Installing & Running the HPCC Systems® Platform

Boca Raton Documentation Team

Installing & Running the HPCC Systems® Platform

Boca Raton Documentation Team

We welcome your comments and feedback about this document via email to <docfeedback@hpccsystems.com>

Please include **Documentation Feedback** in the subject line and reference the document name, page numbers, and current Version Number in the text of the message.

2025 Version 9.14.24-1

Welcome

These instructions will guide you through installing and running the HPCC[1] Systems® Community Edition on a single node to start and then optionally, expand it to a larger cluster of nodes.

The HPCC Systems Thor technology is designed to effectively process, analyze, and find links and associations within high volumes of complex data. This can detect non-obvious relationships, scale to support petabytes of data, and is significantly faster than competing technologies while requiring less hardware and resources.

The HPCC Systems Roxie technology - also known as the Rapid Data Delivery Engine or RDDE - uses a combination of technologies and techniques that produce extremely fast throughput for queries on indexed data.

This translates into better quality answers in less time so that organizations can cope with massive data and efficiently turn information into knowledge.

We suggest reading this document in its entirety before beginning. The entire process can take an hour or two, depending on your download speed.

NOTE: This document focuses primarily on the bare-metal implementation, for cloud and containerized deployments refer to the *Containerized HPCC Systems® Platform* document.

[1] **H**igh **P**erformance **C**omputing **C**luster (HPCC) is a massively parallel processing computing platform that solves Big Data problems. See https://hpccsystems.com/Why-HPCC/How-it-works for more details.

Quick Start Guide

We recommend taking the time to read this manual in its entirety; however, the following is a quick start summary of steps. There are many aspects of the HPCC Systems platform and this guide is intended to help you get the most out of your system. This section is not intended to replace the more comprehensive material in the remainder of this book.

1. Install HPCC Systems platform.

   Download the installation package from https://hpccsystems.com/download and install.

   On CentOS/Red Hat:

   ```
   sudo yum install hpccsystems-platform<rpm_file_name>
   ```

   On Ubuntu/Debian:

   ```
   sudo apt install <filename>
   ```

   Then to update dependencies:

   ```
   sudo apt-get install -f
   ```

2. Start your HPCC Systems platform.

   ```
   sudo systemctl start hpccsystems-platform.target
   ```

   NOTE: We provide sample scripts (see Appendix:Example Scripts) to make starting larger multi-node systems easier.

   System V users please refer to Appendix: hpcc-init.

3. Run **ECL Watch**. Check out your system.

   Using a browser, go to **ECL Watch** running on port 8010 of your HPCC Systems Node.

   For example, http://nnn.nnn.nnn.nnn:8010, where nnn.nnn.nnn.nnn is your node's IP address.

4. Create and run some ECL.

   You can do this right from ECL Watch. In ECL Watch, click on the **ECL** icon then click on the **Playground** link.

5. Go to https://hpccsystems.com/download get and install the ECL IDE and Client tools.

Now What?

Now that you have HPCC Systems started and running, what do you want to do? Maybe evaluate your needs and proceed to develop a custom configuration suitable for those needs. Maybe you want to expand your system and add nodes. Those topics and several others are covered in the following sections.

To familiarize yourself with what your system can do we recommend following the steps in:

- The **HPCC Systems Data Tutorial**
- Read **Using Config Manager** to learn how to configure an HPCC Systems platform using Advanced View.
- Use your new skills to process your own massive dataset!

HPCC Systems Installation and Startup

Follow these steps to install the packages and start components in a single-node configuration to begin. Once it is successfully installed, you will use the Configuration Manager to customize or expand your system.

Configuration Manager is the utility with which we configure the HPCC Systems platform. It is run on your Linux Server and you access its interface using a browser.

Figure 1. System Overview: Thor

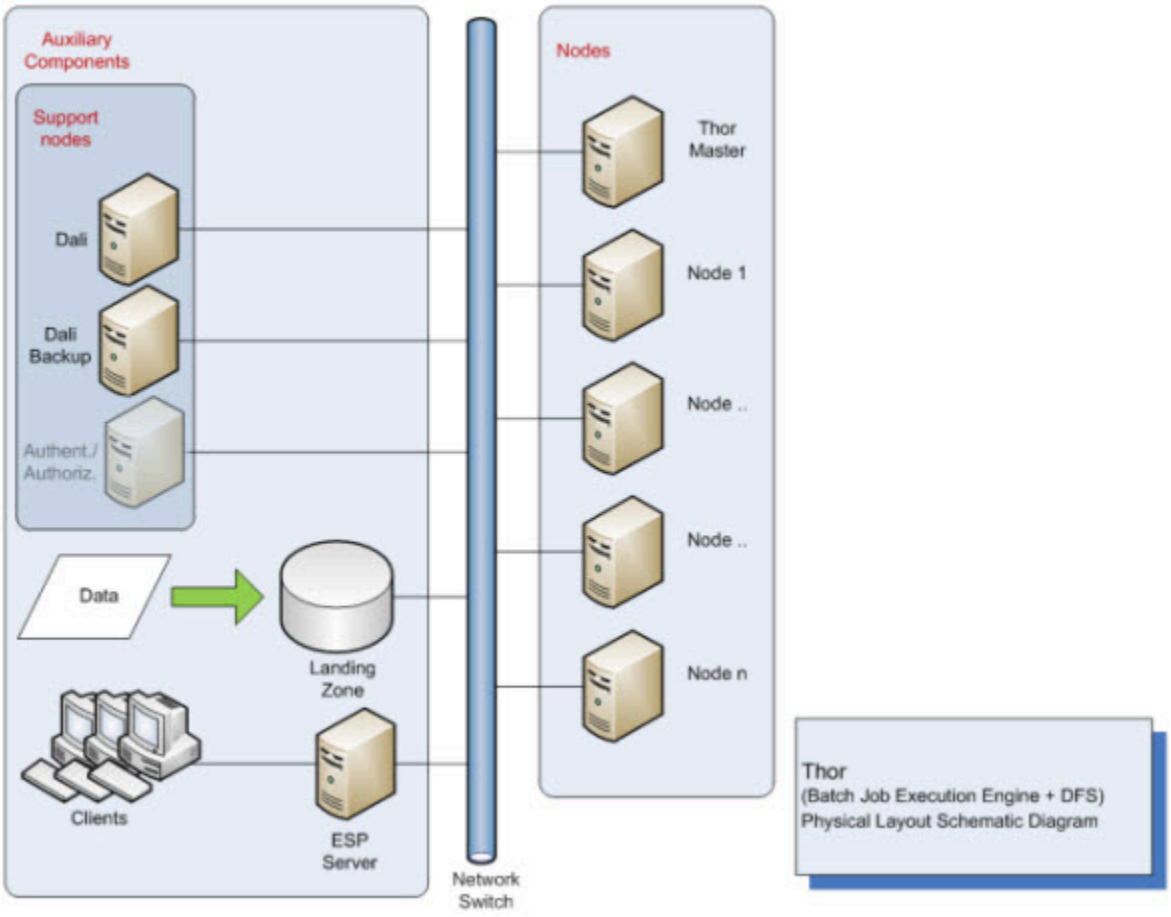
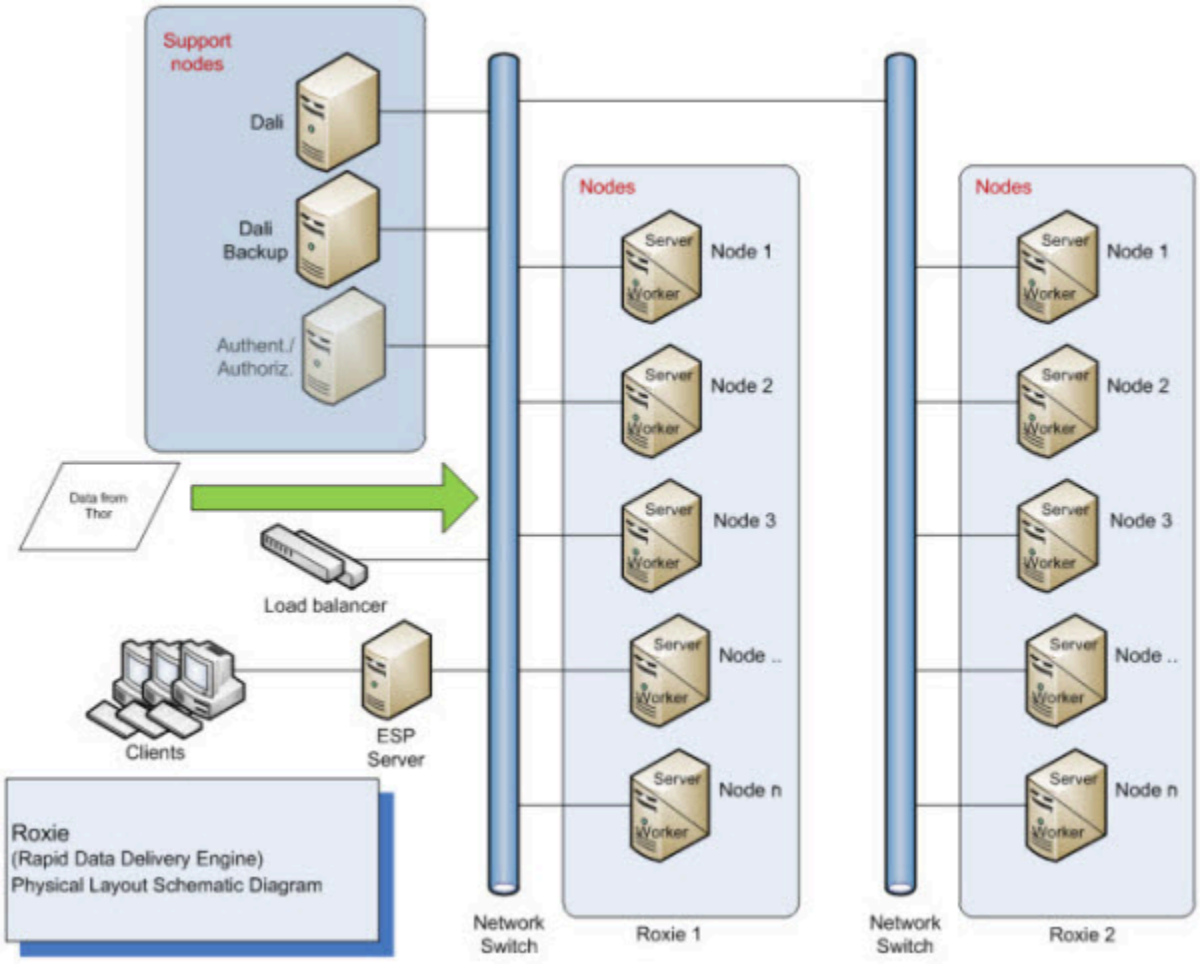


Figure 2. System Overview: Roxie



Initial Setup-Single Node

This section covers installing the HPCC Systems on a single node. This will enable the HPCC Systems platform to operate successfully; however, the real strength of the HPCC Systems platform is when it is run in a multi-node environment and can leverage the ability to perform operations using Massively Parallel Processing (MPP).

In addition, on a production system, you would dedicate one or more nodes to each server process. See the *Using Configruation Manager* manual for more details.

Installing the Package

The installation and package that you download is different depending on the operating system you plan to use. The installation packages will fail to install if their dependencies are missing from the target system.

Packages are available from the HPCC Systems® website: https://hpccsystems.com/download/

To install the package, follow the appropriate installation instructions:

CentOS/Red Hat

To install the HPCC Systems Platform you should have the appropriate rights and permissions to install packages on your system.

One way to install the platform is using yum.

```
sudo yum install -y epel-release
sudo yum install -y <hpccsystems platform rpm package>
```

Optionally you can install packages with rpm (recommended using the -Uvh options), however you would then have to negotiate installing any dependencies.

Ubuntu/Debian

For Ubuntu installations, to install the package, use:

```
sudo apt install <filename>
```

After installing the package, run the following to update any dependencies.

```
sudo apt-get install -f
```

Plugins

As of version 9.10, the plugins are automatically included. There is no need to install separately.

Initial Startup

1. Start the system using the default configuration.

```
sudo systemctl start hpccsystems-platform.target
```

There are log files for each component in directories below **/var/log/HPCCSystems** (default location) including an hpcc-init log for the start up process. If any component fails to start, these logs can help in troubleshooting.

*Additional information about the hpcc-init system and logs in the hpcc-init appendix.

Note: If you are using older System V based systems, please see the Appendix: System V.

Running an ECL Query on your Single-Node System

The single node system is running, and you can now create and run some ECL[1] code using either ECL IDE, the command line ECL compiler, or the ECL Command line tool.

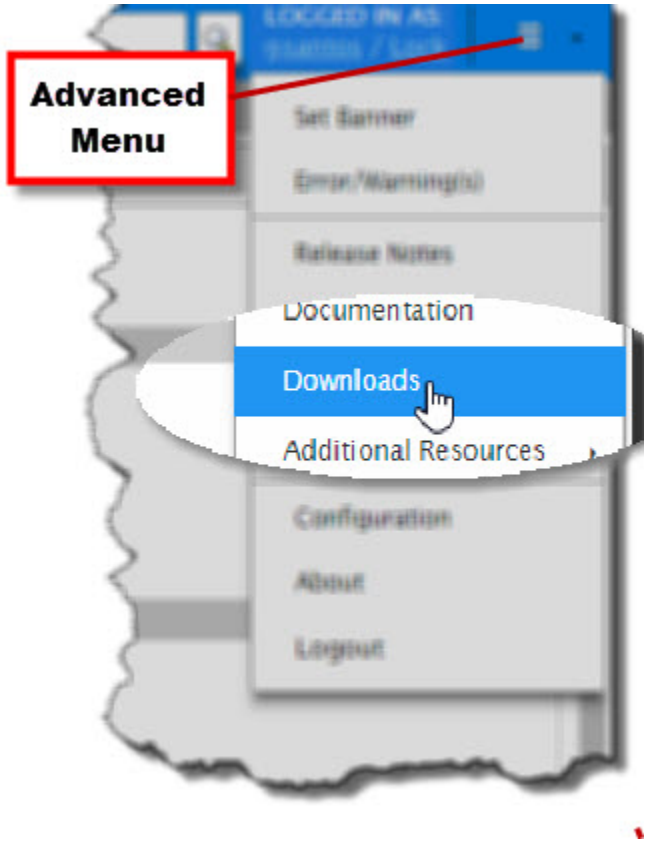
Install the ECL IDE and HPCC Systems Client Tools

1. In your browser, go to the **ECL Watch** URL. For example, http://nnn.nnn.nnn.nnn:8010, where nnn.nnn.nnn.nnn is your node's IP address.

	Your IP address could be different from the ones provided in the example images. Please use the IP address of **your** node.

2. From the ECL Watch Advanced menu, select the **Downloads** link.

Figure 3. ECL Watch Resource Page



Follow the link to the HPCC Systems portal download page.

Alternatively, you could use your browser to go directly to https://hpccsystems.com/download

3. Follow the instructions on that page to download the **ECL IDE and Client Tools for Windows**.

[1] **E**nterprise **C**ontrol **L**anguage (ECL) is a declarative, data centric programming language used to manage all aspects of the massive data joins, sorts, and builds that truly differentiate HPCC Systems (High Performance Computing Cluster) from other technologies in its ability to provide flexible data analysis on a massive scale.

4. Install the **ECL IDE and Client Tools for Windows**.

   Note: The ECL IDE only runs on Windows operating systems.

5. Once the ECL IDE is successfully installed, you can proceed.

Running a basic ECL program

Now that the package is installed on your Linux node and ECL IDE is installed on your Windows workstation, you can run your first ECL program. ECL programs may be run locally or remotely. For larger ECL jobs, you will want to target a remote cluster of machines, which may not be running the same operating system as the machine you are working on.

In this section we will use the **ECL Command line interface** to the compiler to compile and run ECL code locally.

The ECL compiler (eclcc) installs on to the eclcc server node when a package is installed. :This should be in your path, so you can run it from anywhere on the server. It is also installed on a Windows machine when you install the ECL IDE. To compile and run on Windows, you also need the Visual Studio 2008 C++ compiler (see *User Workstation Requirements* for details).

1. Create a file called hello.ecl and type in the following text (including the quotes):

   ```
   OUTPUT('Hello world');
   ```

   You can either use your favorite editor, or you can use the command line by typing the following

   ```
   echo "OUTPUT('Hello world');" > hello.ecl
   ```

2. Compile your program using eclcc by typing the following command:

   ```
   eclcc hello.ecl
   ```

3. An executable file is created which you can run as follows:

   ```
   # on a Linux machine:
      ./a.out
   # on a Windows machine:
      a.out
   ```

   This generates the output "Hello world" (excluding quotes), to the std output, your terminal window in this example. You can redirect or pipe the output to a file or program if you choose. This verifies that the compiler is working properly.

Running remotely using ECL Command Line

The **ECL Command Line Interface (CLI)** application accepts command line parameters to send directly to an ECL execution engine. You can use this utility to control the creation and execution of larger ECL jobs which target a remote system. To compile jobs on a remote system, eclcc is used to create an archive of the ECL code to be compiled, and the ecl CLI is used to submit it to a target cluster for compilation by the remote compiler server (eclccserver).

To submit a job using the ECL CLI, make sure the HPCC Systems platform has been started and use the following syntax:

```
ecl run  hello.ecl --target=hthor --server=<IP Address of the ESP node>:8010
```

The workunit[2] result is returned to the command line.

View the full details of the workunit using the ECL Watch interface for your HPCC Systems platform at this location http://nnn.nnn.nnn.nnn:8010, where nnn.nnn.nnn.nnn is the IP of your ESP server node. Either

[2]A Workunit is a record of a task submitted to an HPCC Systems cluster. It contains an identifier--workunit ID, the ECL code, results, and other information about the job.

search for the workunit using the workunit ID or select ECL Workunits/Browse and find your workunit in the list provided.

Setting up an **ecl.ini** file makes running a workunit a little easier when you want to use the same settings every time you submit a workunit in this way. See the *HPCC Systems Client Tools* manual for details.

If your ECL is more complex than a single source file, you can use the eclcc compiler locally to create an archive to be sent to the eclccServer:

```
eclcc hello.ecl hello2.ecl helloN.ecl -E | ecl run - --target=thor --server=<IP Address of the ESP>:8010
```

The target parameter must name a valid target cluster name as listed in your environment's topology section.

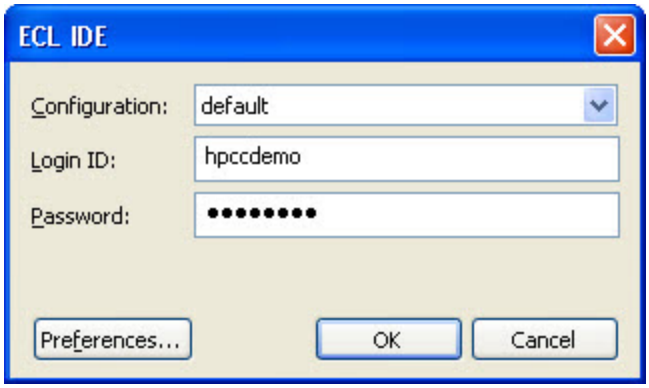
Running a basic ECL program from the ECL IDE

1. Open the ECL IDE on your Windows workstation, from your start menu. (Start **>>** All Programs **>>** HPC-CSystems **>>** ECL IDE).

	You can create a shortcut on your desktop to provide quick access to the ECL IDE.

2. Enter your **Login ID** and **Password** provided in the Login dialog.

Figure 4. Login Window



3. Open a new **Builder Window** (CTRL+N) and write the following code:

```
OUTPUT('Hello World');
```

This could also be written as:

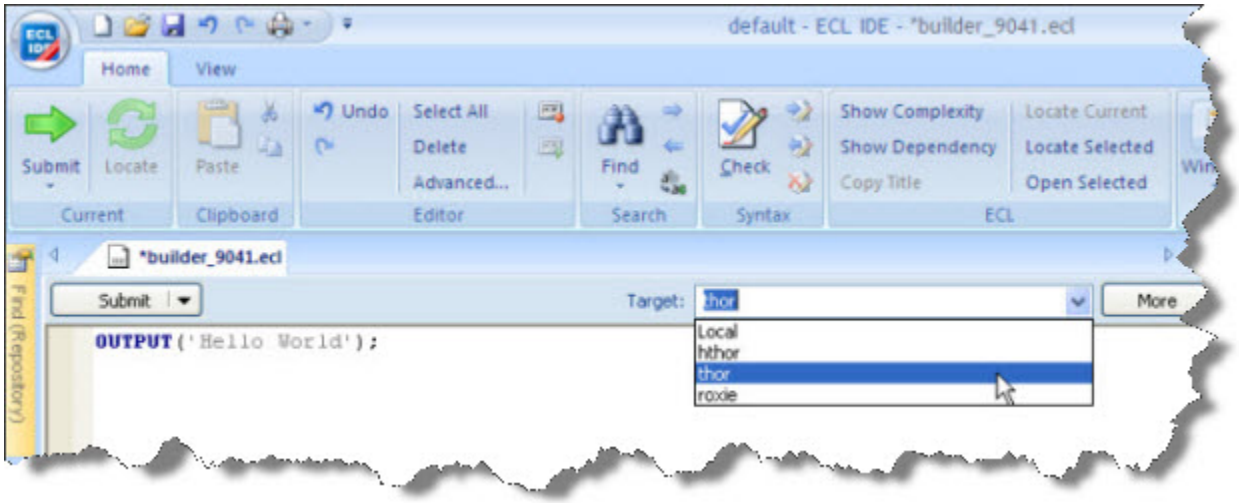
```
'Hello World';
```

In the second program listing, the OUTPUT keyword is omitted. This is possible because the language is declarative and the OUTPUT action is implicit.

4. Select **thor** as your target cluster.

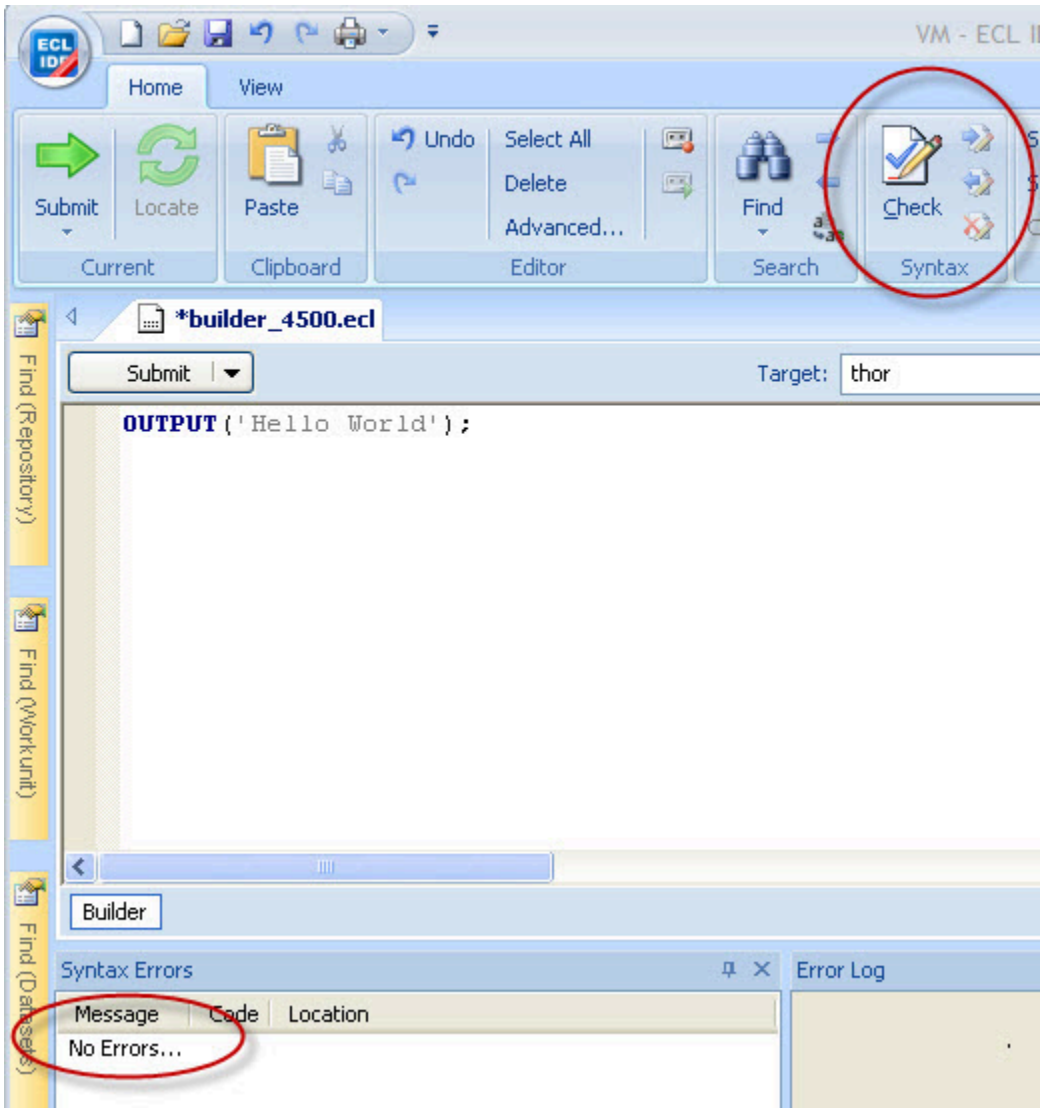
   Thor is the Data Refinery component of your HPCC Systems platform. It is a disk based massively parallel computer cluster, optimized for sorting, manipulating, and transforming massive data.

