Apache NiFi
System Administration

Security Configuration

- NiFi allows for the system to run securely over HTTPS
- To run over HTTPS, several properties need to be set

Required Security Properties

Property Name	Description
nifi.security.keystore	Filename of the Keystore that contains the server's private key
nifi.security.keystoreType	The type of Keystore (PKCS12 or JKS)
nifi.security.keystorePasswd	The password for the Keystore
nifi.security.keyPasswd	The password for the certificate within the Keystore. May leave blank if same as nifi.security.keystorePasswd

Required Security Properties

Property Name	Description
nifi.security.truststore	Filename of the Truststore that will be used to authorize all clients connecting to NiFi. If unset, all users will be provided access as the Anonymous user.
nifi.security.truststoreType	The type of Truststore (PKCS12 or JKS)
nifi.security.truststorePasswd	The password for the Truststore

Required Security Properties

Property Name	Description
nifi.security.needClientAuth	Whether or not connecting clients must authenticate themselves. This property is used by the NiFi cluster protocol. A value of true indicates that the nodes in a cluster will be authenticated and must have certificates that are trusted by the Truststore. If the Truststore properties are not set, this must be false.
nifi.security.anonymous.authorities	Specifies the role(s) that should be granted to all users that connect over HTTPS anonymously. All roles granted to the client by an administrator will take precedence once the user connects using their certificate or by logging in.

Securing with Self-signed certificates

NiFi can be secured using the Self-signed certificates found on RequiTest's website

```
nifi.security.keystore=/path/to/keystore.jks
nifi.security.keystoreType=JKS
nifi.security.keystorePasswd=changeme
nifi.security.keyPasswd=changeme
nifi.security.truststore=/path/to/truststore.jks
nifi.security.truststoreType=JKS
nifi.security.truststorePasswd=changeme
nifi.security.needClientAuth=true
```

Note – These certificates are for test purposes only and should not be used on production systems

Enabling HTTPS

- Once the previous properties have been configured, the NiFi instance can be configured for HTTPS via the following properties:
  - `nifi.web.https.host` – The hostname of the server the system will be run on. Leaving the property blank or with a value of 0.0.0.0 will allow the HTTPS interface to be accessable from all network interfaces
  - `nifi.web.https.port` – The port that HTTPS should be running on

Note:

When enabling HTTPS, the `nifi.web.http.port` property should be unset

Securing Cluster and Site-to-Site communications

Once the UI has been secured, setting `nifi.remote.input.secure` and `nifi.cluster.protocol.is.secure` to `true` will secure Site-to-Site connections and inner-cluster communications, respectively.

User Access Control

- When configured to run securely, NiFi provides multiple levels of access for users
- Level of Access allows for definition of human users vs. machine users
- Controlled through the use of an ***Authority Provider***

Authority Providers

- A pluggable mechanism for providing authorization to different users

- Standard providers are
  - `file-provider`
  - `cluster-node-provider`
  - `cluster-ncm-provider`

file-provider

- The default provider is the `file-provider` Authority Provider
- Configured to use the permissions granted in the *conf/authorized-users.xml* file
- Typically sufficient for “standalone” NiFi systems

cluster-node/ncm-provider

- When NiFi is configured to run in a cluster, the nodes will typically use the `cluster-node-provider` Provider and the NCM will use the `cluster-ncm-provider` Provider
- This allows all authorization configuration to be provided by the Cluster Manager and must only be maintained in a single location
- Sample configuration can be found in the *conf/authorized-users.xml* file

User Levels of Access

Administrator

- Configure thread pool sizes and user accounts
- Purge dataflow change history

Data Flow Manager

- Can manipulate the flow (add, remove, change components on the graph)
- Can add, remove, and change Controller Services and Reporting Tasks
- Create and manage templates
- View statistics and bulletin board

User Levels of Access

Read Only

- Able to view the dataflow, but cannot make changes

Provenance

- Able to query the Data Provenance repository and view data lineage
- Able to view or download FlowFile content (if it is still in the content repository and the Authority Provider grants access)
- Must have Data Flow Manager role also in order to replay a Provenance Event

User Levels of Access

NiFi

- Intended for machines that will interact with NiFi via NiFi's Site-to-Site mechanism
- Allows the client to send data or retrieve data from Root Group ports that it has permission to interact with

Proxy

- Assigned to a system that will be acting on behalf of a user

Configuring Access

Configured through two properties in the *nifi.properties* file

- `nifi.authority.provider.configuration.file`
  - Specifies the configuration file for Authority Providers
- `nifi.security.user.authority.provider`
  - Indicates which of the configured Authority Providers should be used

Configuring Access

- Cluster Manager or standalone node require manual designation of an ADMIN user in the *conf/authorized-users.xml* file before running securely:

```
<users>
    <user dn="[user dn - read only and admin]">
        <role name="ROLE_ADMIN"/>
    </user>
</users>
```

- The user Distinguished Name (DN) should be used in place of "user dn – read only and admin"
- If using the self-signed certificates found on RequiTest's website, the user DN for the admin user should be "CN=NiFi Admin, OU=Demo, O=NiFi"

Configuring Access

- Once an ADMIN user has been specified and the system has been restarted, the ADMIN user will be able to access the UI
- The ADMIN user will now have access to the full Management menu in the UI

Granting User Access

- NiFi can be configured to grant a default Level of Access to Anonymous Users via the `nifi.security.anonymous.authorities` property

- If NiFi is not configured with default Level of Access for anonymous users, a new user that connects will be greeted by an Account Justification form

Submit Justification

home

User

NiFi User

Justification

500 characters remaining

Submit

Granting User Access

- Once the user has submitted their justification, all users with a role of ‘Administrator’ will be alerted of a pending request ()

- Clicking this icon will bring up the NiFi users dialog

NiFi Flow Users

Filter | by user

Displaying 2 of 2

Last updated: 11:13:42 EST

Show by group | Group

	User	Group	Roles	Last Accessed	Status	
	NiFi Admin	No value set	Administrator, Data Flow Manager	01/04/2016 11:13:42 EST	ACTIVE	
	NiFi User	No value set	Authorization Pending	No value set	PENDING	

User Roles

User
NiFi User

Justification
Testing access

Roles

- [ ] Administrator
- [ ] Data Flow Manager
- [ ] Read Only
- [ ] Provenance
- [ ] NiFi
- [ ] Proxy

Cancel | Apply

Click here to grant access via the User Roles dialog

NiFi Flow Users

Filter | by user

Displaying 2 of 2

Last updated: 11:14:42 EST

Show by group | Group

	User	Group	Roles	Last Accessed	Status	
	NiFi Admin	*No value set*	Administrator, Data Flow Manager	01/04/2016 11:13:42 EST	ACTIVE	
	NiFi User	*No value set*	Data Flow Manager	*No value set*	ACTIVE	

Click here to revoke access

Further Resources

- RequiTest Website:
  http://requitest.com/
- Apache NiFi Website:
  http://nifi.apache.org/
- Apache NiFi Users Mailing List:
  http://mail-archives.apache.org/mod_mbox/nifi-users/
- Apache NiFi Developers Mailing List:
  http://mail-archives.apache.org/mod_mbox/nifi-dev/