keystore.pkcs12 file into browser.

When you are logging into a secured NiFi or NiFi Registry instance, services search first for any client certificate imported in the browser for authentication. If the client certificate exists and the certificate DN/ Identity represents a user that is authorized to access the UI or Flow (as an initial admin or manually configured user in NiFi/NiFi Registry), they are successfully logged in. Otherwise, if a login-identity provider is configured for Kerberos/LDAP, a login screen displays.

Related Information

Enable TLS for NiFi

Enable TLS for NiFi Registry

Configure Kerberos Authentication

Both NiFi and NiFi Registry support authentication supported by Kerberos/Spnego. Cluster must have Kerberos enabled before proceeding. See Cloudera Manager Security documentation for more details.

About this task

Perform these steps in both the NiFi and NiFi Registry configuration fields.

Procedure

1. In the **Enable Kerberos Authentication** field, click the box for the CFM service.
2. In the **Identity Providers: Default Kerberos Identity Property - Default Realm** field, enter the KDC realm.
3. If this is your initial security setup, you can set the **Initial Admin Identity** to a Kerberos user.
4. Restart each of the CFM services.

   For Kerberos, the default Kerberos provider is used. You may keep nifi.security.user.login.identity.provider value blank or set it to kerberos-provider. Cloudera Manager sets this value to kerberos-provider by default.

Results

When the login screen displays, you may confirm your login with a KDC user.

Related Information

Cloudera Manager Security Documentation

Kerberos Authentication

Configure LDAP Authentication

Related Information

Lightweight Directory Access Protocol (LDAP)

LDAP Login Identity Provider Configuration

Cloudera Manager has default LDAP login identity provider properties available for configuration. You can use the following to set up the Default LDAP login provider for CFM services.

Table 1: NiFi Properties

Property Name	Description	Default Value
xml.loginIdentityProviders.provider.ldap-provider.class	Default LDAP Provider Class	org.apache.nifi.ldap.LdapProvider"
xml.loginIdentityProviders.provider.ldap-provider.property.Identity Strategy	Default LDAP Identity Strategy	USE_DN
xml.loginIdentityProviders.provider.ldap-provider.property.Authentication Strategy	Default LDAP Authentication Strategy	START_TLS
xml.loginIdentityProviders.provider.ldap-provider.property.Manager DN	Default LDAP Manager DN	
xml.loginIdentityProviders.provider.ldap-provider.property.Manager Password	Default LDAP Manager Password	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Keystore	Default LDAP TLS - Keystore	

xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Keystore Password	Default LDAP TLS - Keystore Password	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Keystore Type	Default LDAP TLS - Keystore Type	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Truststore	Default LDAP TLS - Truststore	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Truststore Password	Default LDAP TLS - Truststore Password	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Truststore Type	Default LDAP TLS - Truststore Type	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Client Auth	Default LDAP TLS - Client Auth	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Protocol	Default LDAP TLS - Protocol	
xml.loginIdentityProviders.provider.ldap-provider.property.TLS - Shutdown Gracefully	Default LDAP TLS - Shutdown Gracefully	
xml.loginIdentityProviders.provider.ldap-provider.property.Referral Strategy	Default LDAP - Referral Strategy	FOLLOW
xml.loginIdentityProviders.provider.ldap-provider.property.Connect Timeout	Default LDAP Connect Timeout	10 secs
xml.loginIdentityProviders.provider.ldap-provider.property.Read Timeout	Default LDAP Read Timeout	10 secs
xml.loginIdentityProviders.provider.ldap-provider.property.Url	Default LDAP Url	ldap://localhost:389
xml.loginIdentityProviders.provider.ldap-provider.property.User Search Base	Default LDAP User Search Base	sAMAccountName={0}
xml.loginIdentityProviders.provider.ldap-provider.property.User Search Filter	Default LDAP User Search Filter	
xml.loginIdentityProviders.provider.ldap-provider.property.Authentication Expiration	Default LDAP Authentication Expiration	12 hours

You can add any properties that are not available by default in Cloudera Manager using the safety valves for loginIdentityProviders.