Figure 5. Select target



5. Press the syntax check button on the main toolbar (or press F7).

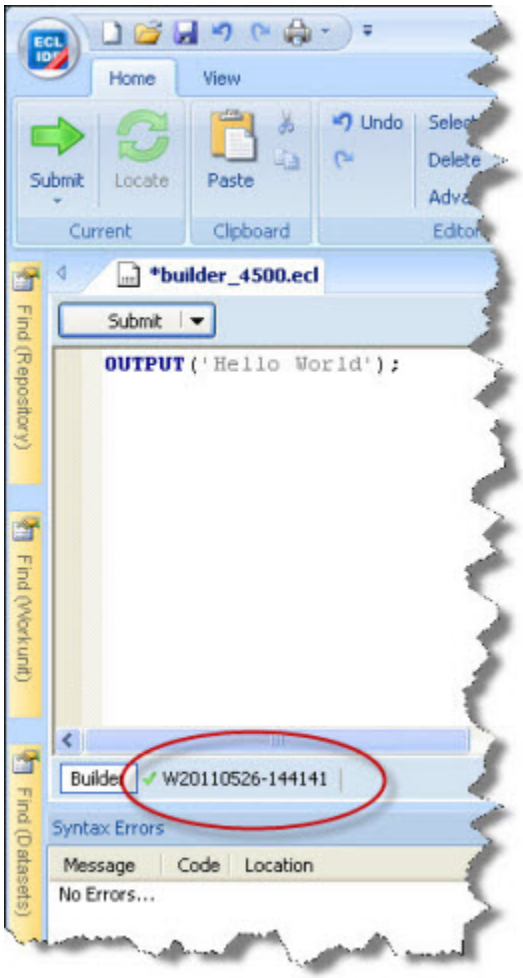
Figure 6. Syntax Check



A successful syntax check displays the "No Errors" message.

6. Press the **Submit** button (or press ctrl+enter).

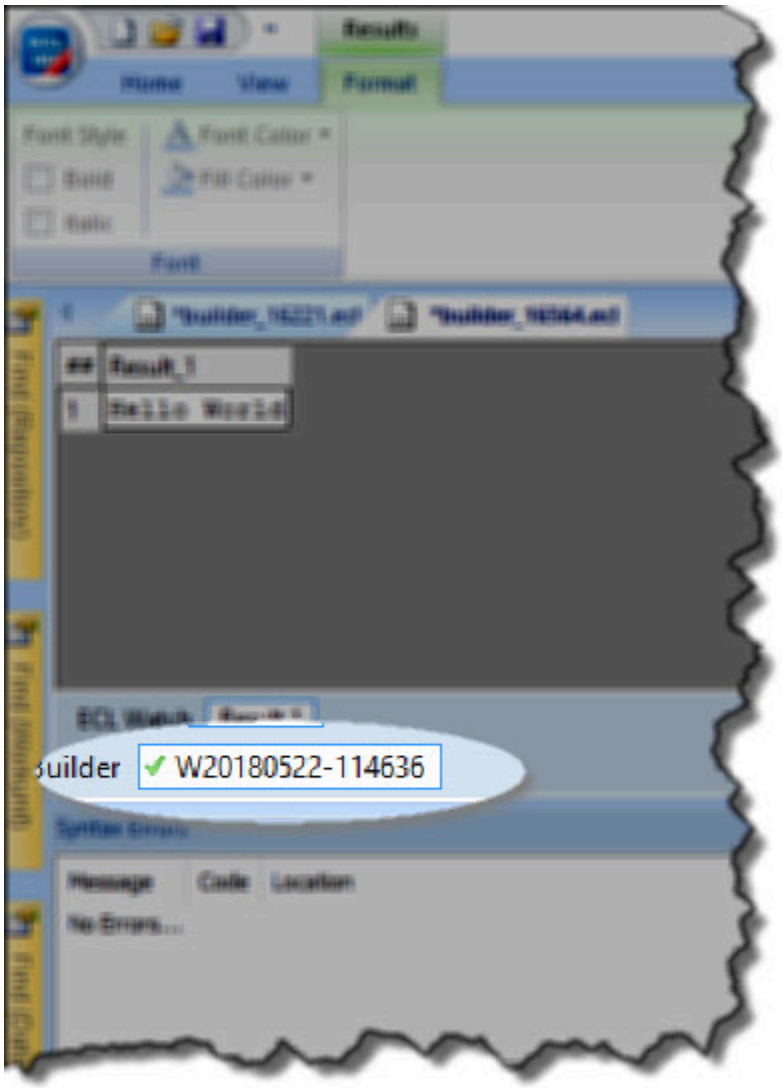
Figure 7. Completed job



The green check mark indicates successful completion.

7. Click on the workunit number tab to see the output.

Figure 8. Completed job output



Configuring a Multi-Node System

While the single-node system is fully-functional, it does not take advantage of the true power of HPCC Systems--the ability to perform operations using Massively Parallel Processing (MPP). This section provides the steps to expand your single-node system into a multi-node system using the Configuration Manager Wizard.

To run a multi-node system, ensure that you have exactly the same packages installed on every node. Follow the steps below to configure your multi-node system to leverage the full power of Massively Parallel Processing.

Using the Configuration Manager Wizard

This section details reconfiguring a system to use multiple nodes. Before you start this section, you must have already downloaded the correct packages for your distro from the HPCC Systems® website: https://hpccsystems.com/download.

1. If it is running, stop the HPCC Systems platform, using this command:

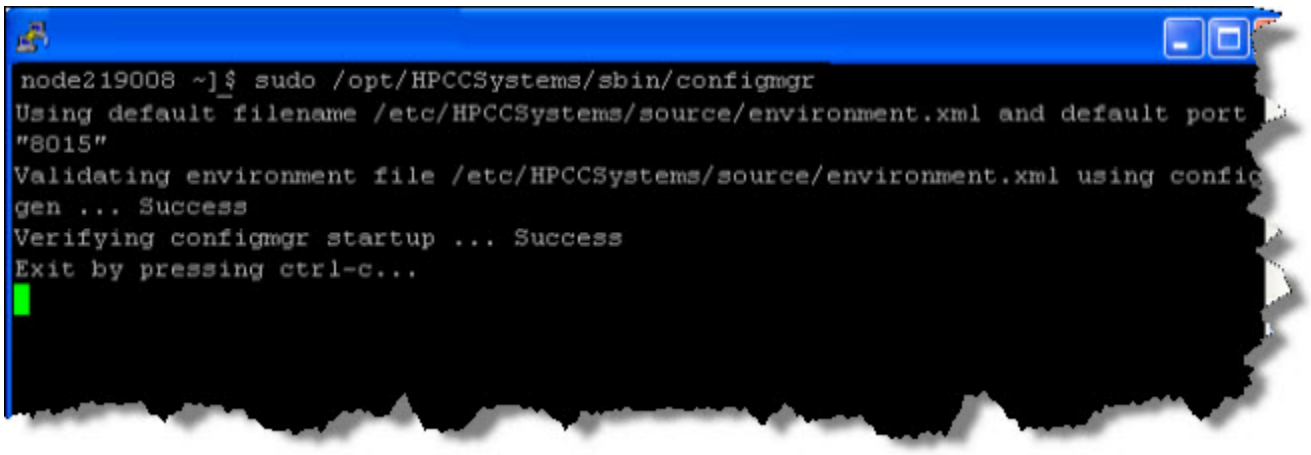
```
sudo systemctl stop hpccsystems-platform.target
```

You can use this command to confirm HPCC Systems processes are stopped:

```
sudo systemctl status hpccsystems-platform.target
```

2. Start the Configuration Manager service.

```
sudo /opt/HPCCSystems/sbin/configmgr
```

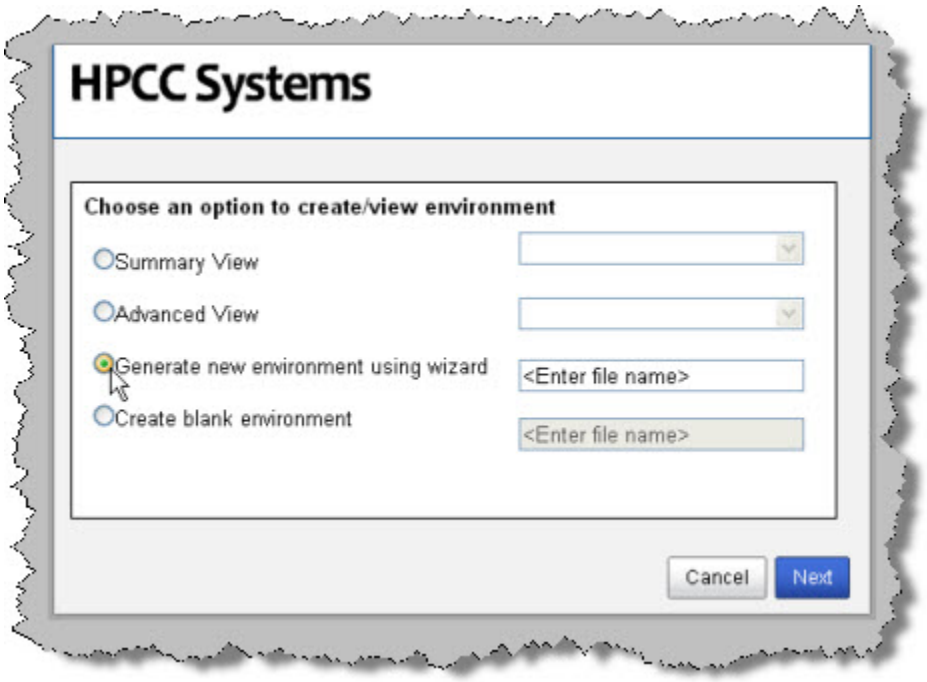


3. Leave this window open. You can minimize it, if desired.

4. Using a Web browser, go to the Configuration Manager's interface:

```
http://<node ip >:8015
```

5. The Configuration Manager startup wizard displays. To use the wizard, select the Generate new environment using wizard button.



6. Provide a name for the environment file.

   This will then be the name of the configuration xml. For example, we will name this *NewEnvironment.xml*.

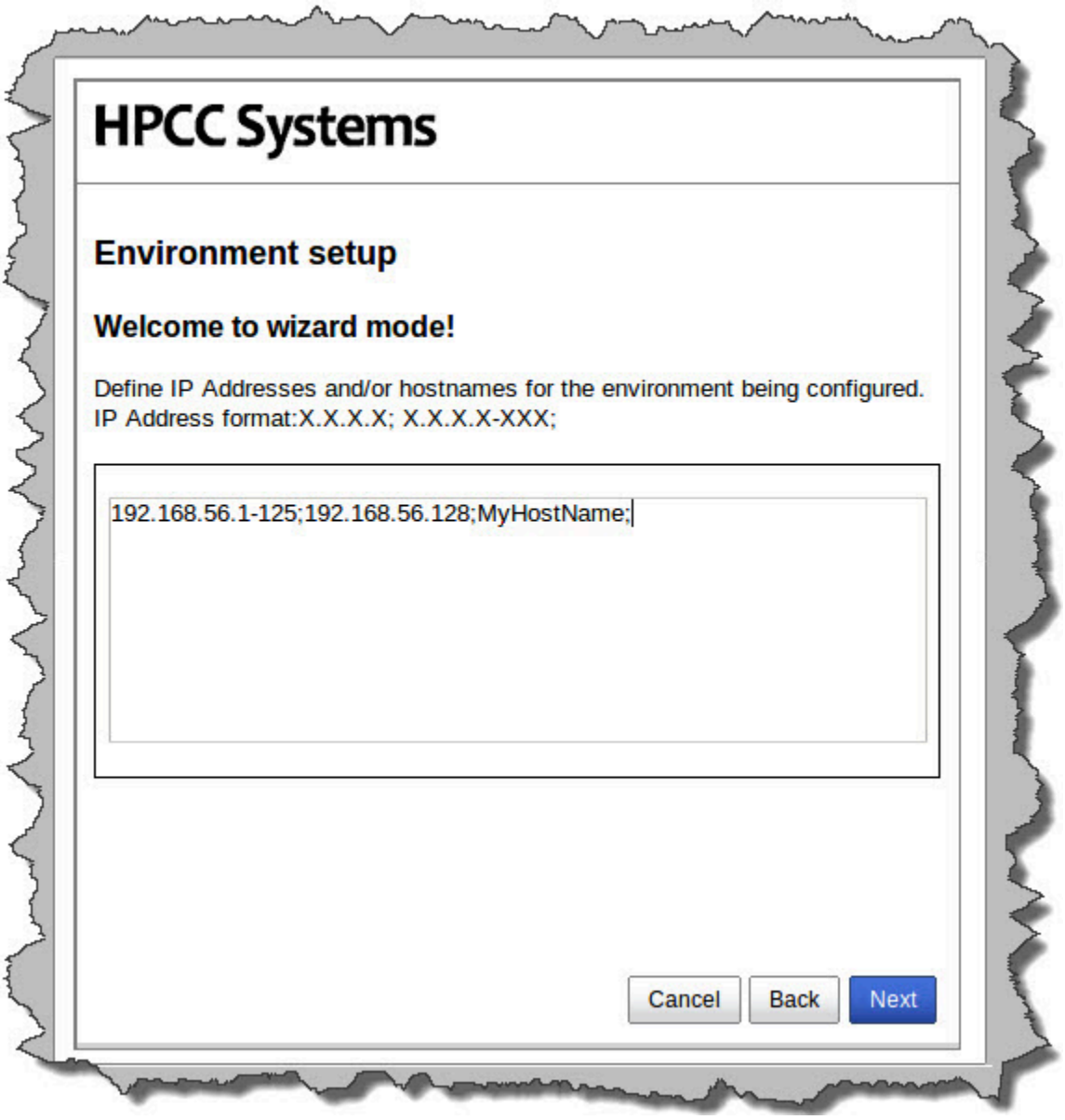
7. Press the **Next** button.

   Next you will need to define the IP addresses that your system will use.

8. Enter all the IP addresses you want to use for this HPCC Systems cluster. Alternatively, you could enter the hostname(s).

   The IP addresses do not need to be contiguous. In the image below, we specified the IP addresses nn.nnn.nnn.1-125 and nn.nnn.nnn.128. These are separated with a semi-colon.

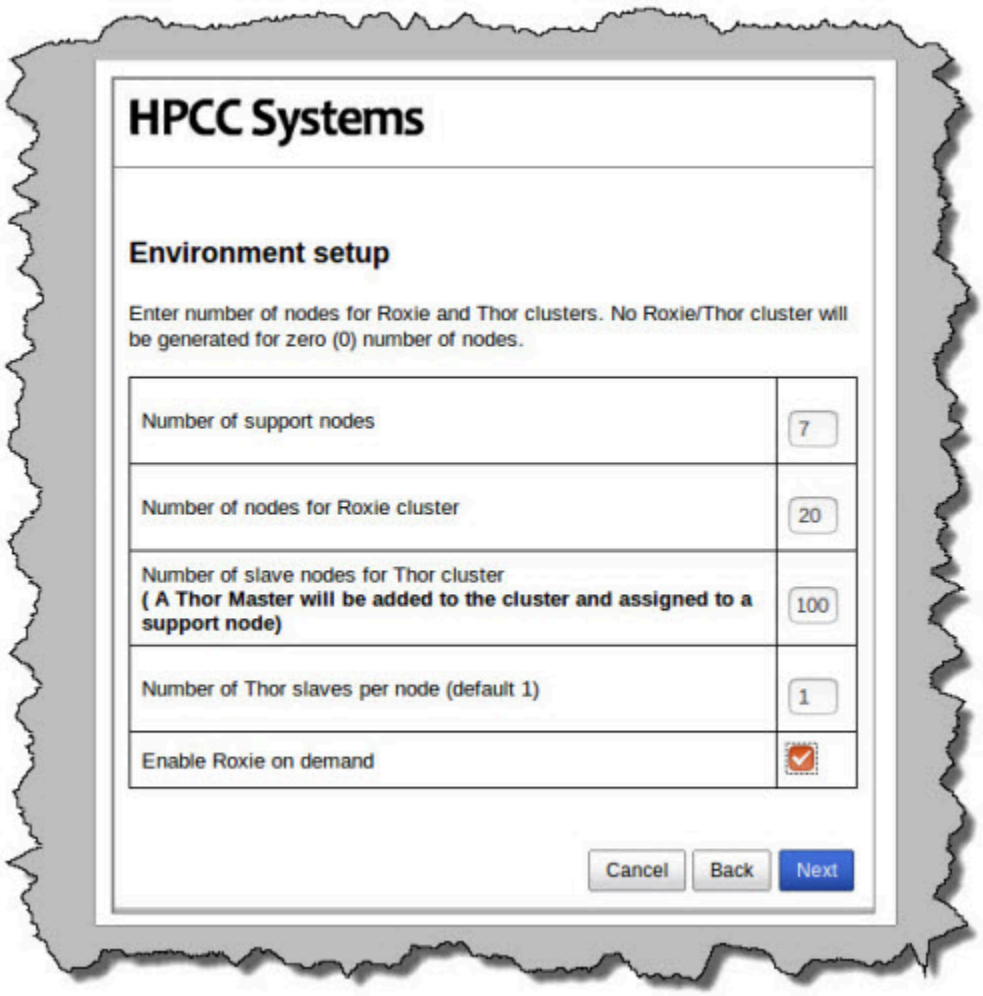
   You can specify a range of IPs using a hyphen (for example, 192.168.55.1-125). IP Addresses can be specified individually using semi-colon delimiters.



9. Press the **Next** button.

   Now you will define how many nodes to use for the Roxie and Thor clusters.

10 Enter the appropriate values as indicated.



Number of support nodes: Specify the number of nodes to use for support components. The default is 1.

Number of nodes for Roxie cluster: Specify the number of nodes to use for your Roxie cluster. Enter zero (0) if you do not want a Roxie cluster.

Number of slave nodes for Thor cluster Specify the number of slave nodes to use in your Thor cluster. A Thor master node will be added automatically.

Number of Thor slaves per node (default 1) Specify the number of Thor slave processes to instantiate on each slave node. Enter zero (0) if you do not want a Thor cluster.

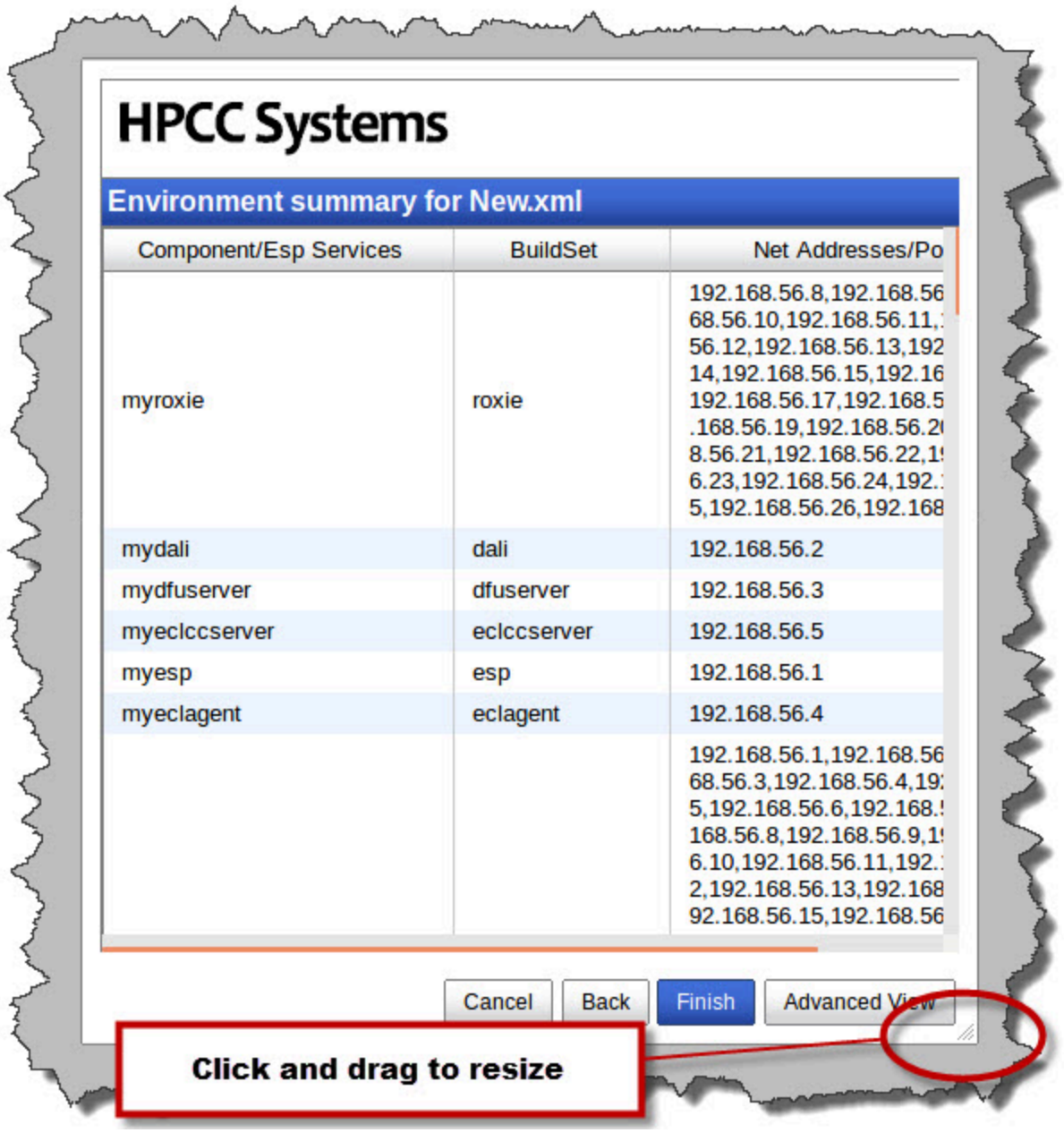
Enable Roxie on demand Specify whether or not to allow queries to be run immediately on Roxie. (Default is true)

11 Press the Next button

The Environment Summary displays.

12. Click on **Finish** to accept these values. This saves the file.

	Keep in mind, that your HPPC configuration may be different depending on your needs. For example, you may not need a Roxie or you may need several smaller Roxie clusters. In addition, in a production [Thor] system, you would ensure that Thor and Roxie nodes are dedicated and have no other processes running on them. This document is intended to show you how to use the configuration tools. Capacity planning and system design is covered in a training module.



	You can resize the Environment Summary by clicking and dragging the lower right corner.

13. You will now be notified that you have completed the wizard.

At this point the system has created a file named NewEnvironment.xml in the **/etc/HPCCSystems/source** directory

14. Stop the Configuration Manager in the terminal where you started it by pressing CTRL-C.

	Be sure system is stopped before attempting to move the environment.xml file.

15. Copy the NewEnvironment.xml file from the source directory to the /etc/HPCCSystems and rename the file to environment.xml

```
# for example
sudo cp /etc/HPCCSystems/source/NewEnvironment.xml /etc/HPCCSystems/environment.xml
```

	Make sure that you have sufficient privileges to write file(s) to the destination directory before attempting to copy. If prompted to overwrite the destination file, you should answer **yes**.

16. If you have added new machines to the cluster, you need to copy and install the HPCC Systems package onto all nodes, and generate and clone the SSH keys. This can be done using the install-cluster.sh script which is provided with HPCC Systems. Use the following command:

```
/opt/HPCCSystems/sbin/install-cluster.sh -k <package-file-name>
```

Where <package-file-name> is the name of the package file that you want to install on every node - this will be in the form hpccsystems-platform-*xxxx-n.n.nnnn*.rpm (or .deb) depending on the version and distro. More details including other options that may be used with this command are included in the appendix.

17. Copy the **/etc/HPCCSystems/environment.xml** to **/etc/HPCCSystems/** on **every** node.

You may want to create a script to push out the XML file to all nodes. A sample script is provided with HPCC Systems. The following command copies the XML files out to all nodes as required:

```
sudo /opt/HPCCSystems/sbin/hpcc-push.sh -s <sourcefile> -t <destinationfile>
```

Where the <sourcefile> is the absolute path to the file you want to copy, and the <destinationfile> is the absolute path to the file you want written out. See the appendix (Appendix:Example Scripts) for more information on using this script.

18. Restart the HPCC Systems on **every** node. The following command starts HPCC Systems on an individual node:

```
sudo systemctl start hpccsystems-platform.target
```

You may want to use a script to push this command out to every node. A sample script is provided with HPCC Systems. Use the following command to start HPCC Systems on all nodes:

```
sudo /opt/HPCCSystems/sbin/hpcc-run.sh start
```

This script can also be used to stop HPCC Systems on all nodes and to start and stop individual components on all nodes. See the appendix (Appendix:Example Scripts) for more details.

Additional SSH Key Information

On multi-node HPCC Systems, certificates and SSH keys must all match across all nodes for the system to work properly. If you used the *install-cluster.sh* script as outlined in the steps above, this would make sure that everything is properly in sync. However, it is still a good idea to verify that they do all match up. Another way to ensure this is to use the delivered *hpcc-push.sh* script. For example, the following commands would push out the certificate, key, and public key out to all hosts defined in the environment.

```
sudo /opt/HPCCSystems/sbin/hpcc-push.sh \
     -s /home/hpcc/certificate/public.key.pem -t /home/hpcc/certificate/public.key.pem
sudo /opt/HPCCSystems/sbin/hpcc-push.sh \
     -s /home/hpcc/certificate/key.pem -t /home/hpcc/certificate/key.pem
sudo /opt/HPCCSystems/sbin/hpcc-push.sh \
     -s /home/hpcc/certificate/certificate.pem -t /home/hpcc/certificate/certificate.pem
```

See the appendix (Appendix:Example Scripts) for more information on using this script.

Update SSH Keys

You may want to periodically refresh or rotate your SSH keys. We recommend using a provided script for installing or updating SSH Keys. See the appendix (Appendix:Example Scripts) for more information on using this script.

Starting and Stopping

Start, Stop, Restart the System

Once you have your system environment established, the **init** system can be used to start, stop, or restart components.

The following commands can be used:

To start the system:

To start your HPCC Systems platform issue the following command;

```
sudo systemctl start hpccsystems-platform.target
```

For older System V based systems see Appendix: hpcc-init.

To stop the system:

To stop your HPCC Systems platform issue the following command;

```
sudo systemctl stop hpccsystems-platform.target
```

For older System V based systems see Appendix: hpcc-init.

You can use a script to start or stop multiple nodes in the system. See *Example Scripts* in the Appendix section.

Start or Stop Single Components

To start a single component,

```
systemctl start <component-type>@<component-name>.service
```

To stop a single component,

```
systemctl stop <component-type>@<component-name>.service
```

For older System V based systems see Appendix: hpcc-init.

Start or Stop Configuration Manager

Configure the system as desired using Configuration Manager.

1. If the system is running, stop the HPCC Systems platform, using this command on **every** node:

   ```
   sudo systemctl stop hpccsystems-platform.target
   ```

2. Start the Configuration Manager service on one node (usually the first node is considered the head node and is used for this task, but this is up to you)

   ```
   sudo /opt/HPCCSystems/sbin/configmgr
   ```

3. Using a web browser, go to the Configuration Manager's interface:

```
http://<ip of installed system>:8015
```

Configuring HPCC Systems® for Authentication

This section details the steps to configure your HPCC Systems platform to use authentication. There are currently a few ways to use authentication with your HPCC Systems platform: simple htpasswd authentication, LDAP, or another plugin security method.

The htpasswd authentication method is basic password authentication. It only grants or denies access to a user, based upon MD5 encrypted password authentication.

LDAP authentication offers more features and options. LDAP can not only authenticate users, but adds granularity to the authentication. LDAP allows you to control grouped access to features, functions, and files.

You should consider your system needs and decide which of these methods is appropriate for your environment.

When implementing any form of authentication, we strongly recommend that you enable your ESP server to use HTTPS (SSL) and set ALL service bindings to only use HTTPS. This ensures that credentials are passed over the network using SSL encryption. See *Configuring ESP Server to use HTTPS (SSL)* **for details.**

You should not attempt this until you have already deployed, configured, and certified the environment you will use.

Using htpasswd authentication

htpasswd provides basic password authentication to the entire system. This section contains the information to install and implement htpasswd authentication.

Connect to Configuration Manager

In order to change the configuration for HPCC Systems components, connect to the Configuration Manager.

1. Stop all HPCC Systems components, if they are running.
2. Verify that they are stopped. You can use a single command, such as :

   ```
   sudo /opt/HPCCSystems/sbin/hpcc-run.sh status
   ```

3. Start Configuration Manager.

   ```
   sudo /opt/HPCCSystems/sbin/configmgr
   ```

4. Connect your web browser to the Configuration Manager web interface.

   (using the url of http://<*configmgr_IP_Address*>:8015, where <*configmgr_IP_Address*> is the IP address of the node running Configuration Manager)

5. Select the **Advanced View** radio button.
6. Use the drop list to select the XML configuration file.

   Note: Configuration Manager **never** works on the active configuration file. After you finish editing you will have to copy the environment.xml to the active location and push it out to all nodes.

7. Check the **Write Access** box.

Default access is read-only. Many options are only available when write-access is enabled.

Enabling htpasswd authentication in HPCC Systems

8. Create an instance of the **Security Manager** Plugin:

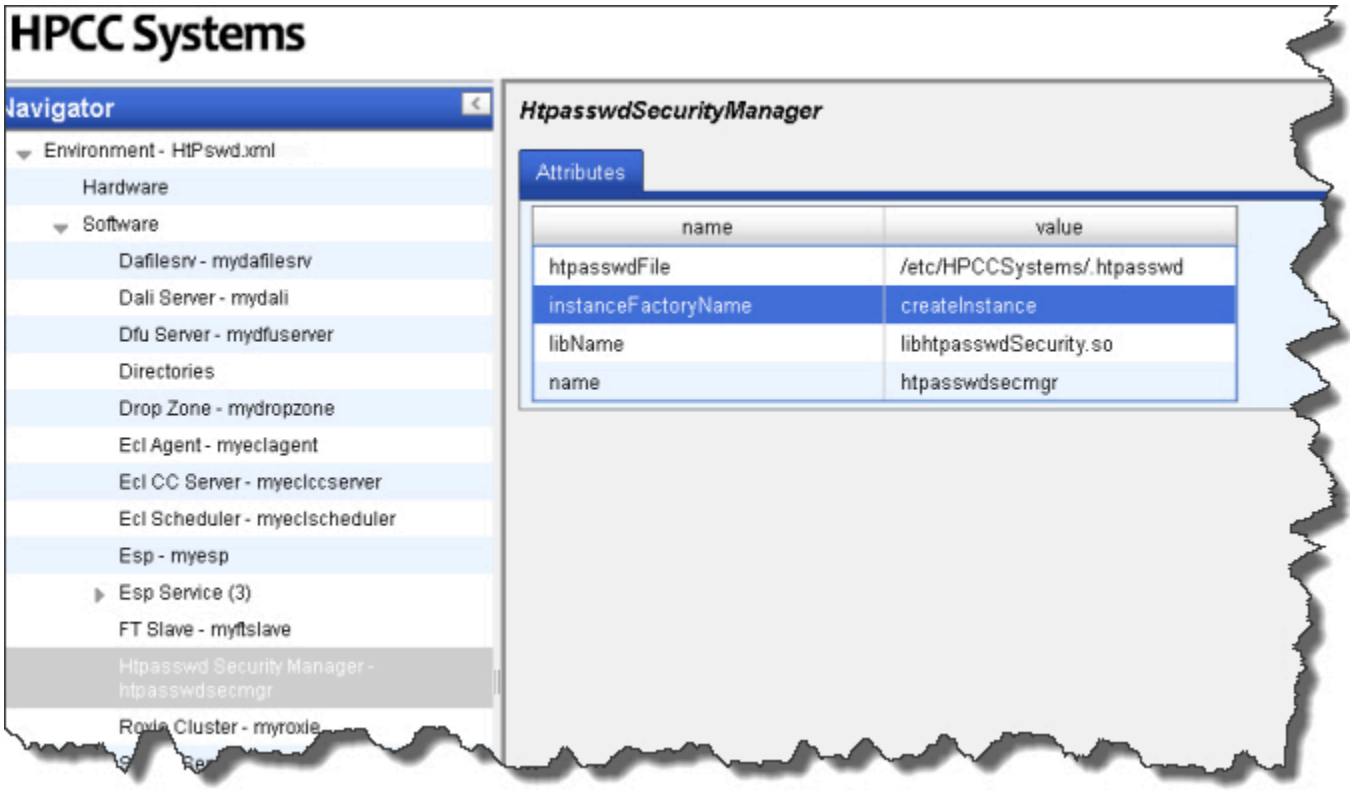
   a. Right-click on Navigator Pane on the left side.

   b. Select **New Components**

   c. Select the **htpasswdsecmgr** component

9. Configure the htpasswd plugin

Figure 9. Security Mgr Configuration page



   a. Enter the location of the Htpasswd file containing the username and password on the Linux file system for the value of **htpasswdFile**

   b. **InstanceFactoryName** is the name of the security manager factory function, implemented in the security library. The default is "createInstance". For implementing Htpasswd, leave the default.

   c. Provide a library name value for **libName**. For Htpasswd, use libhtpasswdSecurity.so

   d. Provide an instance **name** for the name value. For example, htpasswdsecmgr.

10. Select **Esp - myesp** in the Navigator panel on the left hand side.

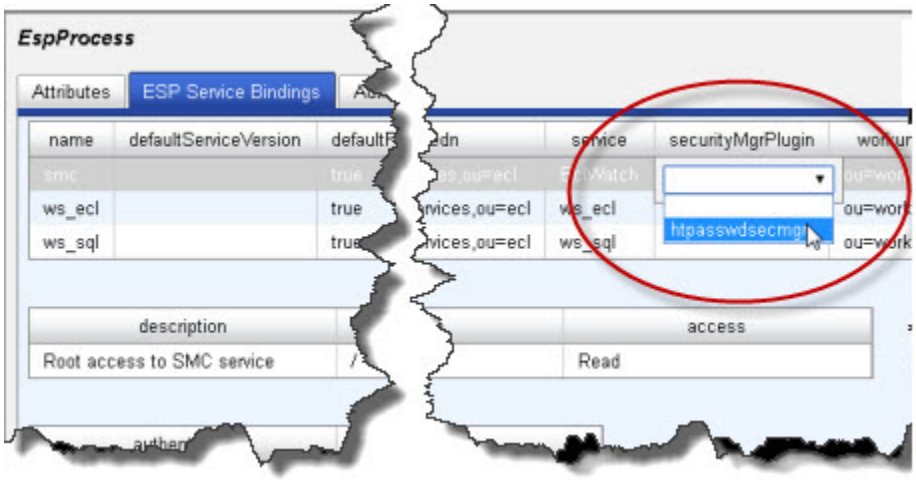
Note: If you have more than one ESP Server, each one should have its own authentication set up.

11 Associate the Security Manager Plugin with the ESP binding(s)

a. Click on the target **Esp** in the Navigator Pane on the left side.

b. Select the **ESP Service bindings** tab

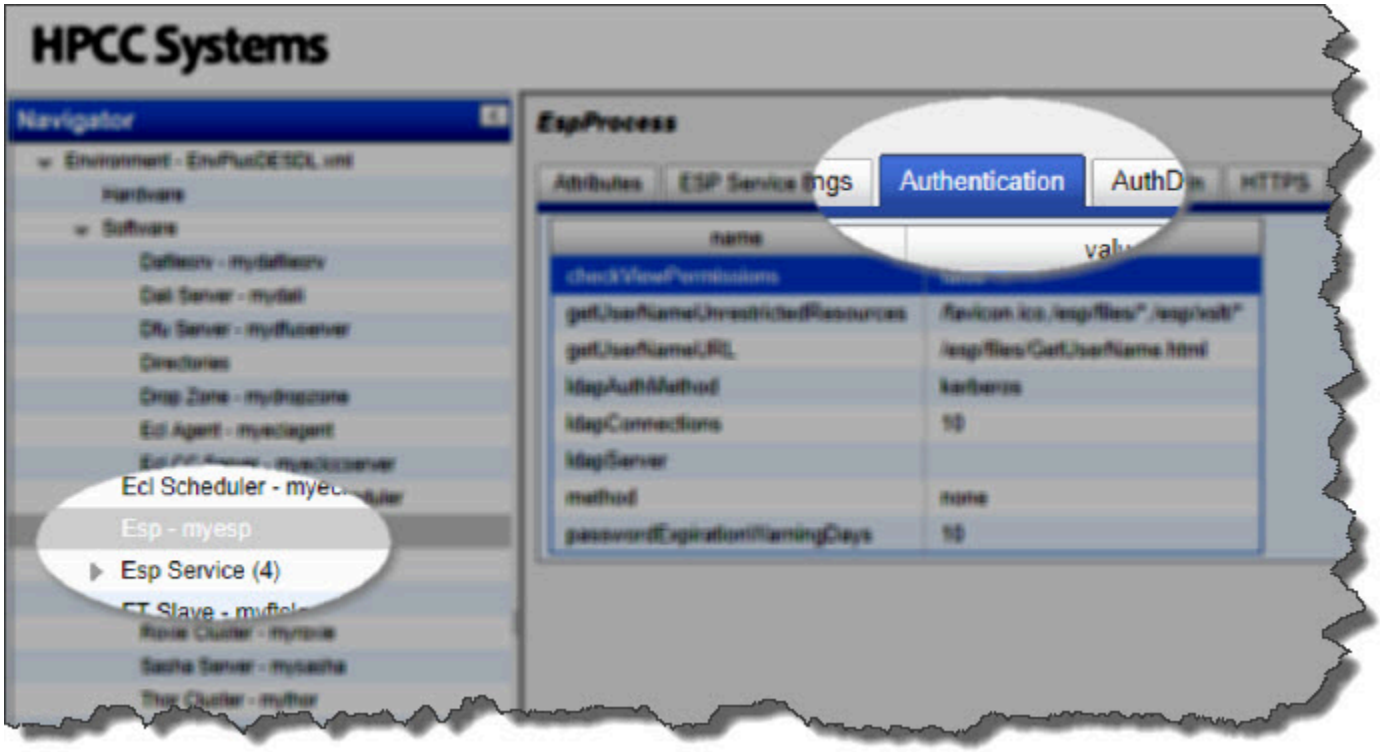
c. On the target binding(s) select the appropriate securityMgrPlugin instance from the drop list.



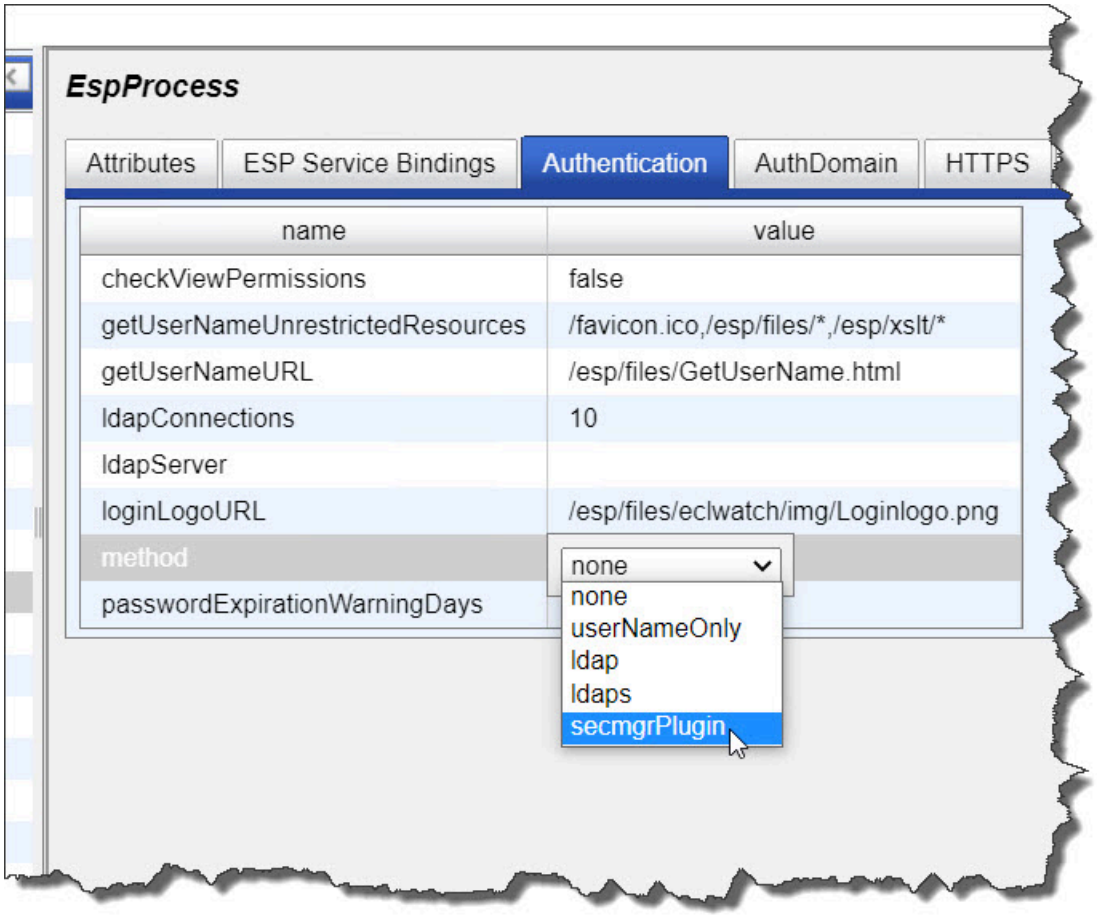
12 Select the security Plugin for each service that requires a security manager.

For example, in the above image, select htpasswdsecmgr for the smc service. Then, select it for ws_ecl and every other service that you want to use htpassword security.

13 Select the **Authentication** tab



14.Click on the value column drop list to display the choices for **method**.



15.Choose **secmgrPlugin** from the drop list.

16.Click on the disk icon to save.

User administration with htpasswd

Users and passwords are kept in the htpasswd file. The htpasswd file must exist on the ESP Node where you have enabled authentication. HPCC Systems only recognizes MD5 encrypted passwords.

The default location is: **/etc/HPCCSystems/.htpasswd** on the ESP node that has been configured to authenticate, but it is configurable from the Htpasswd Security Manager as outlined above (step 9).

You can use the htpasswd utility to create the .htpasswd file to administer users.

You may already have the htpasswd utility on your system, as it is a part of some Linux distributions. Check your Linux distribution to see if you already have it. If you do not have it you should download the utility for your distribution from The Apache Software Foundation.

For more information about using htpasswd see: http://httpd.apache.org/docs/2.2/programs/htpasswd.html.

Single User Security Manager

The Single User security manager is a specialized security manager that allows a username/password combination to be specified on the ESP startup command line. At runtime, when you attempt to access any authenticating ESP feature, such as ECL Watch, you must specify a username/password combination.

A single user security manager could be useful for a custom deployment where you do not want to configure an entire LDAP server or create a Linux HTPASSWD file, such as a classroom environment or a custom HPCC Systems Virtual Machine.

See the *Security Manager Plugin Framework* document for more information on configuring and deploying Security Manager plugins.

Using LDAP Authentication

This section contains the information to install and implement LDAP based authentication. LDAP Authentication provides the most options for securing your system, or parts of your system. In addition to these configuration settings you should run the **initldap** utility to create the required default HPCC Systems Admin user on your LDAP server.

If you choose to use LDAP authentication you must enable LDAP security in your HPCC Systems configuration. With LDAP security enabled on your system you can then choose to enable file scope security. You can choose to use LDAP authentication without enabling file scope security. The following sections describe how to enable LDAP authentication and file scope security for your HPCC Systems platform.

Connect to Configuration Manager

In order to change the configuration for HPCC Systems components, connect to the Configuration Manager.

1. Stop all HPCC Systems components, if they are running.

2. Verify that they are stopped. You can use a single command, such as :

   ```
   sudo /opt/HPCCSystems/sbin/hpcc-run.sh -a hpcc-init status
   ```

3. Start Configuration Manager.

   ```
   sudo /opt/HPCCSystems/sbin/configmgr
   ```

4. Connect to the Configuration Manager web interface.

   (using the url of http://<*configmgr_IP_Address*>:8015, where <*configmgr_IP_Address*> is the IP address of the node running Configuration Manager)

5. Select the **Advanced View** radio button.

6. Use the drop list to select the XML configuration file.

Note: Configuration Manager **never** works on the active configuration file. After you finish editing you will have to copy the environment.xml to the active location and push it out to all nodes.

Modifying the configuration

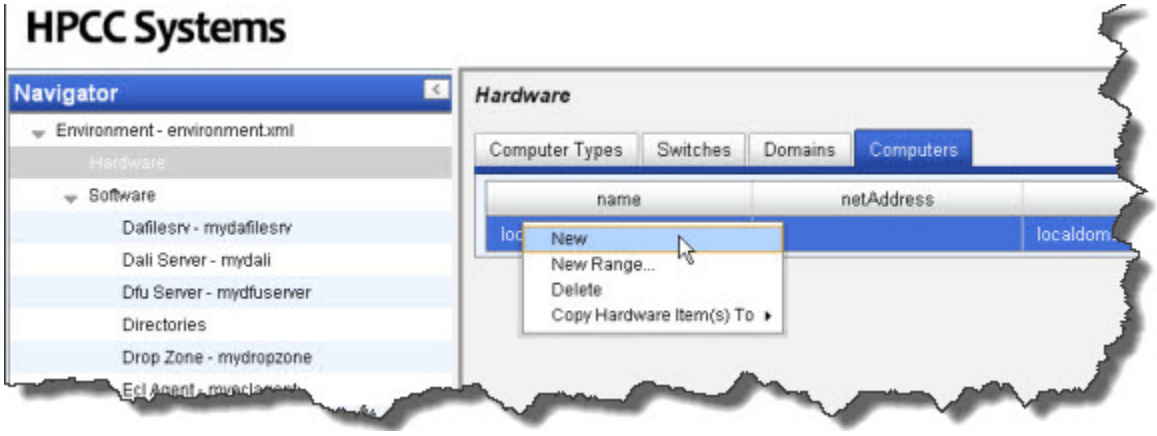
Follow the steps below to modify your configuration.

1. Check the box for **Write Access.**

2. From the **Navigator** pane, select **Hardware**.

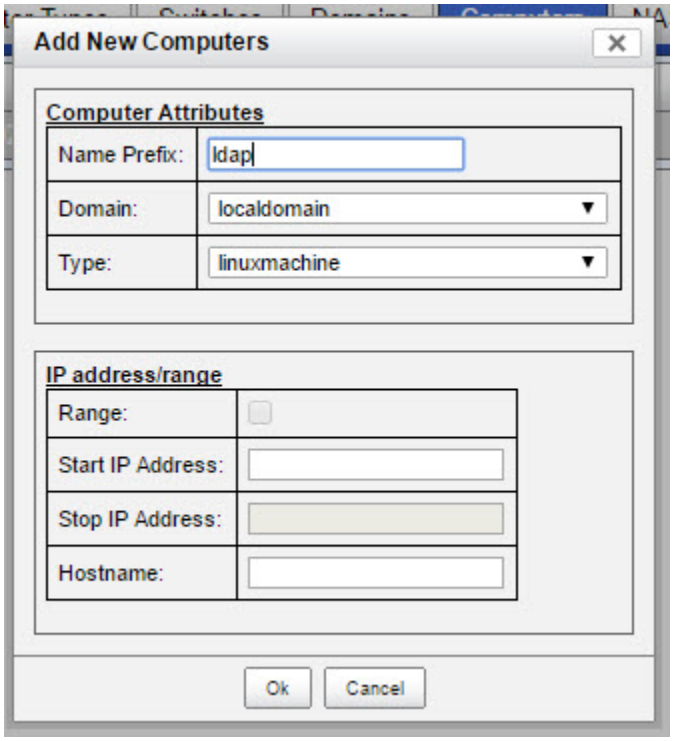
3. Select the **Computers** tab from the panel on the right.