Table 2: NiFi Registry Properties

Property Name	Description	Default Value
xml.identityProviders.provider.ldap-provider.class	Default LDAP Provider Class	org.apache.nifi.registry.security.ldap.LdapIdentityProvider
xml.identityProviders.provider.ldap-provider.property.Identity Strategy	Default LDAP Identity Strategy	START_TLS
xml.identityProviders.provider.ldap-provider.property.Authentication Strategy	Default LDAP Authentication Strategy	
xml.identityProviders.provider.ldap-provider.property.Manager DN	Default LDAP Manager DN	
xml.identityProviders.provider.ldap-provider.property.Manager Password	Default LDAP Manager Password	
xml.identityProviders.provider.ldap-provider.property.Connect Timeout	Default LDAP Connect Timeout	10 secs

xml.identityProviders.provider.ldap-provider.property.Read Timeout	Default LDAP Read Timeout	10 secs
xml.identityProviders.provider.ldap-provider.property.Url	Default LDAP Url	ldap://localhost:389
xml.identityProviders.provider.ldap-provider.property.User Search Base	Default LDAP User Search Base	OU=Users,DC=example,DC=com
xml.identityProviders.provider.ldap-provider.property.User Search Filter	Default LDAP User Search Filter	sAMAccountName={0}
xml.identityProviders.provider.ldap-provider.property.Authentication Expiration	Default LDAP Authentication Expiration	12 hours
xml.identityProviders.provider.ldap-provider.property.Referral Strategy	Default LDAP - Referral Strategy	FOLLOW

LDAP User Sync Configuration

You can allow LDAP User Sync for NiFi by using Cloudera Manager safety valves for authorizers.xml to extend the configuration.

The user group provider, once defined, can be used to replace the default user group property for file access providers.

Property Name	Description	Property Value (Default)
xml.authorizers.userGroupProvider.ldap-user-group-provider.class		org.apache.nifi.ldap.tenants.LdapUserGroupProvider
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Authentication Strategy		SIMPLE
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Manager DN	Identity of Manager DN for LDAP	
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Manager Password	LDAP Manager DN password	
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Referral Strategy	Referral Strategy	FOLLOW
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Connect Timeout	Connection Timeout	10 secs
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Read Timeout		10 secs
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Url	LDAP URL (e.g. ldap://localhost:389)	
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Page Size		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Sync Interval		1 min
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.User Search Base	User Search Base	
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.User Object Class	Example (Person, PosixAccount)	

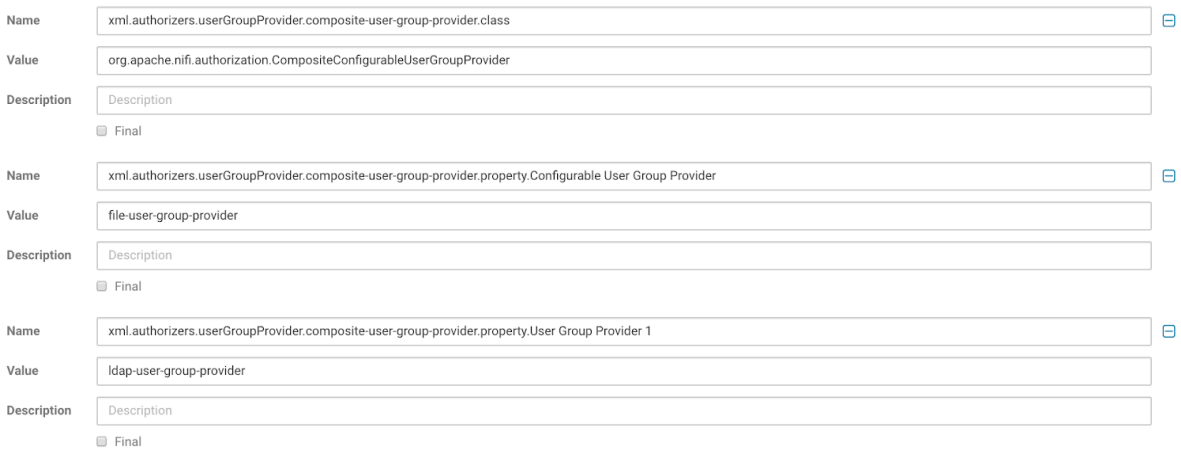
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.User Search Scope		ONE_LEVEL
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.User Search Filter		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.User Identity Attribute		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.User Group Name Attribute		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.User Group Name Attribute - Referenced Group Attribute		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Group Search Base		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Group Object Class		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Group Search Scope		ONE_LEVEL
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Group Search Filter		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Group Name Attribute		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Group Member Attribute		
xml.authorizers.userGroupProvider.ldap-user-group-provider.property.Group Member Attribute - Referenced User Attribute		

Pairing with the Composite Group Provider

If you need to combine multiple user/group provider mechanisms into a composite provider, you can do so using Cloudera Manager safety valves for authorizers.xml.

This example shows how File based users/group provider can be paired with an LDAP user group provider using a CompositeConfigurableUserGroupProvider.