4. Right-click on the table below computers and select **New** from the pop up menu.



The **Add New Computers** dialog displays.

5. Fill in the values for the **Computer Attributes**



a. Provide a **Name Prefix**, for example: ldap.

This helps you to identify it in the list of computers.

b. Fill in **Domain** and **Type** with the values of your domain name, as well as the types of machines you are using.

In the example above, **Domain** is localdomain, and the **Type** is linuxmachine. These should correspond to your domain and type.

If you need to add a new domain or machine type to your system to be able to define an existing LDAP server, you should set these up first in the other two tabs in the hardware section.

c. Add the IP address as appropriate for the LDAP server.

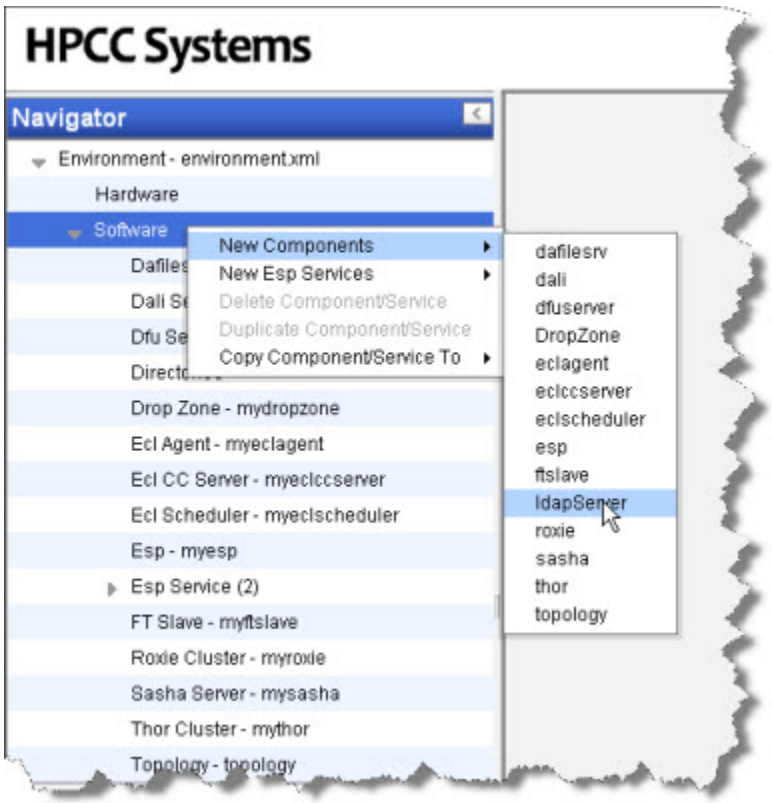
d. Press the **Ok** button.

e. Click on the disk icon to save.

Adding the ldapServer component

After the LDAP Server node has been added to the Hardware configuration, configure the Software LDAP server definition.

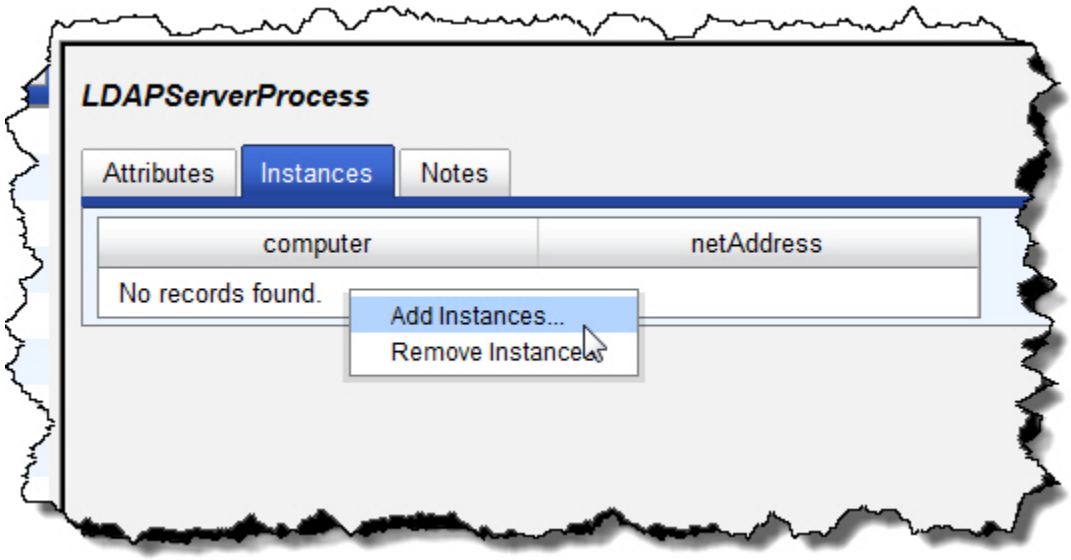
1. Right-click on **Navigator** Pane and choose **New Components** from the pop-up menu, then choose **ldapServer** from the pop-up menu.



	Note: The ldapServer component is merely a definition that specifies an existing LDAP server. It does not install one.

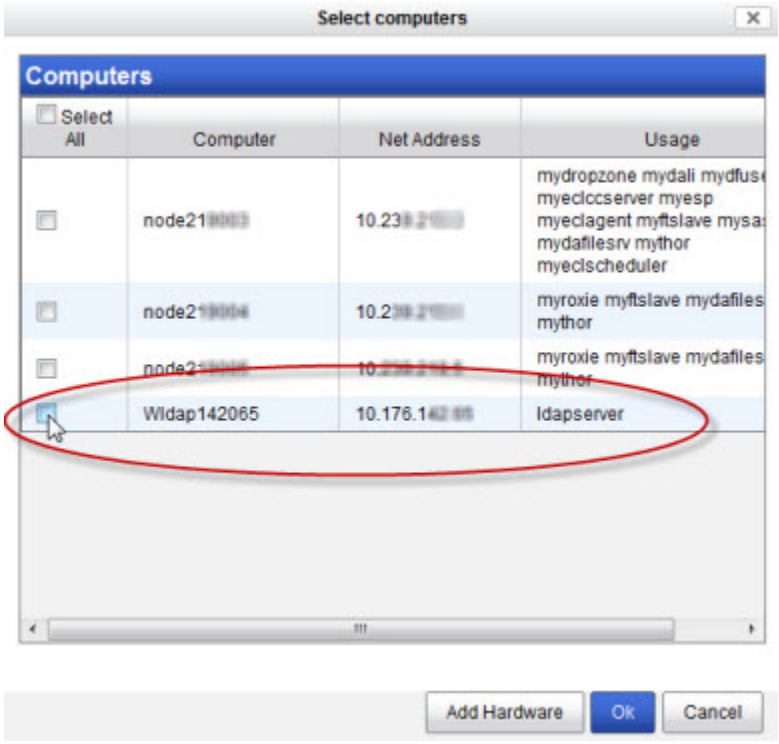
2. Fill in the **LDAP Server Process** properties:

   a. On the **Instances** tab, Right-click on the table on the right hand side, choose **Add Instances...**



   The **Select computers** dialog appears.

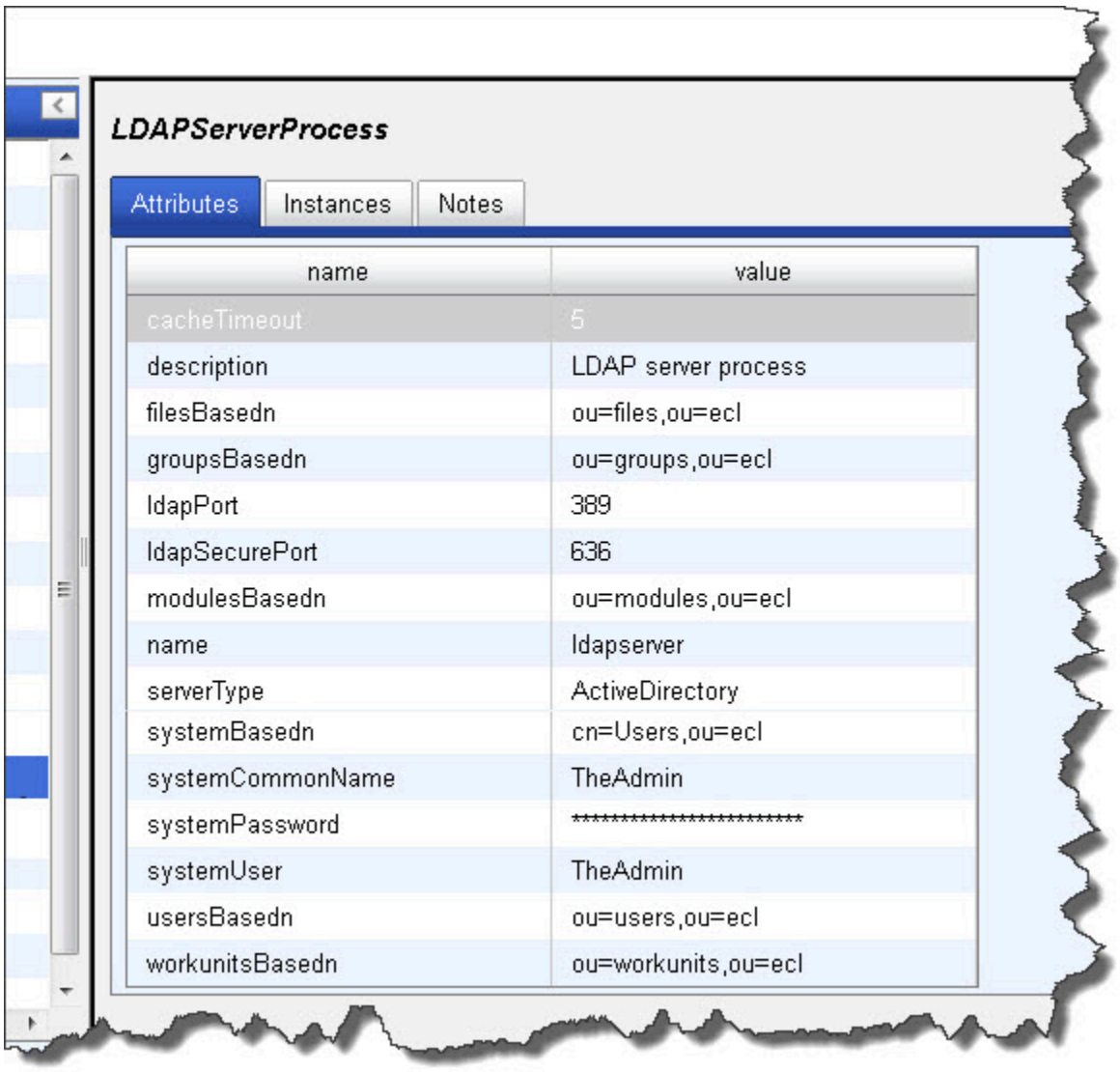
   b. Select the computer to use by checking the box next to it.



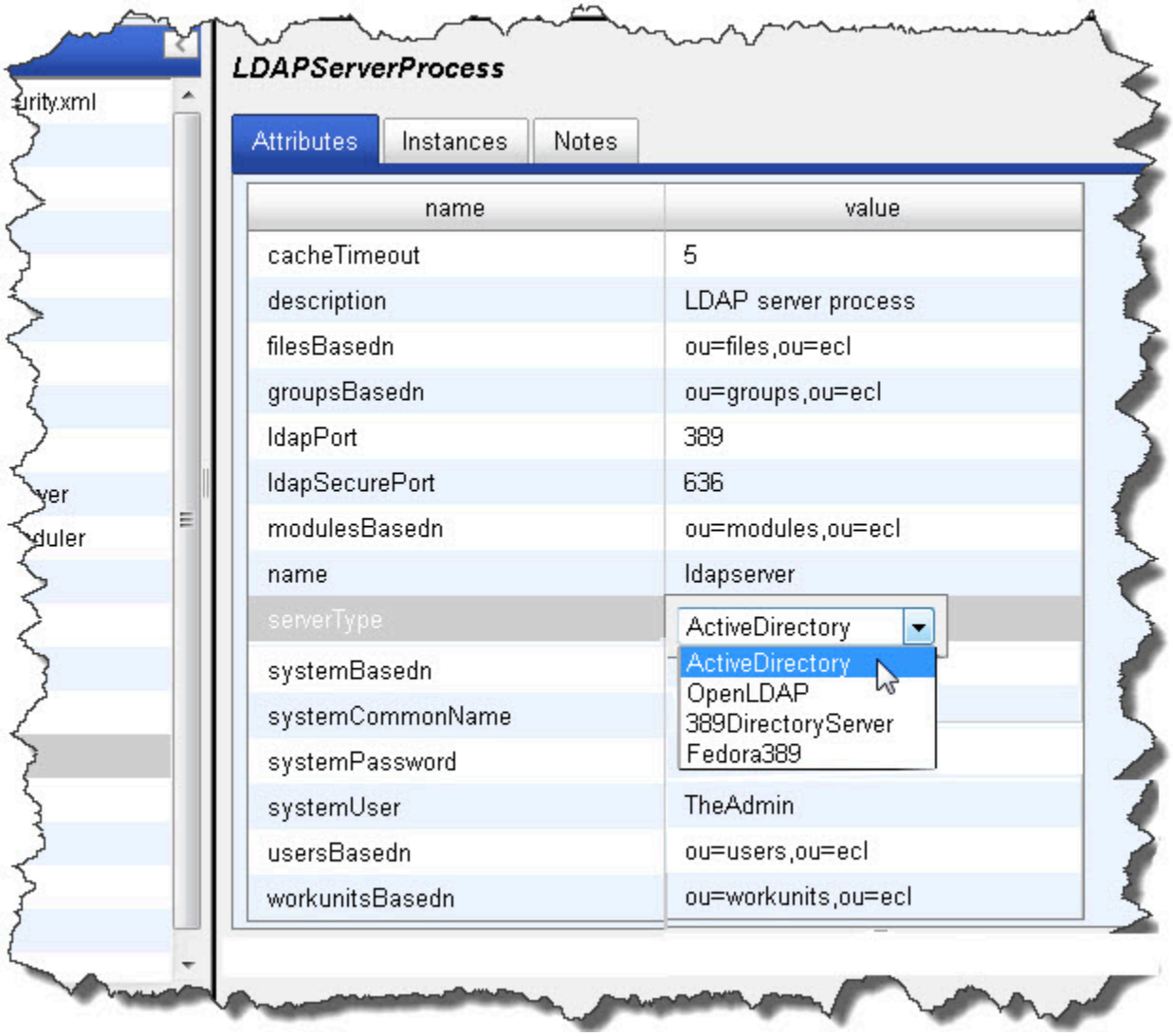
   This is the computer you added in the **Hardware** / **Add New Computers** portion earlier.

   c. Press the **Ok** button.

d. Fill in the **Attributes** tab with the appropriate settings from your existing LDAP Server.



e. Choose the LDAP server type from the serverType attribute drop box.



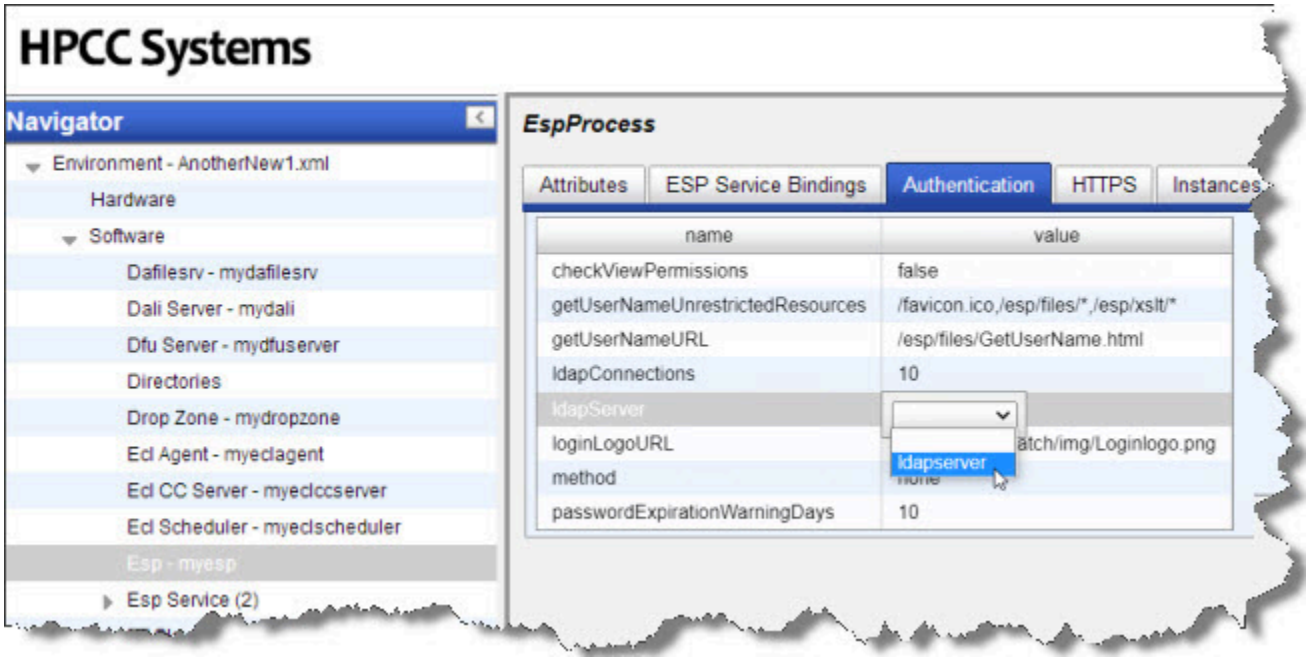
NOTE: Support for OpenLDAP has been deprecated. The option is included only for legacy purposes.

f. Click on the disk icon to save.

Note: The **cacheTimeout** value is the number of minutes that permissions are cached in ESP. If you change any permissions in LDAP, the new settings will not take effect until ESP and Dali refresh the permissions. This could take as long as the cacheTimeout. Setting this to 0 means no cache, but this has performance overhead so it should not be used in production.

3. In the Navigator pane, click on **ESP -- myesp**

4. On the **EspProcess** page on the right hand side, select the **Authentication** tab.



Fill in the appropriate values:

a. Change the **ldapConnections** to the number appropriate for your system (10 is for example only, may not be necessary in your environment).

b. Select the **ldapServer** component that you added earlier from the drop list, for example: ldapserver.

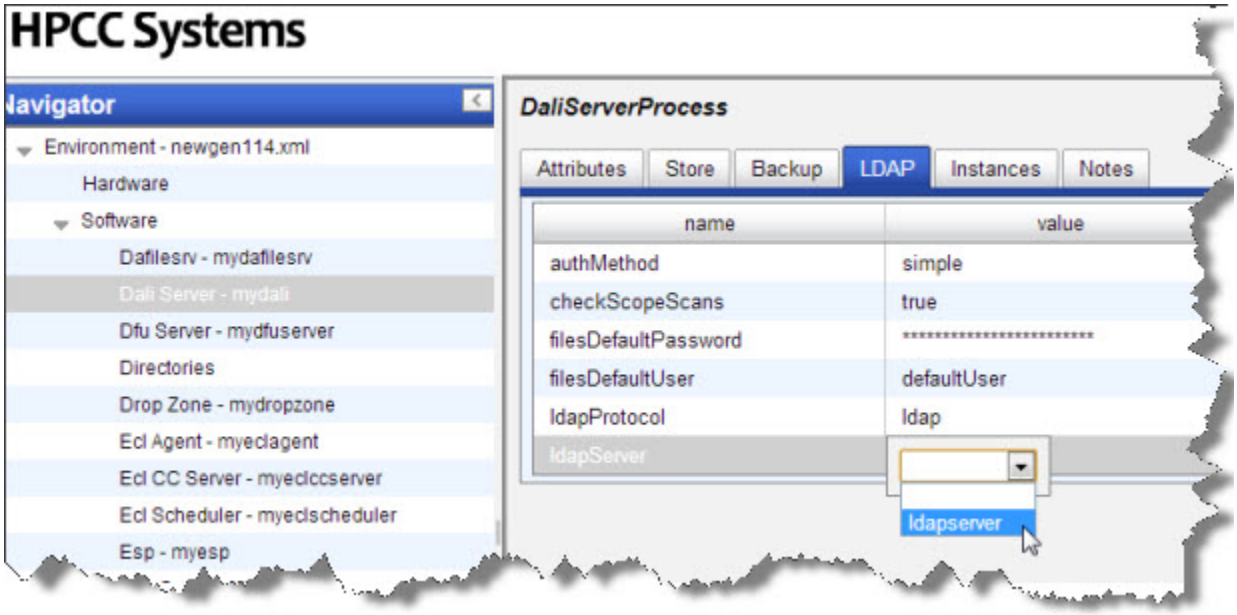
c. Change the **method** value to ldap.

d. Select the ESP Service bindings tab. Verify that your LDAP settings appear in the **resourcesBasedn** and **workunitsBasedn**

e. Click on the disk icon to save.

5. To enable the file scope permissions, configure the file scope security for the Dali Server.

   In the Navigator pane, click on the **Dali Server -- mydali**



   Fill in the values as appropriate:

   a. Select the **LDAP** tab.

   b. Change the **authMethod** to simple

   c. Set the **checkScopeScans** value to *true*.

      Only set this value to true when you want file scope security enabled. Security settings can have three states.

      - None, no authentication and no file scope security.
      - LDAP security for authentication only, without enabling file scope security.
      - LDAP authentication and file scope security enabled.

   d. Change the LDAP values as appropriate to match the settings in your LDAP server component in configuration manager.

      For example, change the **ldapServer** to the value you gave your LDAP Server, in our example it is: *ldapserver.*

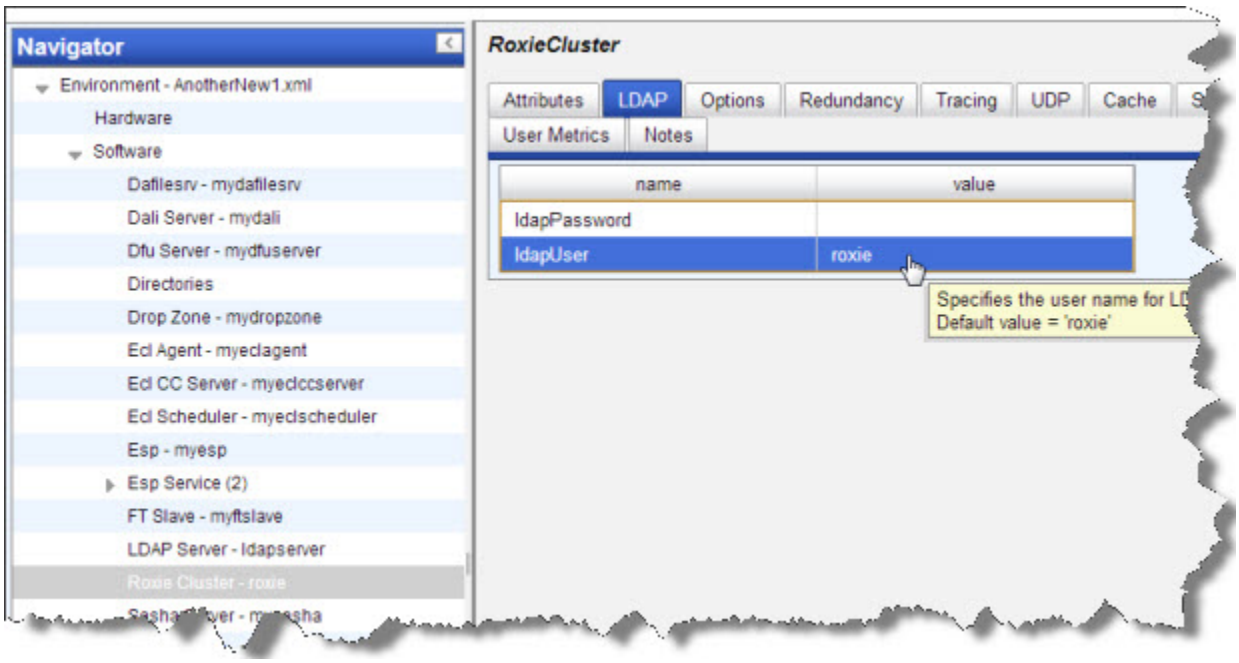
      Confirm the change when prompted.

      The **filesDefaultUser** is an LDAP account used to access files when no user credentials are supplied. This is similar to a guest account, so it should be an account with **very** limited access, if used at all. To disable access without credentials, leave **filesDefaultUser** blank.

      The **filesDefaultPassword** is the password for that account.

   e. Click on the disk icon to save.

6. In the Navigator pane, click on the **Roxie Cluster -- myroxie**



a. On the **RoxieCluster** page on the right hand side, select the **LDAP** tab.

b. Locate the **ldapUser** field and verify that there is a valid HPCC Systems user who is a member of the Authenticated Users group on your LDAP server. For example, the "*roxie*" user assumes that the "*roxie*" user is a valid HPCC Systems authenticated user.

c. Add the password security for Roxie by adding it to the **ldapPassword** field on the same tab.

	In order to run Roxie queries with File Scope security, ensure that a Roxie user is created in the list of authenticated users. In the following section, *Adding and editing users*, add the *roxie* user and make sure that password is the same as the one entered in Configuration Manager.

Installing the Default Admin user

After enabling your configuration for LDAP security, you must copy your environment file to the /etc/HPCCSystems directory. See the section *Configuring a Multi-Node System* for more info about configuring your system. With the correct environment.xml file in place, you must then run the **initldap** utility that initializes the security components and the default users.

The initldap Utility

The initldap utility creates the HPCC Systems Administrator's user account and the HPCC Systems OUs for a newly defined LDAP server. The initldap utility extracts these settings from the LDAPServer component(s) in the environment.xml bound to the configured ESPs.

You run the **initldap** utility once you complete your configuration with LDAP components enabled and have distributed your environment.xml file to all nodes.

```
sudo /opt/HPCCSystems/bin/initldap
```

The **initldap** utility prompts you for LDAP Administrator credentials. Enter the appropriate values when prompted.

The following example of initldap for a 389DirectoryServer deployment.

```
Enter the '389DirectoryServer' LDAP Admin User name on '10.123.456.78'...Directory Manager
Enter the LDAP Admin user 'Directory Manager' password...********

Ready to initialize HPCC Systems LDAP Environment, using the following settings
       LDAP Server     : 10.123.456.78
       LDAP Type       : 389DirectoryServer
       HPCC Admin User : HPCCAdmin389
Proceed?  y/n
```

User Security Maintenance

Configuring an HPCC Systems® platform to use Active Directory or LDAP-based security allows you to set permissions to control access to Features, File Scopes, and Workunit Scopes.

Introduction

HPCC Systems® maintains security in a number of ways. HPCC Systems® can be configured to manage users' security rights by pointing either at Microsoft's Active Directory on a Windows system, or a 389Directory Server on Linux systems.

Using the Permissions interface in ECL Watch, administrators can control access to features in ECL IDE, ECL Watch, ECL Plus, DFU Plus, and the ECL modules within the Attribute Repository. Optionally, you can also implement file and workunit access control by enabling that setting in the Dali server.

Establish permissions by group or by user and define them by association with a particular feature of the HPCC Systems platform. Permissions can be defined for each unique combination of group and feature. Permissions are separated into the following categories:

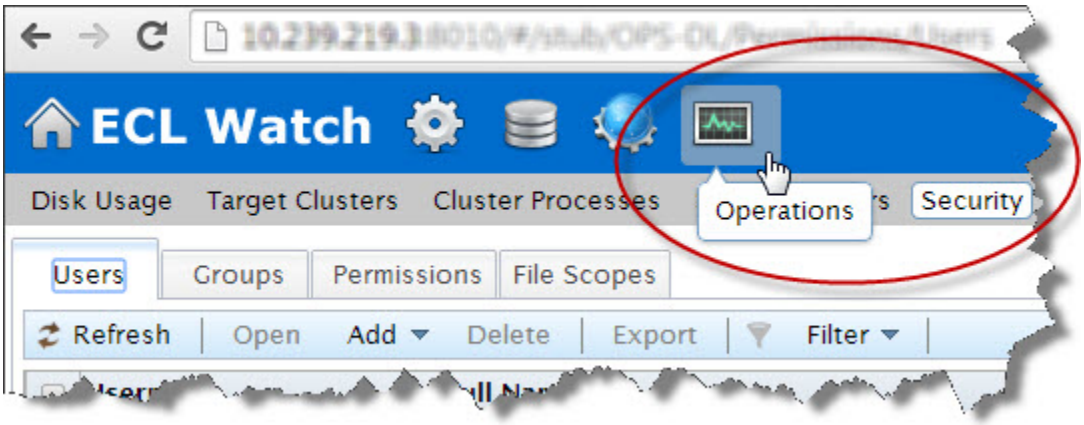
Esp Features for SMC	Controls access to features in ECLWatch and similar features accessed from ECL IDE.
Esp Features for WsEclAccess	Controls access to the WS-ECL web service
Esp Features for EclDirectAccess	Controls access to the ECLDirect web service
File Scopes	Controls access to data files by applying permissions to File scopes
Workunit Scopes	Controls access to Workunits by applying permissions to Workunit scopes
Repository Modules	Controls access to the Attribute Repository and Modules in the repository (legacy)

Security Administration using ECL Watch

Administrator rights are needed to manage permissions. Once you have administrator access rights, open ECL Watch in your browser using the following URL:

- **http://nnn.nnn.nnn.nnn:pppp (where nnn.nnn.nnn.nnn is your ESP Server's IP Address and pppp is the port. The default port is 8010).**

Security administration is controlled using the **Security** area of ECL Watch. To access the Security are click on the**Operations** icon, then click the **Security** link from the navigation sub-menu.



There are three areas where permissions may be set:

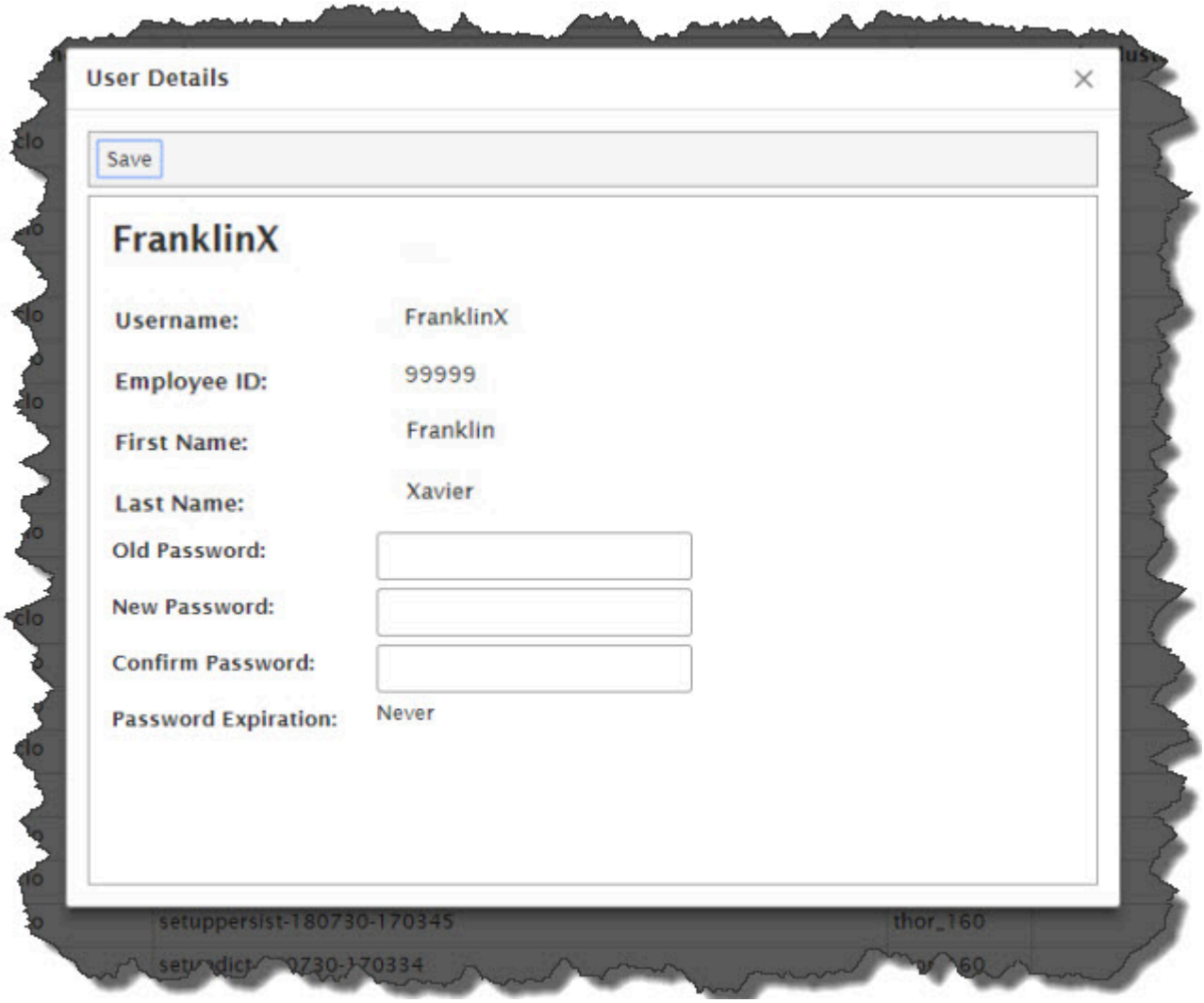
- **Users**. Shows all the users currently setup. Use this area to add or delete a user, edit a user's details, set/reset a user's password and view the permissions currently assigned to a user.
- **Groups**. Shows all the groups currently setup. Use this area to add or delete a group, view and edit the members of a group, view and edit the permissions that have been set for a group.
- **Permissions**. Shows the features of the HPCC Systems where permissions may be set. Use this area to view the permissions currently set for any area of HPCC Systems, or to add groups and users and set/modify their permission for a specific feature

	**NOTE:** Use caution when setting any explicit **deny** permission setting. The most restrictive permission always applies.

Information about your account

To find out more information about your account, in ECL Watch click on your username link under **Logged In As:** at the top of the ECL Watch page.

- A **User Details** tab with your account information displays.



- You can change your password here, if desired.
- You can also verify the password expiration date, if your password is set to expire.

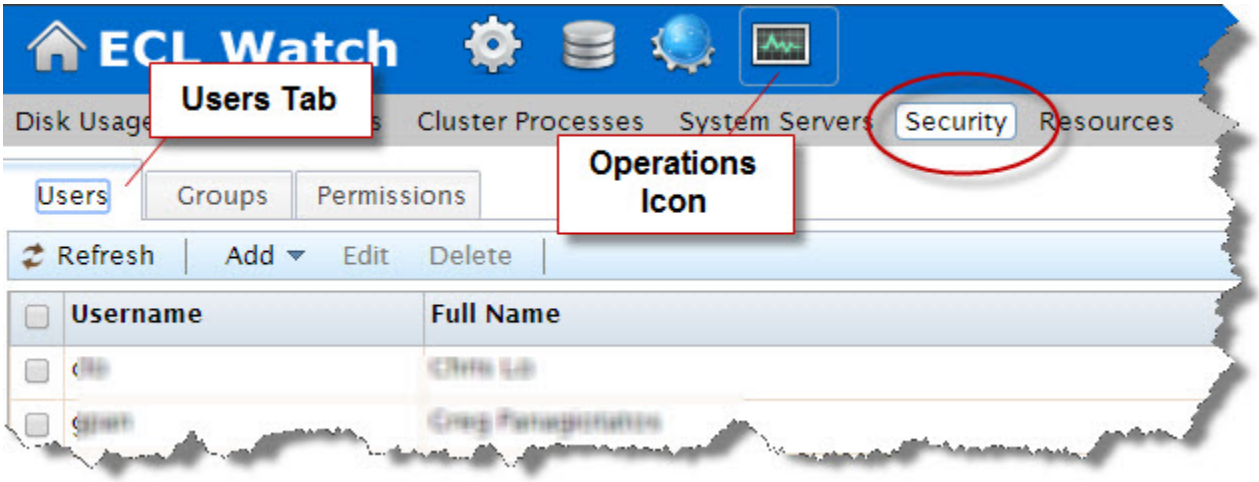
Setting and modifying user permissions

In a security-enabled environment, access to ECL Watch and its features is controlled using a login and password. The **Users** area enables you to control who has access to ECL Watch and the features of your HPCC Systems to which they have access. Permissions can be set for users based on their individual needs and users can also be added to groups which have already been set up. Use the **Users** menu item to:

- Add a new user (**note**: the Username cannot be changed)
- Delete a user
- Add a user to a group
- Change a user's password
- Modify the details/permissions of an individual user

Adding and editing users

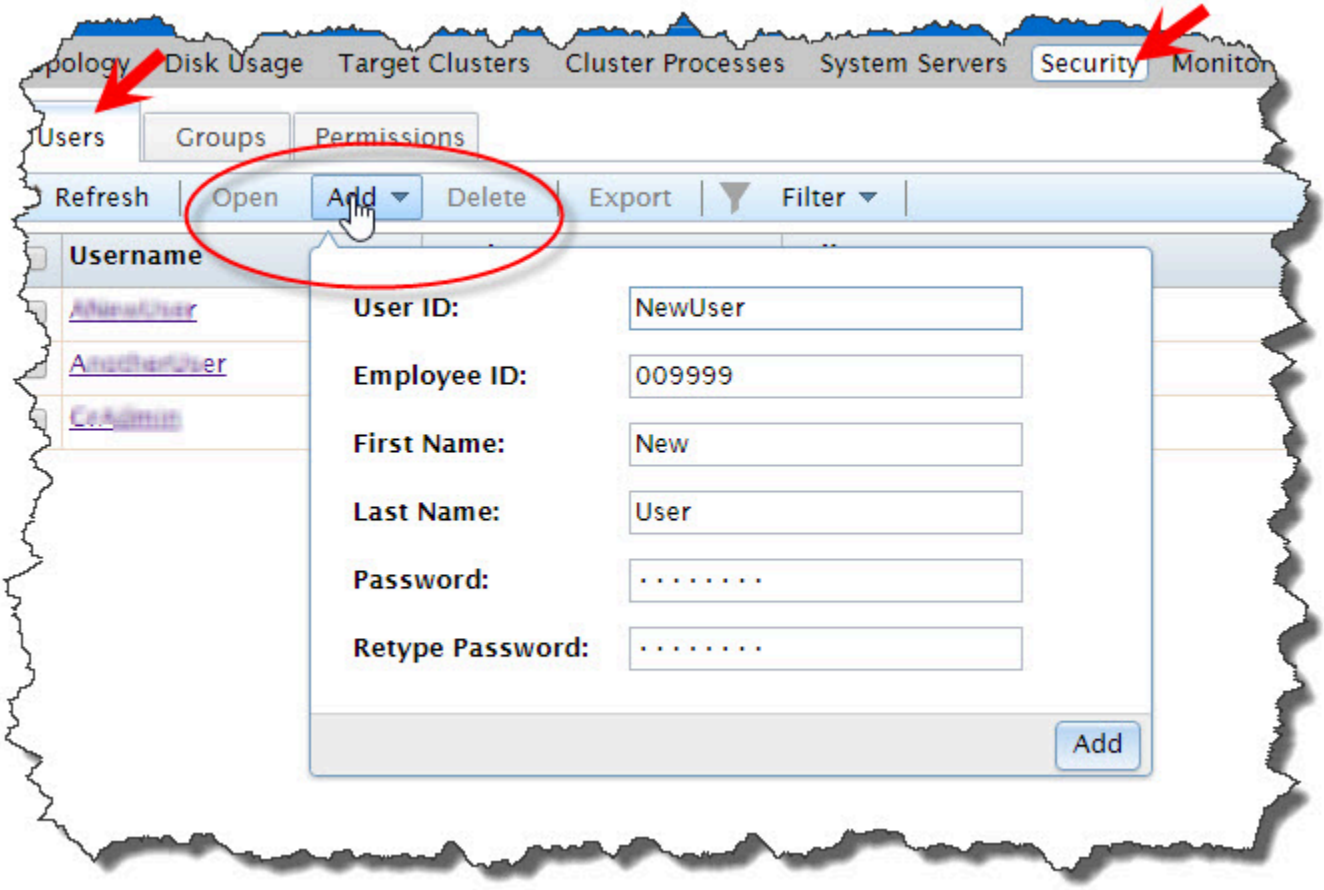
To access the user administration sections click on the **Operations** icon, then click the **Security** link from the navigation sub-menu. Click on the **Users** tab to add or edit users.



All current users are identified in the list by their Username and Full Name.

To add a new user to the list of authenticated users:

To add a new user you must have Administrator level access.



1. Press the **Add** button.

   The add user dialog displays.

2. Enter a **Username**.

   This is the login name to use ECL Watch, ECL IDE, WsECL, etc.

3. Enter the **First Name** and **Last Name** of the user.

   This information helps to easily identify the user and is displayed in the **Full Name** field on the main **Users** window.

4. Enter a **Password** for the user and then confirm it in the **Retype Password** field.

   NOTE: The password must conform to the policy of your security manager server.

5. Press the **Add** button.

   A successful addition opens a new tab where you can verify the new user's information.

6. Press the **Save** button.

Once added, the new user displays in the list and you can modify details and set permissions as required.

To modify a user's details:

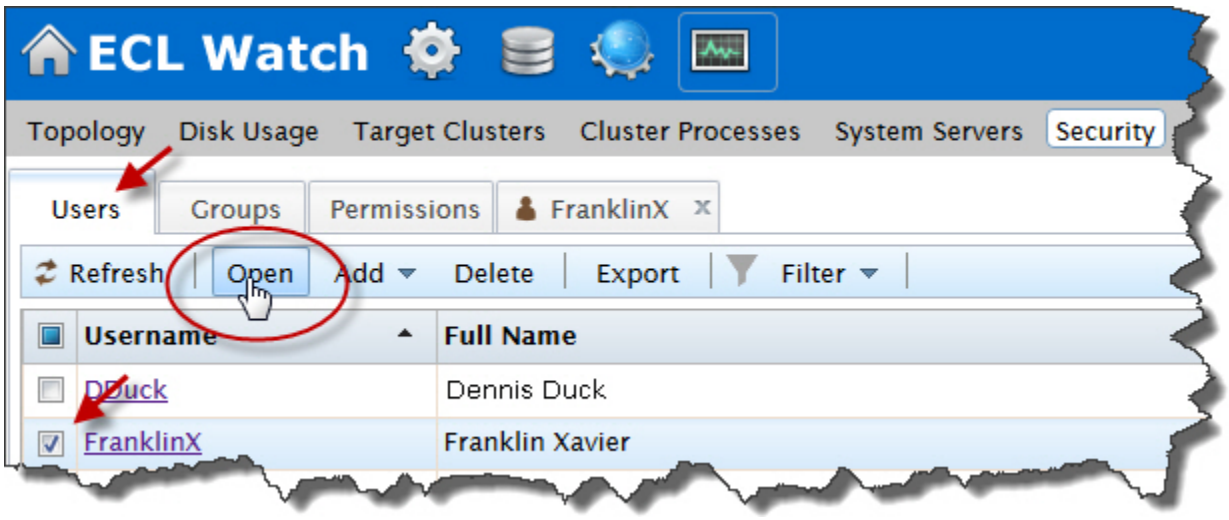
Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Users tab**.

   The users display in a list.

2. Select the user (or users) to modify. Click on the **Username** link to open the users' details tab.

   To select multiple users, check the box next to the Username to select. This enables the Users action buttons. Press the **Open** action button.



A tab opens for each user selected. On each user's tab there are several sub-tabs.

The user's details are on the **Summary** tab.

3. Modify the user's details as required (if more than one user selected, repeat for each user).

   Note: The **Username** cannot be changed.

4. Press the **Save** button.

   A confirmation message displays.

To add a user to a group:

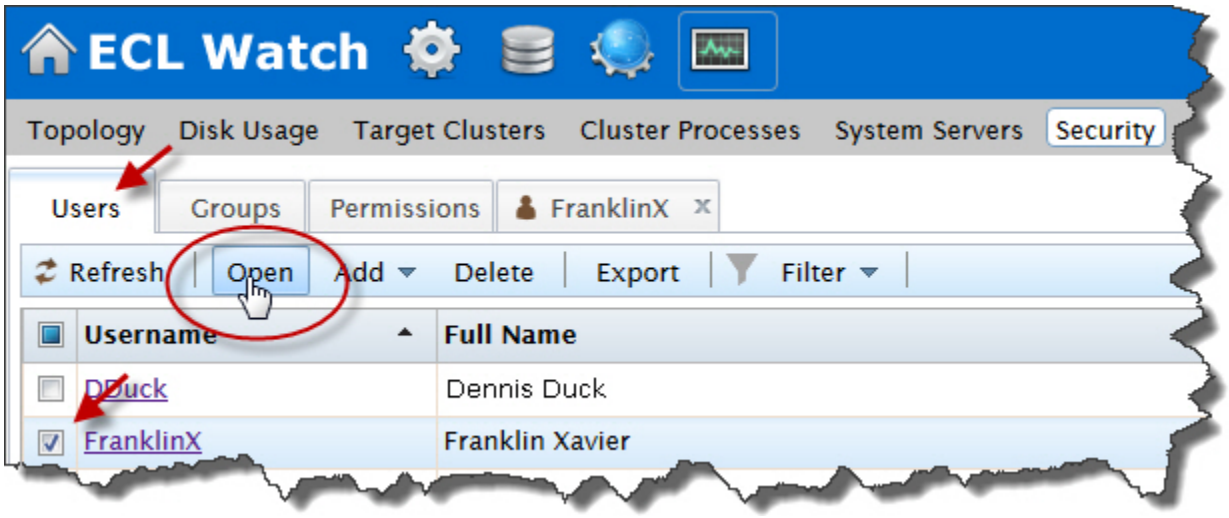
Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Users tab**.

   The users display in a list.

2. Select the user (or users) to modify. Click on the **Username** link to open the users' details tab.

   To select multiple users, check the box next to the Username to select. This enables the Users action buttons. Press the **Open** action button.

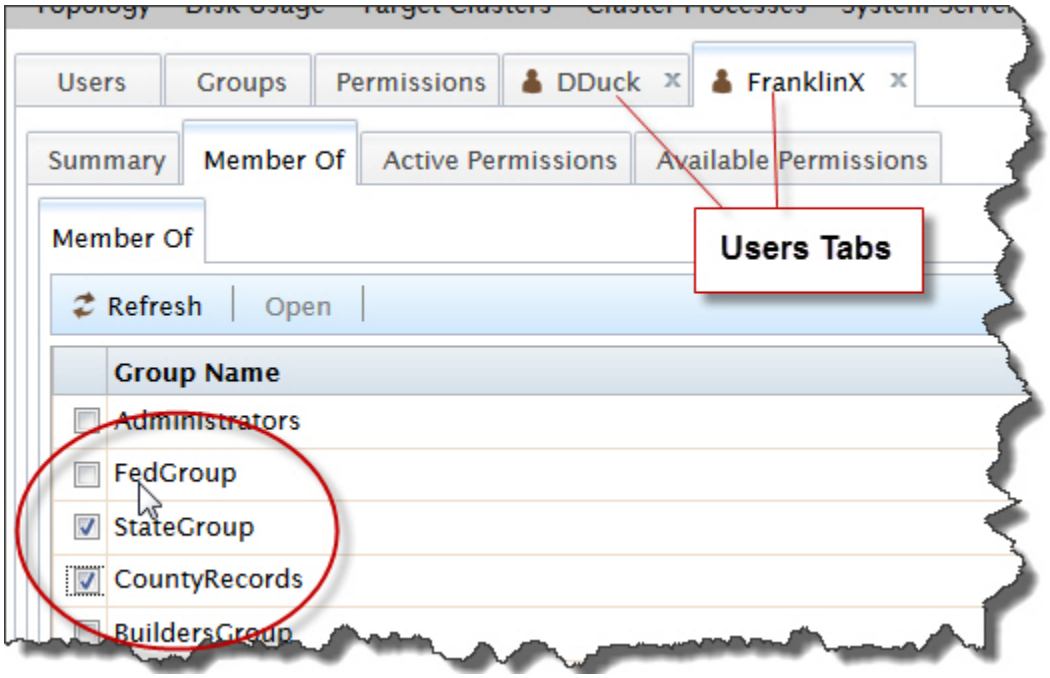


   A tab opens for each user selected. On each user's tab there are several sub-tabs.