Property Name	Description	Property Value (Default)
xml.authorizers.userGroupProvider.composite-user-group-provider.class		org.apache.nifi.authorization.CompositeConfigurableUserGr
xml.authorizers.userGroupProvider.composite-user-group-provider.property.Configurable User Group Provider		
xml.authorizers.userGroupProvider.composite-user-group-provider.property.User Group Provider 1		



Security Configuration Templates

The following security configuration example templates are available for your ease of use.

NiFi User Sync LDAP Properties

```
<!--
    DO NOT INCLUDE COMMENTS WHEN COPYING TO CM XML EDITOR
-->
<!--
    This section of properties defines an LDAP User Group Provider to
 support
    NiFi User sync from LDAP. This user group provider can be used directly
 in the
    Default File Access Policy Property - User Group Provider (setting to
 the ldap-user-group-provider identity)
    or as a part of a Composite Configurable User Group (which properties
 can be added optionally
    as defined below)
-->
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-provider.class</
name>
    <value>org.apache.nifi.ldap.tenants.LdapUserGroupProvider</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Authentication Strategy</name>
    <value>SIMPLE</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Manager DN</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Manager Password</name>
    <value></value>
</property>
<property>
```

```
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Referral Strategy</name>
    <value>FOLLOW</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Connect Timeout</name>
    <value>10 secs</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Read Timeout</name>
    <value>10 secs</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Url</name>
    <value>ldap://localhost:389</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Page Size</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Sync Interval</name>
    <value>1 min</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.User Search Base</name>
    <value>ou=users,dc=localhost.com</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.User Object Class</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.User Search Scope</name>
    <value>ONE_LEVEL</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.User Search Filter</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.User Identity Attribute</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.User Group Name Attribute</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.User Group Name Attribute - Referenced Group Attribute
    </name>
    <value></value>
```

```
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Group Search Base</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Group Object Class</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Group Search Scope</name>
    <value>ONE_LEVEL</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Group Search Filter</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Group Name Attribute</name>
    <value>cn</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Group Member Attribute</name>
    <value></value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.ldap-user-group-
provider.property.Group Member Attribute - Referenced User Attribute
    </name>
    <value></value>
</property>
<!--
    DO NOT INCLUDE COMMENTS WHEN COPYING TO CM XML EDITOR
-->
<!--
    This section of properties aligns with the above LDAP User Group
 Provider with a Composite Group Provider that combines
     LDAP  User Group Provider with a File User Group Provider (which is
 Configurable). Once defined the
     composite-user-group-provider can be used by setting the Default File
 Access Policy Property - User Group Provider
     in the CM UI to composite-user-group-provider
-->
<property>
    <name>xml.authorizers.userGroupProvider.composite-user-group-
provider.class</name>

 <value>org.apache.nifi.authorization.CompositeConfigurableUserGroupProvider</
value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.composite-user-group-
provider.property.Configurable User Group Provider</name>
    <value>file-user-group-provider</value>
</property>
<property>
    <name>xml.authorizers.userGroupProvider.composite-user-group-
provider.property.User Group Provider 1</name>
```

```
    <value>ldap-user-group-provider</value>
</property>
<!--
    DO NOT INCLUDE COMMENTS WHEN COPYING TO CM XML EDITOR
-->
<!--
    This property allows setting an initial admin value to a user in LDAP.
 This is required to ensure the default value is
    overridden which is automatically populated by CM. If a File Based User
 will be the Inital Admin this property is not required
-->
<property>
<name>xml.authorizers.accessPolicyProvider.file-access-policy-
provider.property.Initial Admin Identity</name>
<value></value>
</property>
```

NiFi Registry LDAP TLS Property Configuration

```
<!--
    DO NOT INCLUDE COMMENTS WHEN COPYING TO CM XML EDITOR
-->
<!--
    This represents the ldap tls-ssl properties that can be copied and
 populated CM identity-provider xml safety valves.
-->
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS - Keystore</
name>
<value></value>
</property>
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS - Keystore
 Password</name>
<value></value>
</property>
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS - Keystore
 Type</name>
<value></value>
</property>
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS -
 Truststore</name>
<value></value>
</property>
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS - Truststore
 Password</name>
<value></value>
</property>
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS - Truststore
 Type</name>
<value></value>
</property>
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS - Protocol</
name>
<value></value>
</property>
```

```
<property>
<name>xml.identityProviders.provider.ldap-provider.property.TLS - Shutdown
 Gracefully</name>
<value></value>
</property>
```