   The user's details are on the **Summary** tab.

3. Click on the tab for the user to modify (if more than one user selected, repeat for each user).

   On the user's tab there are several sub-tabs.



Click on the **Member Of** sub-tab to modify that user's groups.

4. On the **Member Of** tab for that user, a list of the available groups display.

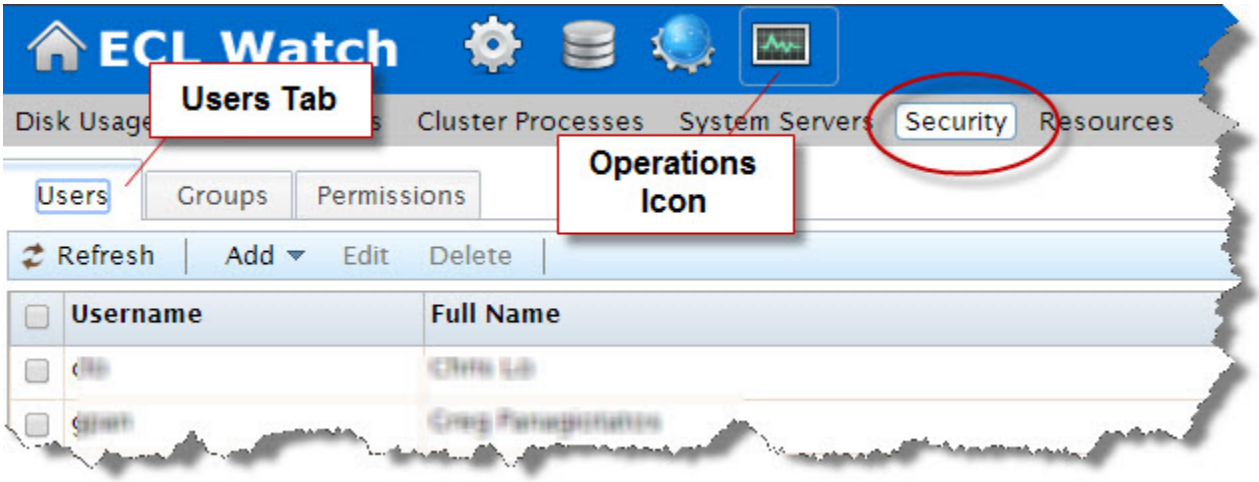
   To add the user to the group, check the box next to the desired group.

5. The changes are automatically saved. Close the tab.

To promote a user to an Administrator

To modify a users credentials you must have Administrator level access. You can designate the HPCC Systems Administrator account to have limited permissions only relating to HPCC Systems elements and not LDAP administrator's rights. To promote a user to an HPCC Systems Administrator, add the user to the configured **Administrators** group.

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

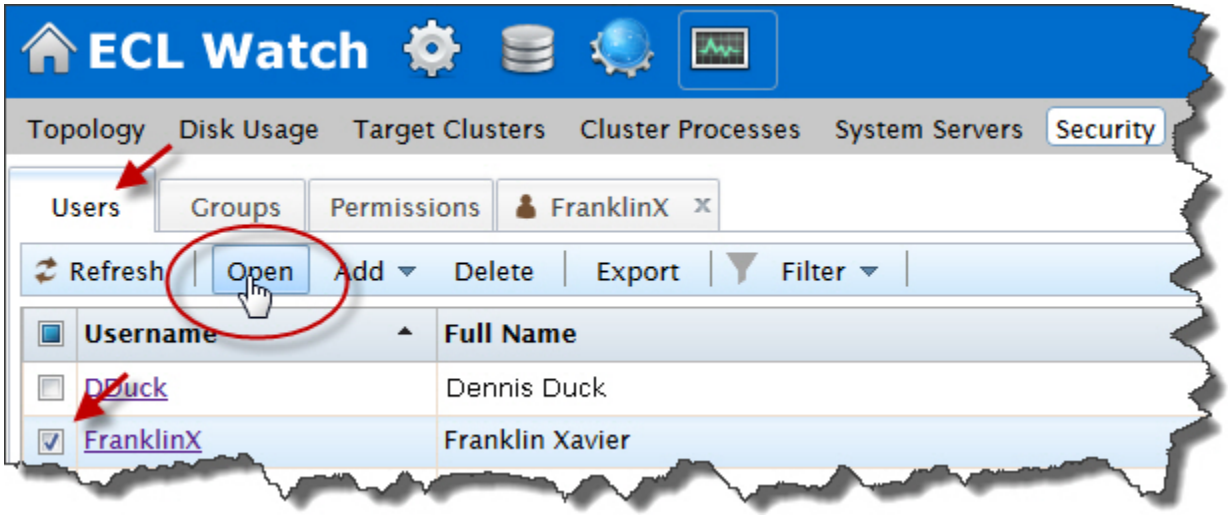


1. Click on the **Users tab**.

The users display in a list.

2. Select the user (or users) to promote. Click on the **Username** link to open the users' details tab.

   To select multiple users, check the box next to the Username to select. This enables the Users action buttons. Press the **Open** action button.



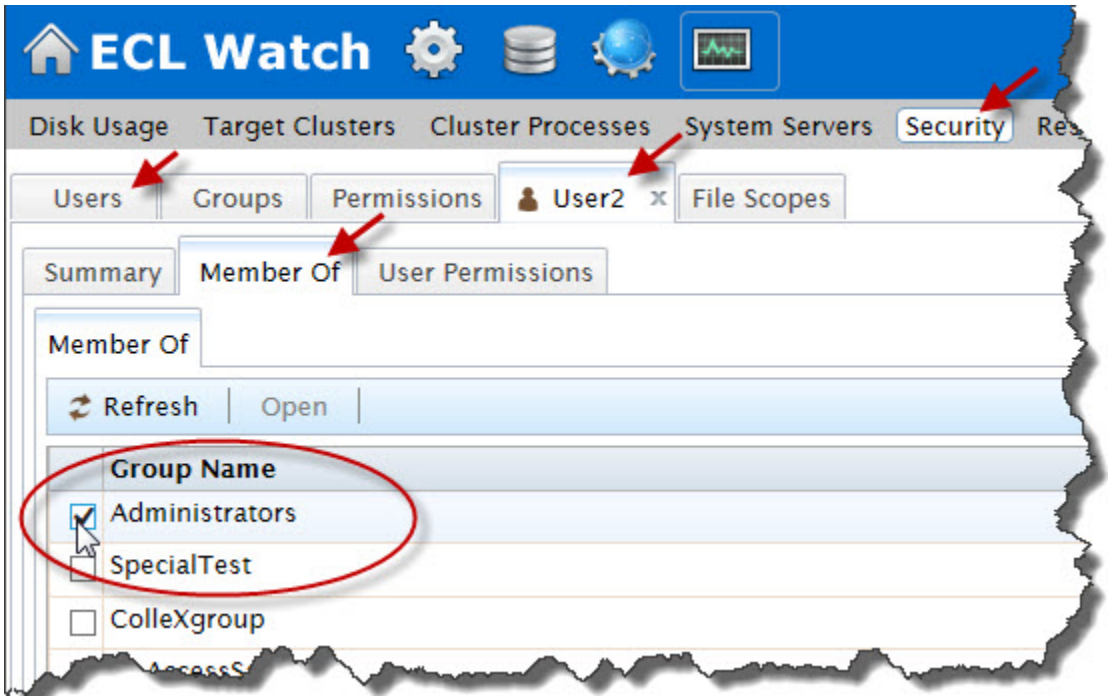
   A tab opens for each user selected. On each user's tab there are several sub-tabs.

   The user's details are on the **Summary** tab.

3. Click on the tab for the user to modify (if more than one user selected, repeat for each user).

   On the user's tab there are several sub-tabs.

   Click on the **Member Of** sub-tab.



4. Select **Administrators** by placing a check in box.

   NOTE: The name of the default Administrators group could vary. It is a configurable value defined as the value of **adminGroupName** in the configuration. For example, if you set the adminGroupName to "HPCCAdministrators", in the environment then HPCCAdministrators would display in the list.

5. The changes are automatically saved. Close the tab(s).

To delete a user from a group:

To delete a user from a group you must have Administrator level access.

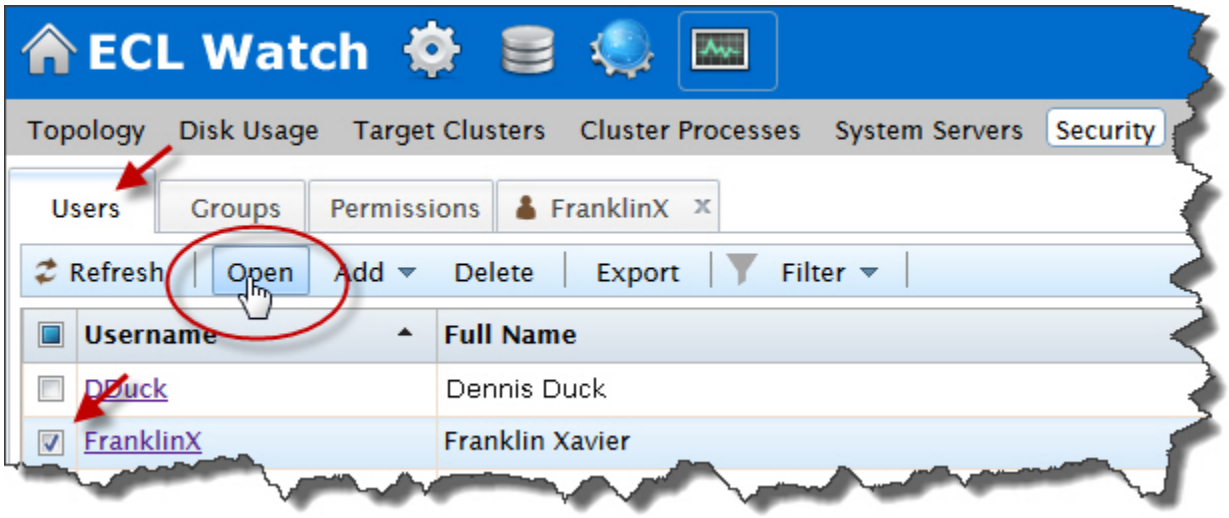
Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Users tab**.

   The users display in a list.

2. Select the user (or users) to remove. Click on the **Username** link to open the users' details tabs.

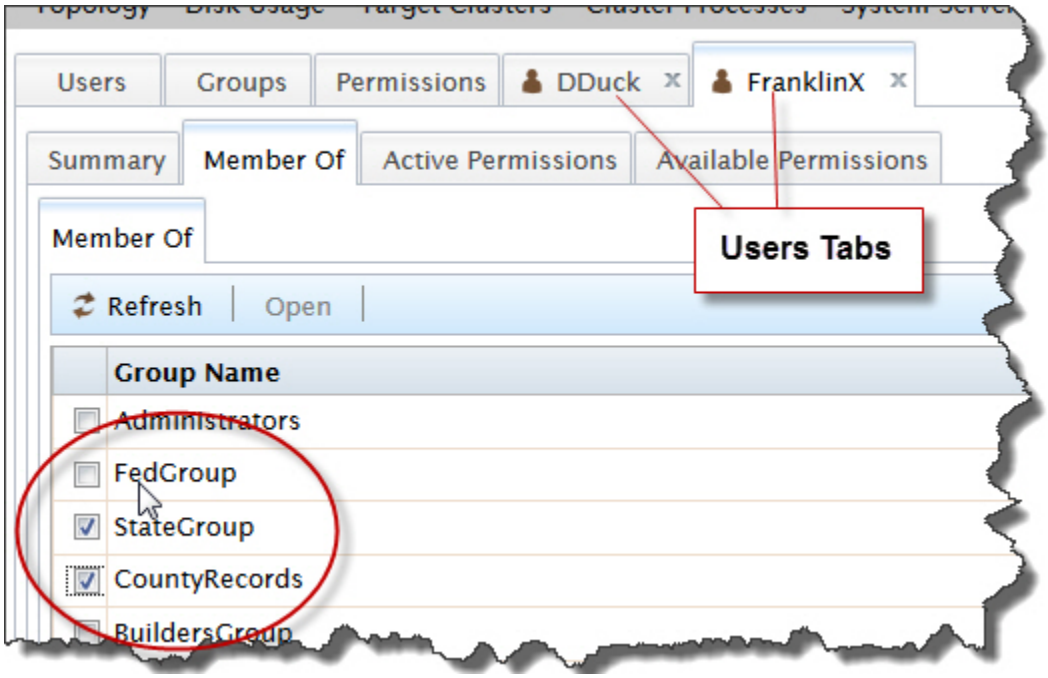
   To select multiple users, check the box next to the Username to select. This enables the Users action buttons. Press the **Open** action button.



   A tab opens for each user selected. On each user's tab there are several sub-tabs.

3. Click on the tab of the user to modify (if multiple users selected, repeat for each user).

   On the user's tab there are several sub-tabs.



Click on the **Member Of** sub-tab to modify that user's groups.

4. On the **Member Of** tab for that user, there is a list of the available groups.

   There is a check in the box next to each group that user belongs to.

   To remove that user from a group, uncheck the box next to the desired group.

5. The changes are automatically saved. Close the tab.

To change a user's password:

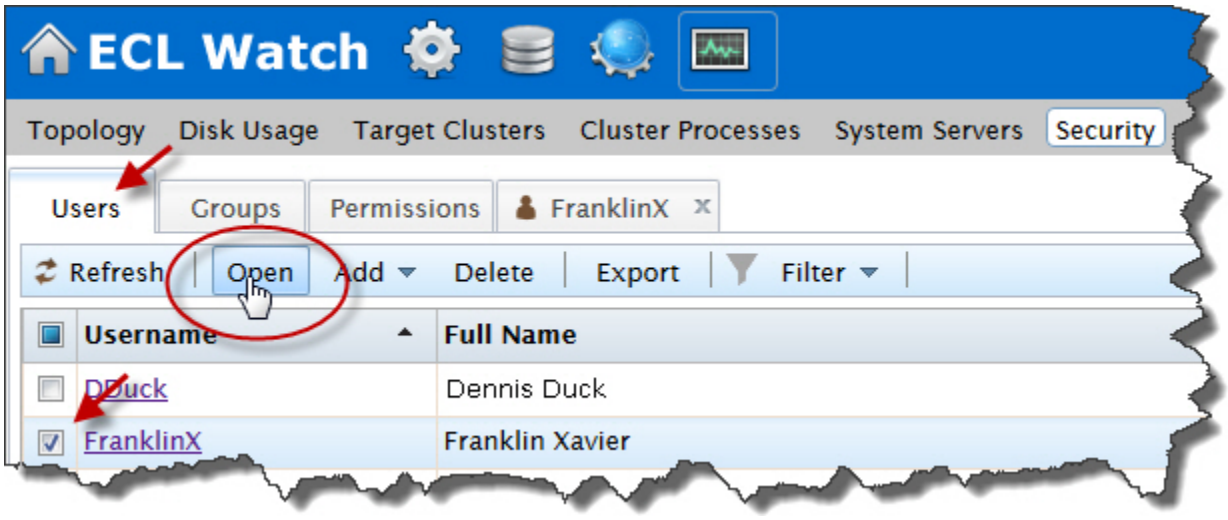
Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Users tab**.

   The users display in a list.

2. Select the user (or users) to modify. Click on the **Username** link to open the users' details tab.

   To select multiple users, check the box next to the Username to select. This enables the Users action buttons. Press the **Open** action button.



A tab opens for each user selected. On that tab there are several sub-tabs.

The user details are on the **Summary** tab.

3. Select the Summary tab.
4. Change the password in the **Password** and **Retype New Password** fields as required on the User details summary tab (if multiple users selected, repeat for each user).

   Note: The **Username** cannot be changed.
5. Press the **Save** button.

   A confirmation message displays.

To delete a user from the list of authenticated users:

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Users** tab.

   The users display in a list.
2. Check the box to the left of the user(s) you want to remove.

   Note: These users will no longer have access to ECL Watch.
3. Press the **Delete** action button.

   Confirmation displays.

Setting permissions for an individual user

There may be occasions when you need to modify the permissions for individual users. For example, users may have individual security needs that are not completely covered in any group or, there may be occasions when a user requires temporary access to an HPCC Systems feature. Permissions set in this area of ECL Watch only affect the user you choose. Most individual permissions you set here overwrite ones set in any group to which the user belongs, except in the case of an explicit deny.

To set permissions for an individual user:

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Users tab**.

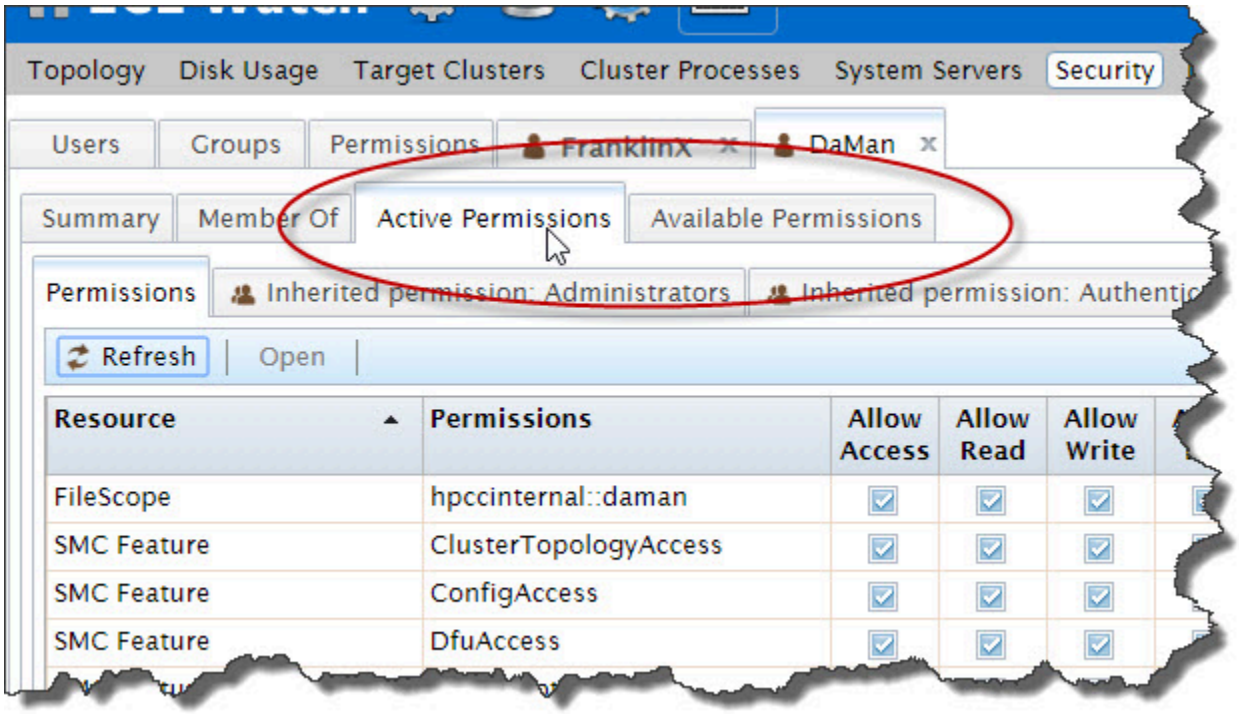
   The users display in a list.

2. Select the user (or users) to modify. Click on the **Username** link to open the users' details tab.

   To select multiple users, check the box next to the Username to select. This enables the Users action buttons. Press the **Open** action button.

3. Click on the tab of the username to modify (if multiple users selected, repeat for each user).

   On the user's tab there are several sub-tabs.

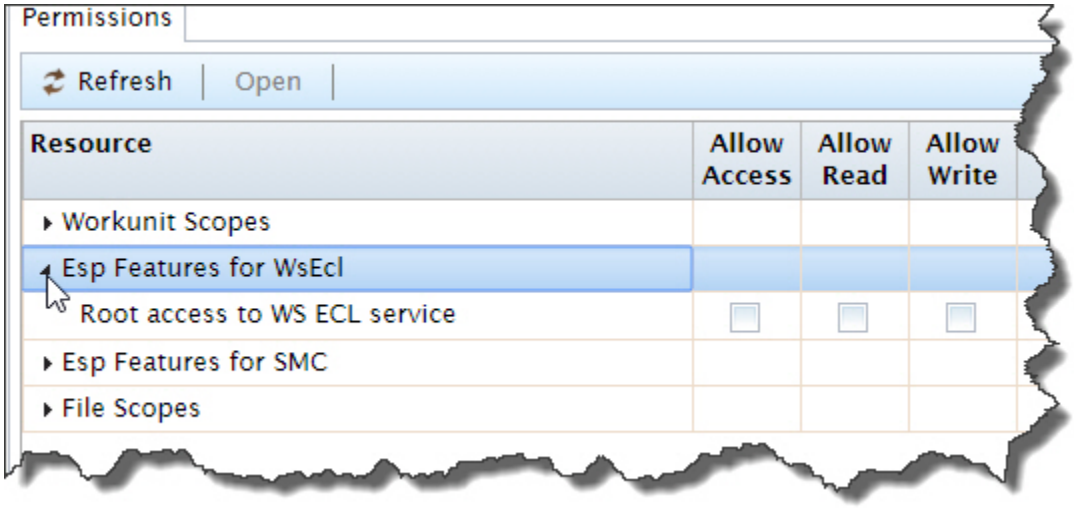


   Click on the **Active Permissions** sub-tab to view the user's current permissions.

4. Click on the **Available Permissions** tab to see all the sets of permissions that are available to apply to that user.

   When you select permissions from the Available Permissions tab, they display and can be set in the Active Permissions tab.

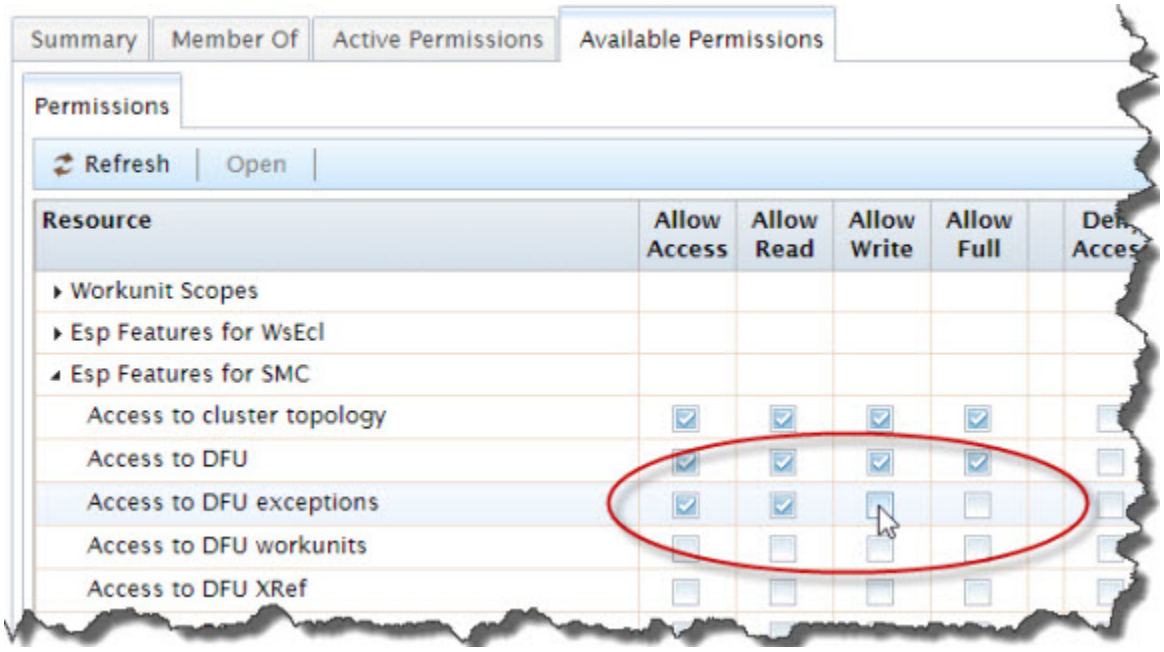
5. Click on the arrow next to the resource to display the permissions that can be set for that resource.



The list of permission groups currently set for this user and the ones the user has inherited are also listed. Click the arrow to allow setting the individual resource settings.

6. There may be more than one resource setting available in each group, be sure to set the permissions for each setting as required.

7. Check the boxes that **allow** and **deny** access as required for the user.



	**NOTE:** Use caution when setting any explicit **deny** permission setting. The most restrictive permission always applies.

8. The changes are automatically saved. Close the tab.

Setting and modifying group permissions

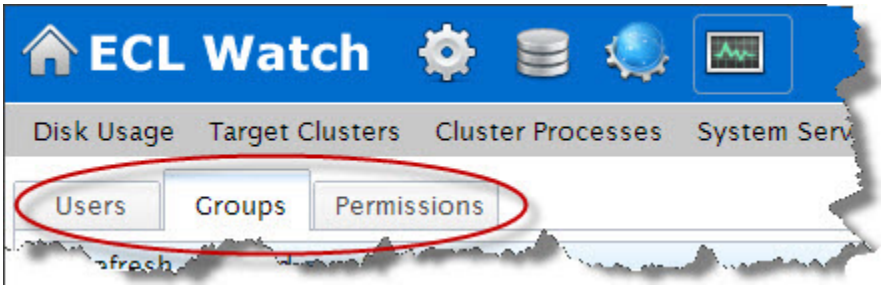
Setting up groups ensures that all users with the same permission needs have the same permission settings. You can give users the access they require to the feature areas of HPCC Systems that they need. There is no limit to the number of groups you can create. You can create as many groups as you need to control access for all your users regardless of their tasks.

Use the **Groups** menu item to:

- Add a new group.
- Delete a group.
- Add members to a group.
- Modify the permissions for a group.

Adding and editing groups

When adding or changing the permissions for a group, all members of that group are given those permission settings. So it is important to be sure that you are giving or denying access to features appropriate for the members of that group. If you need to make a change for a single user (or small number of users), it is probably better to make that change for each individual user as illustrated in the previous sections.

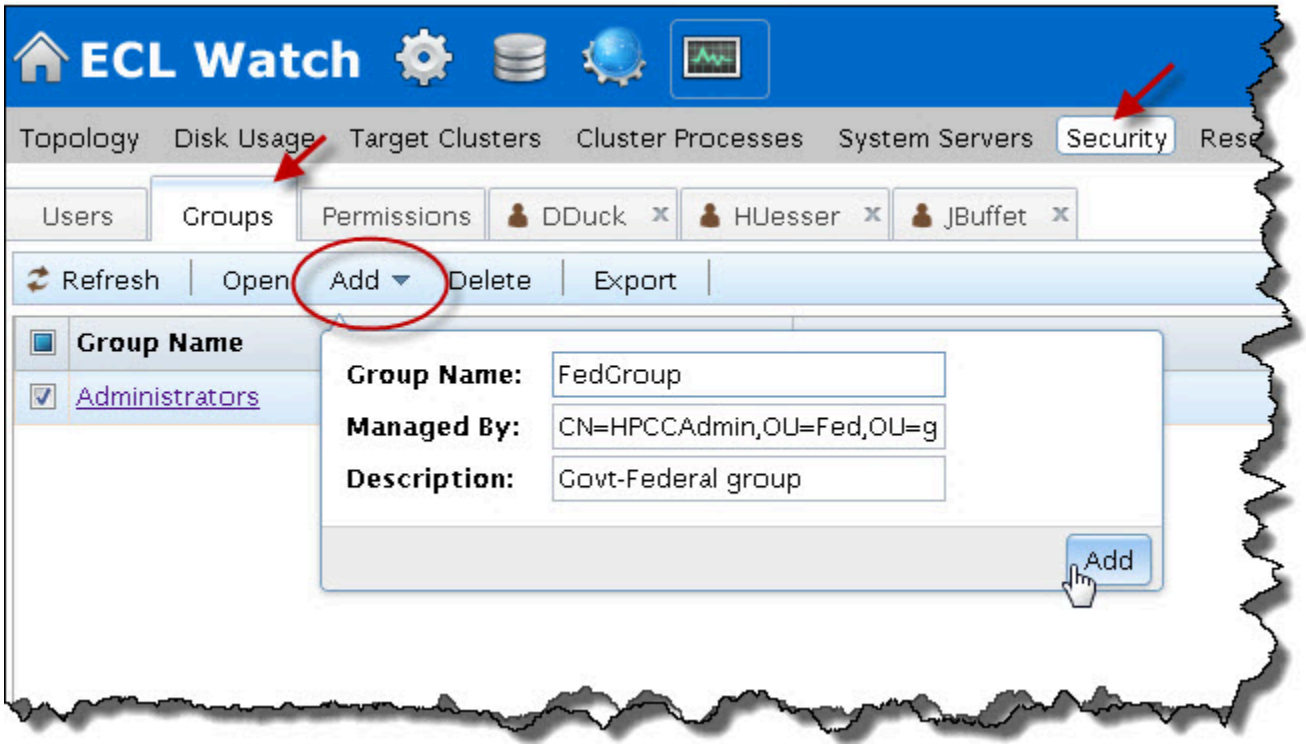


To modify groups, click on the **Operations** icon, then click the **Security** link from the navigation sub-menu. Click on the **Groups** tab.

To add a new group:

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Groups** tab.
2. Press the **Add** action button button.



This opens a dialog where you can enter the name for the group.

3. Enter a **Group Name**.
4. Enter the fully qualified Distinguished Name for the owner of the group **Managed By** field.
5. Enter a description of the group. (optional)
6. Press the **Add** button.

   This opens a new tab for the group and several sub tabs

   The **Summary** sub-tab displays the group name.

   The **Members** tab displays the list of users, check the box next to each user to add to the group.

   The **Active Group Permissions** tab displays the permissions applied to the group.

   The **Available Group Permissions** tab displays all the available permissions, selecting from the Available Permissions applies them to the Active Group Permissions.

   You can set the permissions and add members to this group from the respective sub-tabs on that group tab.

To delete a group:

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Groups** tab.
2. Locate the group in the list and check the checkbox next to it.

3. Press the **Delete** action button.
4. Press the **OK** confirmation button.

   The group no longer displays in the list.

To add new members to a group:

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Groups** tab.
2. Locate the group in the list and check the box next to it.
3. Press **Open** action button.

   This opens a new tab for the group.

   The sub-tabs display: **Summary**, **Members**, **Active Group Permissions**, and **Available Group Permissions**.
4. Select the **Members** tab.

   The members tab displays a list of all users on the system. The users that belong to the selected group have a check in the box next to them.
5. Check the box(es) to the left of the users you want to add to the group.
6. The changes are automatically saved. Close the tab.

To delete members from a group:

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click on the **Groups** tab.
2. Locate the group in the list and check the box next to it.
3. Press the **Open** action button.

   This opens a new tab for the group.

   The Groups tab has several sub-tabs: **Summary**, **Members**, **Active Group Permissions** and **Available Group Permissions**.
4. Select the **Members** tab.

   The Members tab displays a list of all users on the system. The users that belong to the selected group have a check in the box next to them.
5. Uncheck the box(es) to the left for all users you want to delete from the group.
6. The changes are automatically saved. Close the tab.

Setting permissions for a group

By default, all users are members of the **Authenticated Users** group. The **Authenticated Users** group has access rights to almost all resources. To set up more restricted controls, you should create specific groups with more restricted permissions.

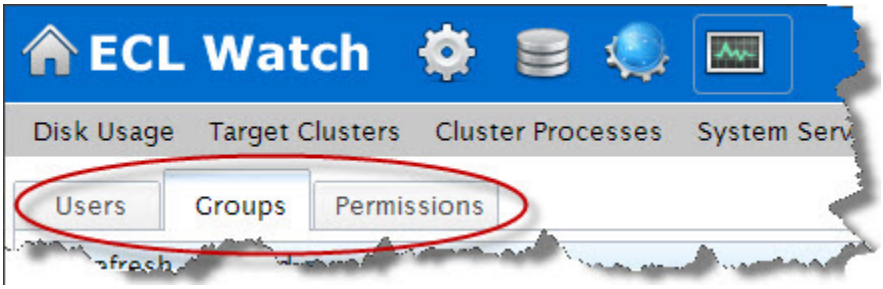
You can then create groups with only those access rights you wish to grant. This approach allows the most flexibility since a single User ID can have multiple group memberships.

As a best practice, you should use **Allow** instead of **Deny** to control access. Denies should be used only as an exception, when possible. If you wish to deny a user access to some specific control, a good practice would be to create a group for that, place the user(s) in that group, then you can deny access to that group.

Remember the most restrictive control takes precedence. For example, if a user is in a group that has deny permission to file access, and the user is in another group where file access is allowed, that user will still not have file access.

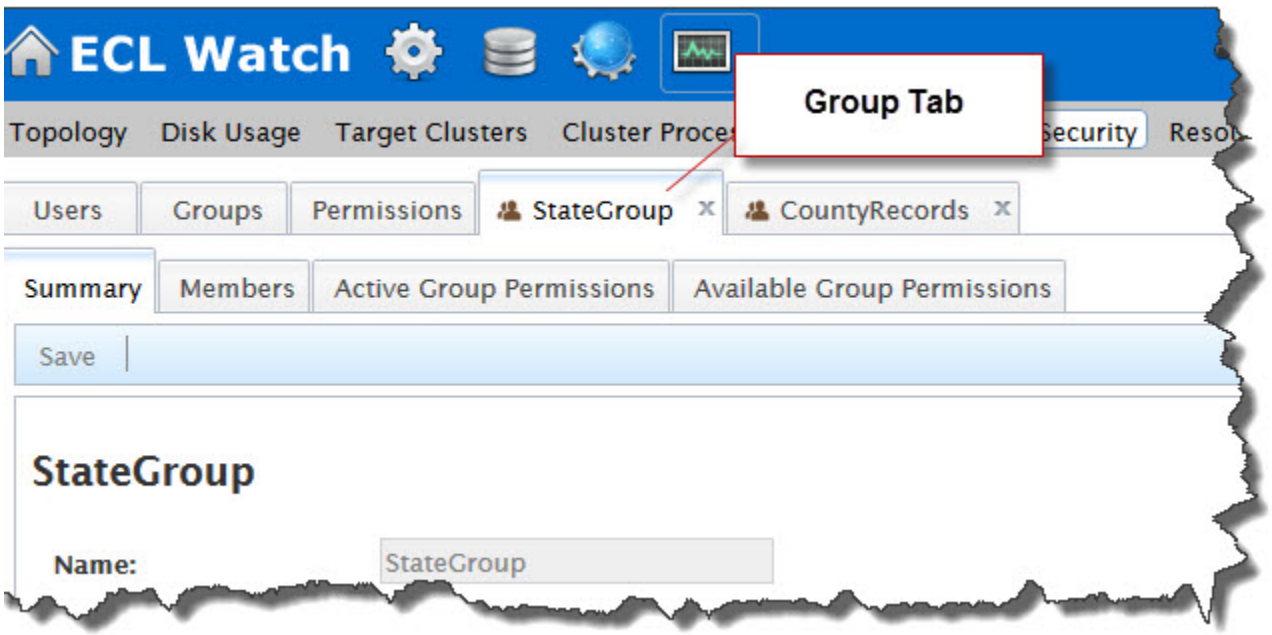
To set permissions for a group:

Click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.



1. Click the **Groups** tab.
2. Locate the group in the list and check the box next to it.
3. Press the **Open** action button.

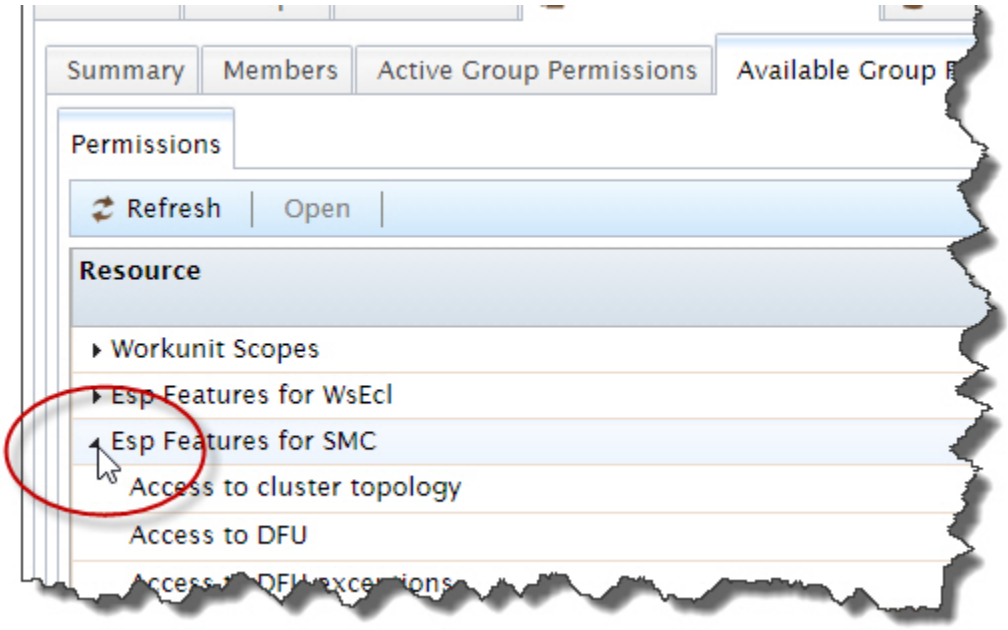
   This opens a new tab for the group.



The group tab displays the sub-tabs: **Summary**, **Members**, **Active Group Permissions** and **Available Group Permissions**.

4. Select the **Available Group Permissions** sub-tab. This displays all the available permission resources.

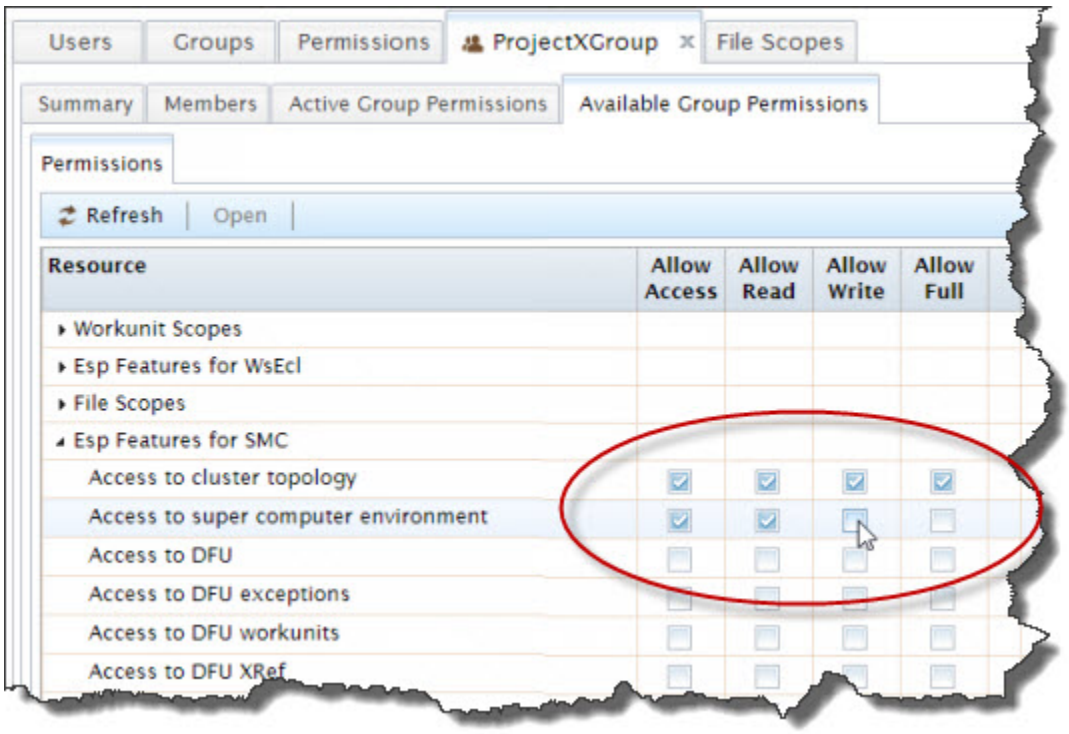
5. Click on the arrow to the left of the **Resource** to expand and expose the permission sets for the resources.



The groups permission resources display.

6. There may be more than one resource setting available in each group, be sure to set the permissions for each setting as required.

7. Check the boxes for **allow** and **deny** as required for the group.



	**NOTE:** Use caution when setting any explicit **deny** permission setting. The most restrictive permission always applies.

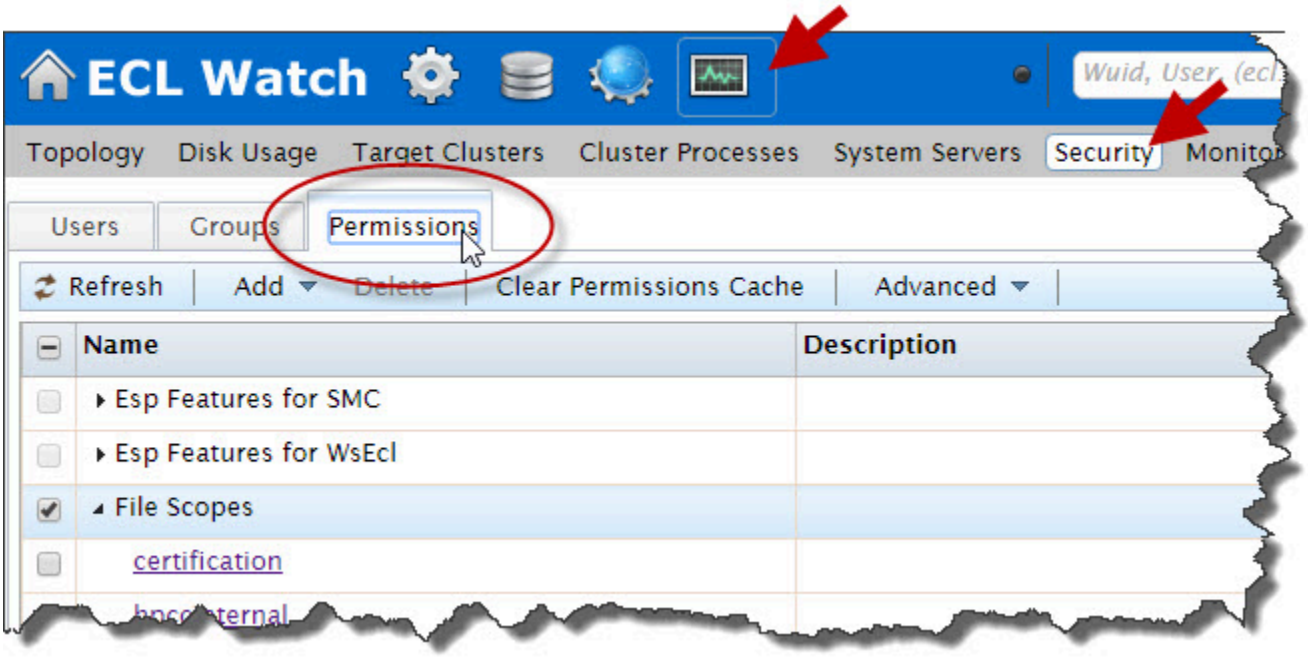
8. There may be more than one resource setting available, select the resource(s) you require from the drop list.

   Repeat for each applicable resource.

9. The changes are automatically saved. Close the tab.

Feature level access control

Access to the feature permissions is available through ECL Watch. In order to modify feature permissions you must have Administrator level access. To access the feature permissions click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

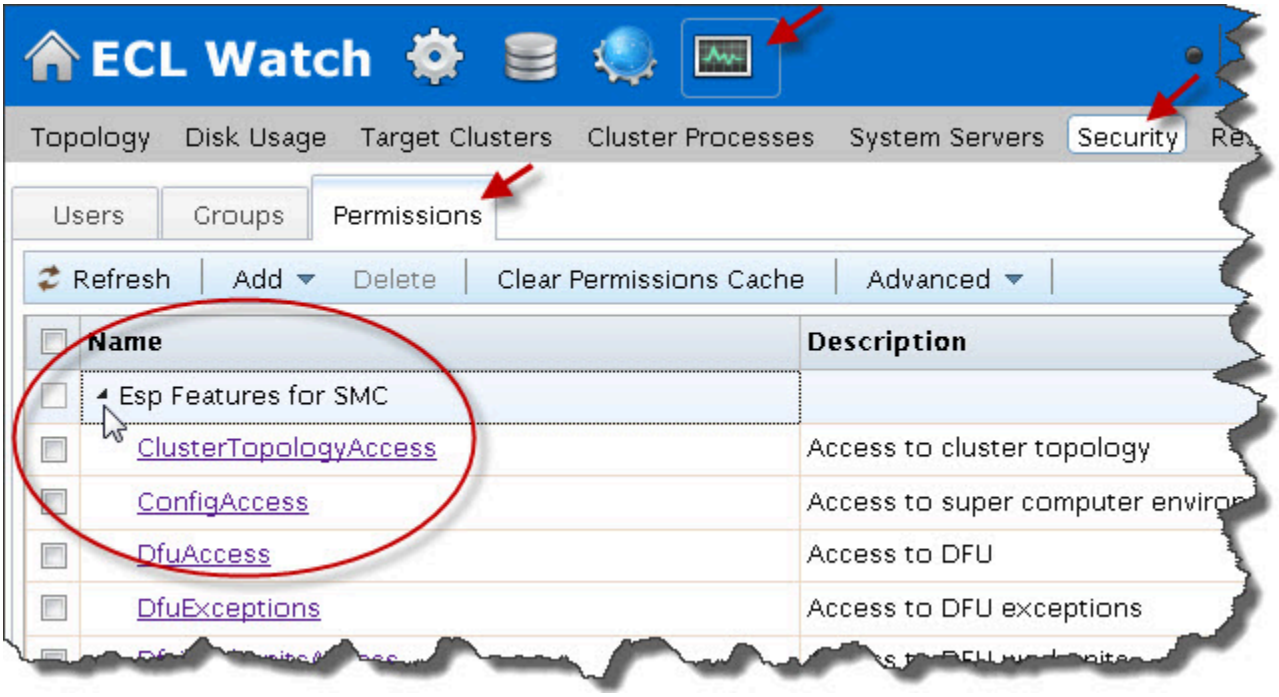


To use the feature level controls, apply the feature resource from the **Available Permissions** tab to the **Active Permissions** for users and groups. Using the feature level controls allow you to:

- View the features and permissions for any resource
- Edit the permissions for any feature
- Update the permissions for users and groups for a specific resource

Feature resources

There are several features for which you can set up access control in HPCC Systems. Access to features of the HPCC Systems platform is controlled by via the **ESP Features for SMC** category.



The available features are listed under the **Permissions** tab. You can view and gain access to the feature controls from here. However, the feature controls must be applied to users, or to groups. If you click on the feature name link, a tab opens that displays the users and groups where those feature permissions are applied.

ECL Watch feature permission settings that are not listed are not relevant and should not be used.

Apply permissions for a feature resource:

To use the feature permissions, you must apply them to a user or group(s). To access the feature permissions click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Identify the user(s) or group(s) which you want to modify the feature permissions.

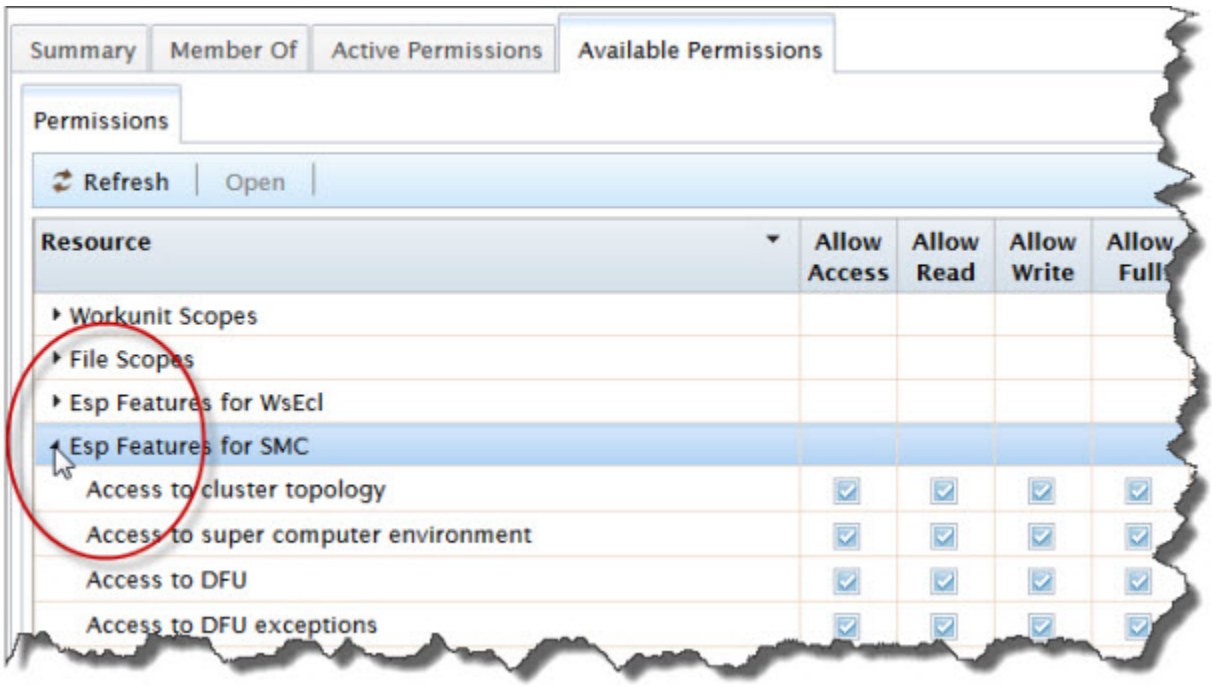
   Select the appropriate tab. (Users or Groups)

2. Check the checkbox(es) next to the user(s) or group(s) to modify.

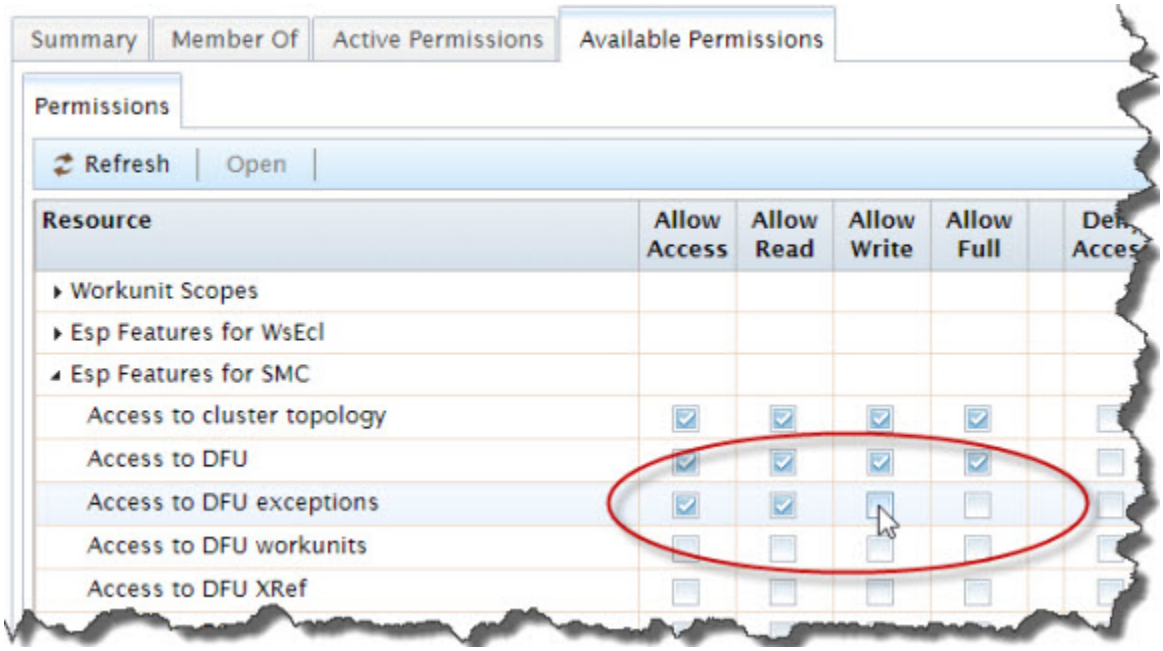
3. Press the **Open** action button. A tab for each user or group selected opens.

4. Click the **Available Permissions** sub-tab.

5. Click on the arrow to the left of the resource to display the features of that resource.



6. Locate the feature resource(s) you want to update.



7. Click the checkbox(es) in the **allow** and **deny** columns as appropriate.

8. The changes are automatically saved. Close the tab(s).

   Note: You must follow this process for each user or group(s) separately.

SMC Feature Permissions

The following table describes the level of access required to be able to use these HPCC Systems ECL Watch features.

Name	Description	Access
ClusterTopologyAccess	Access to Cluster Topology	Read
	Access to log files.	Full
DfuAccess	Access to DFU Logical Files	Read
	Delete Files, add to superfiles, and remove from superfiles	Write
	Erase file history metadata	Full
DfuExceptions	Access to DFU Exceptions	Read
DfuWorkunitsAccess	Access to View DFU Workunits	Read
	Access to Create, Delete, Update, Submit, and Abort DFU Workunits	Write
DfuXrefAccess	Access to DFU XREF	Read
	Clean directory	Write
	Make changes and generate XREF Reports	Full
EclDirectAccess	Access to ECL direct service.	Full
ESDLConfigAccess	ESDL Config Access	Read
	Publish ESDL definition and ESDL binding, configure ESDL binding method.	Write
	Delete ESDL definitions, delete ESDL bindings.	Full
FileDesprayAccess	Allows a user to despray logical files.	Write
FileIOAccess	Access to read files in Drop zone	Read
	Access to write to files in Drop zone	Write
PackageMapAccess	Access to ListPackage, ListPackages, GetPackage, GetPackageMapById, ValidatePackage, GetQueryFileMapping, GetPackageMapSelectOptions, GetPartFromPackageMap	Read
	Access to AddPackage, CopyPackageMap, ActivatePackage, DeActivatePackage, AddPartToPackageMap, RemovePartFromPackageMap	Write
	DeletePackage	Full
FileScopeAccess	Allows access to query, set, modify, and delete File Scope Permissions	Full
FileSprayAccess	Access to Spraying and Copying	Read
	Rename, spray, copy, and replicate files	Write
	Download or delete file on a landing zone	Full
MachineInfoAccess	Access to machine/Preflight Information	Read
MetricsAccess	Access to SNMP Metrics Information (Roxie Metrics)	Read
OthersWorkunitsAccess	Access to View Other User's Workunits	Read

Name	Description	Access
	Access to Modify or Resubmit User's Workunits	Write
	Access to Delete Other User's Workunits	Full
OwnWorkunitsAccess	Access to View Own Workunit	Read
	Access to Create or Modify Own Workunit	Write
	Access to Delete Own Workunits	Full
RoxieControlAccess	Access to Roxie control commands	Read
SmcAccess	Access to ECL Watch (SMC Service)	Read
ThorQueueAccess	Access to Thor Job Queue Control	Full
CodeSignAccess	Access to Code Signing service ListUserIDs	Read
	Sign code	Full
WsELKAccess	Access to ELK integration service	Access
	Read the ELK configuration	Read
WsStoreAccess	Access to WsStore service	Access
	List stores, fetch key-value pairs, listkeys, listnamespaces	Read
	Set key-value pairs	Write
	Delete keys, delete namespaces, fetch keymetadata	Full
WsEclAccess	Access to WS ECL service	Full
WsLogAccess	Allows ability to read component logs	Read
SashaAccess	Access to WsSasha service	Access
	List Workunits	Read
	Archive Workunits, restore archived Workunits	Full

Some Feature Permissions Notes

- SMCAccess is required to be able to successfully login to ECL Watch.
- ThorQueueAccess allows you to manipulate the queue by promoting/demoting queued workunits according to priority.
- ThorQueueAccess also allows you to pause or clear the Thor queue. You can also view Thor usage statistics.
- Depending on the level of access the user has, they can view, modify, and delete their own, or others workunits. This is OwnWorkunitsAccess, and OthersWorkunitsAccess respectively.
- DfuWorkunitsAccess permissions allow users to view and/or manipulate DFU Workunits.
- Users need permission to see files on the dropzone and also to put files there. They need further permissions to be able to spray and copy files from the dropzone to their cluster and also to despray files from the cluster back to the dropzone.
- The WsStore service uses **namespaces** (similar to a database in a DBMS system), **stores** (similar to tables in a database), and **key-value pairs** (similar to fields).

DFU Xref

XREF is used for monitoring files on the cluster(s). Reports generated show where housekeeping is required on the cluster(s) and users require additional permission to use this feature.

	On a large system, we suggest limiting the number of users who can Generate XREF reports by setting DfuXrefAccess access to FULL for only those users.

Users/Permissions

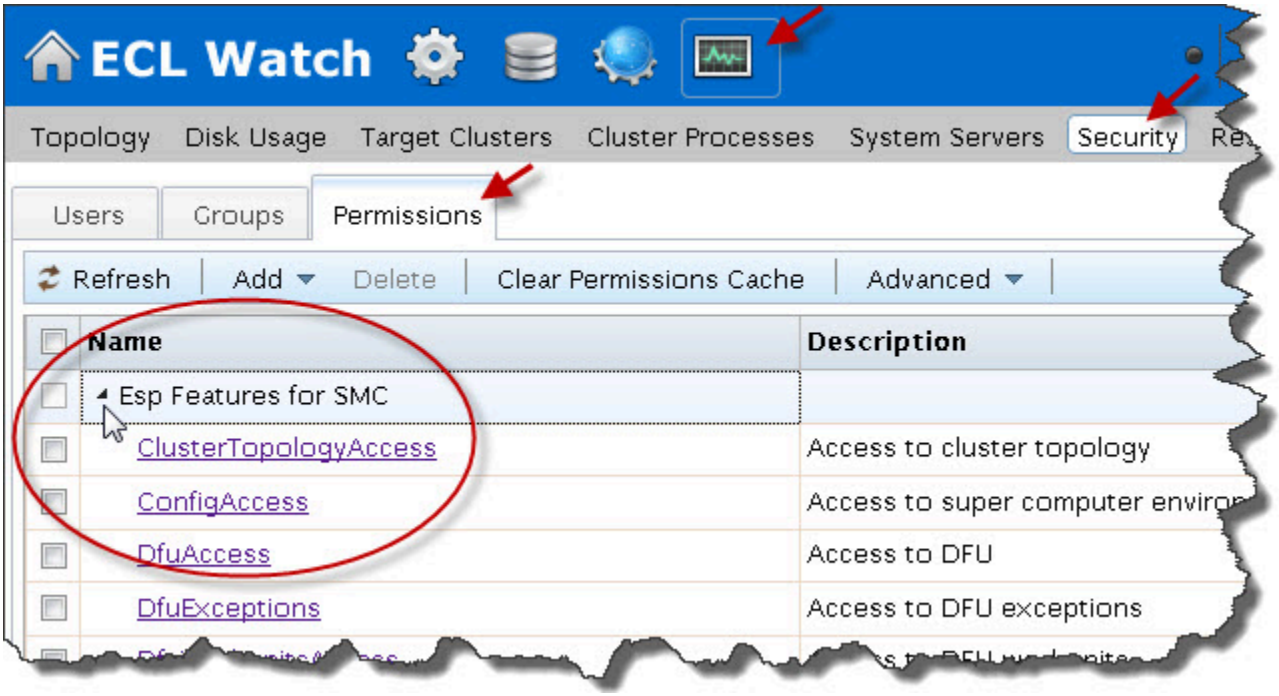
To be able to view the **Users/Permissions** area in ECL Watch, a user must be a member of the Administrators (or similarly named) group with the appropriate permissions on the LDAP or Active Directory server.

File Access Control

The HPCC Systems LDAP **Dali Server** technology provides the ability to set secure access permissions to data file folders (or file scopes). This is controlled by the use of file scope resources.

An OU called **Files** is automatically created when the Dali server starts. To secure data folders, create a file scope for that folder and apply rights to each scope.

Figure 10. File Scopes Permissions



For example, below **Files** there is a unit (OU) representing the cluster, such as **thor** (or the name that you set up for your cluster). Furthering the example, below that could be a unit named **collectionx** which contains two units, **publicdata** and **securedata.** The **publicdata** folder has rights granted to a large group of users and the **securedata** folder has limited access granted. This allows you to prevent unauthorized users from any access to files in the **securedata** folder.

The structure described above corresponds to this logical structure:

collectionx::securedata

Which corresponds to this physical structure:

/var/lib/HPCCSystems/hpcc-data/thor/collectionx/securedata

All HPCC Systems components and tools respect LDAP file access security. The following exceptions are assumed to be system level or for administrative users:

- Network file access using UNCs, Terminal Services, or SSH.
- Administrative utilities

Attempting to access a file in a folder for which access is not granted will result in one of the following errors:

```
DFS Exception: 4 Create access denied for scope <filepath>
```

or

```
DFS Exception: 3 Lookup access denied for scope <filepath>
```

(where <filepath> is the full logical file scope path)

Creating File Scopes

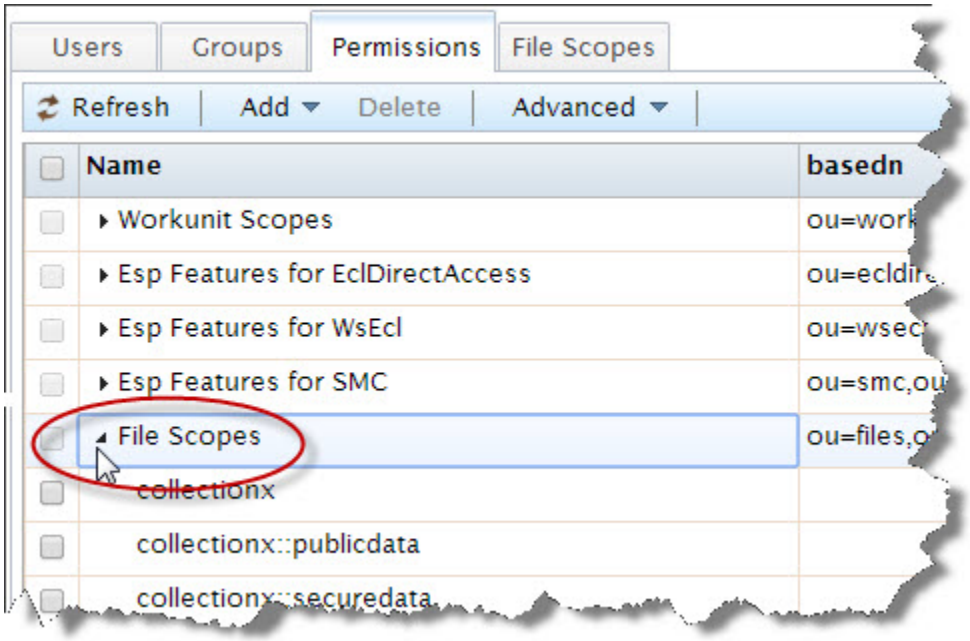
To apply permissions to a file scope, you must first create the file scope(s).

To create file scope(s) click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click the **Permissions** tab.

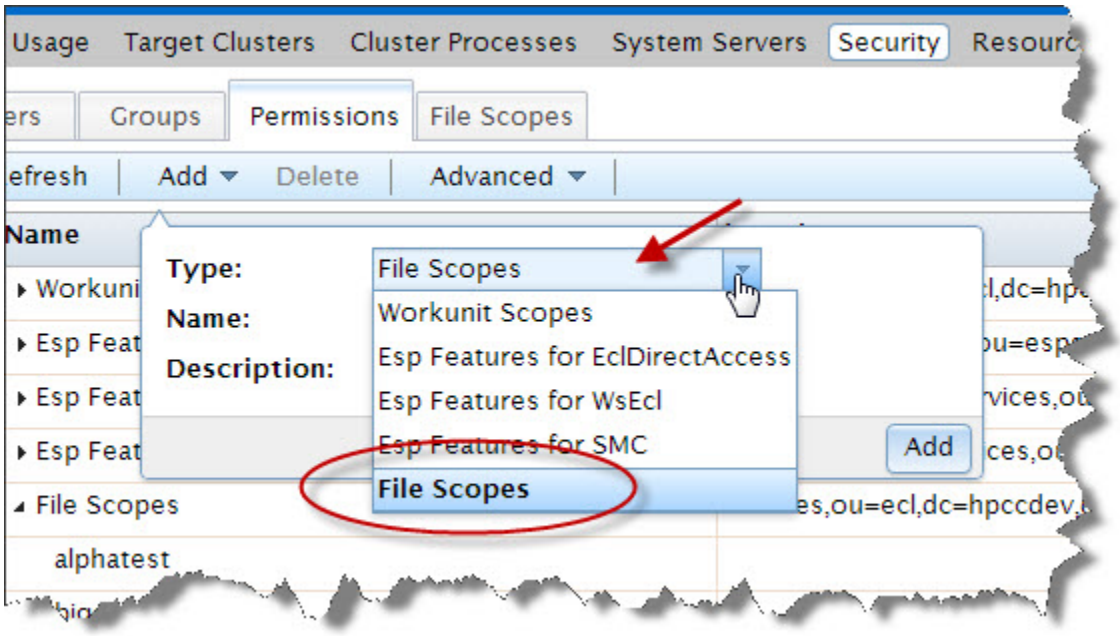
   The feature resources display.

2. Click on the arrow to the left of the **File Scopes** resource to display the file scopes.

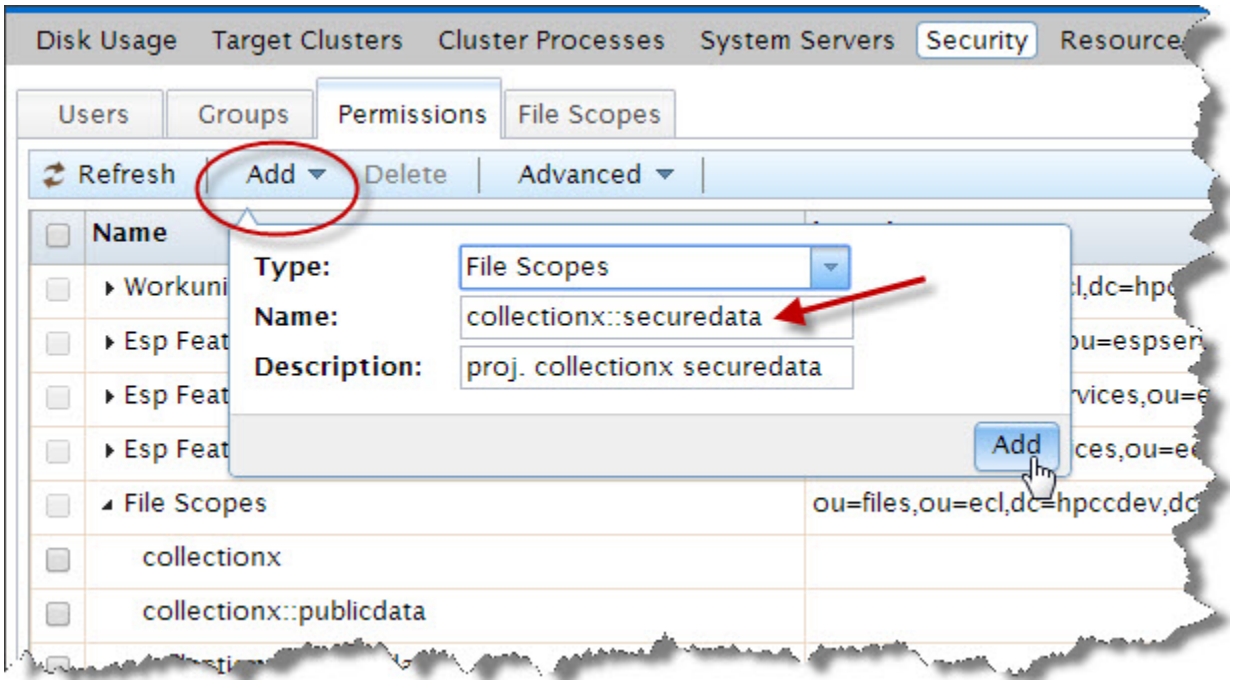


3. Press the **Add** button.

4. Choose **File Scopes** from the drop list.



5. Enter the exact name of the scope you want to add in the **Name** field.



Enter a short description in the **Description field.**

6. Press the **Add** button.

The new scope displays in the list.

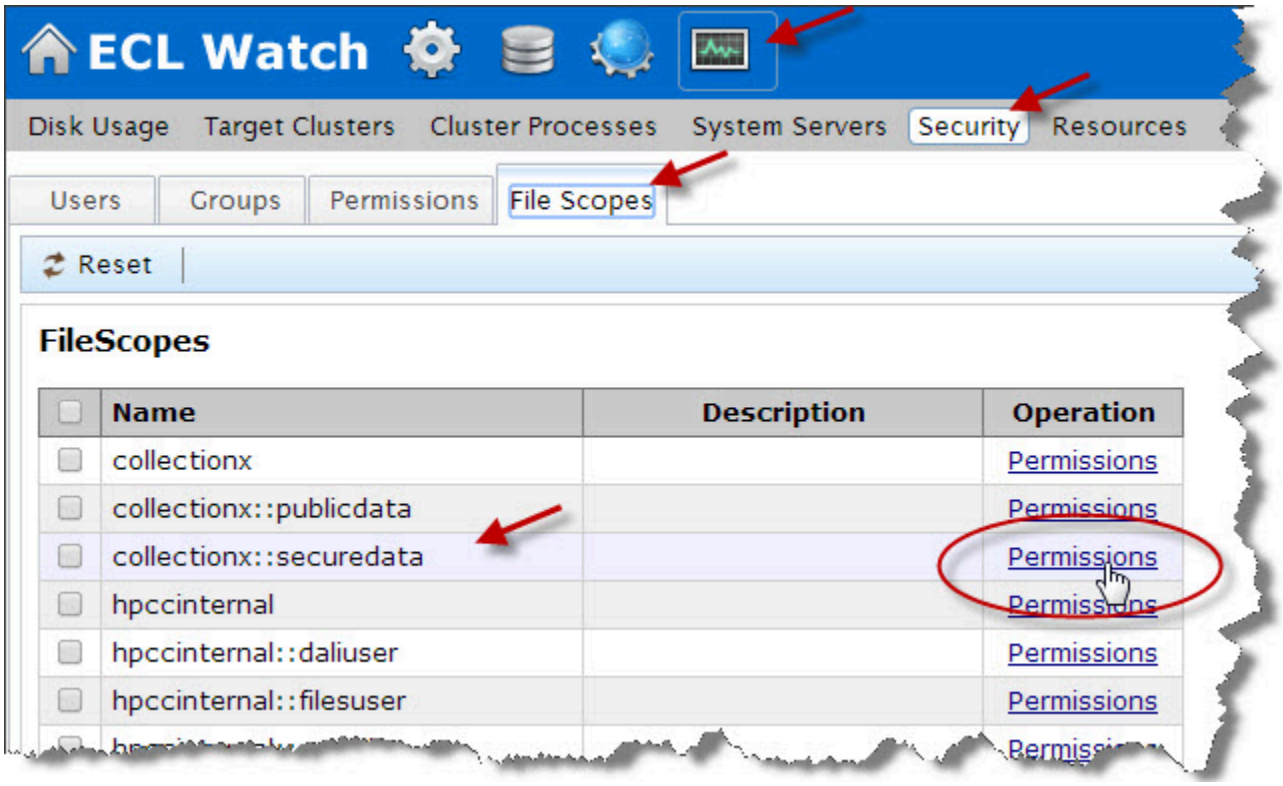
Setting permissions for file scopes

You must apply permissions for file scopes to users or group(s). If you want to apply the scope to a new group, create the group(s) as required.

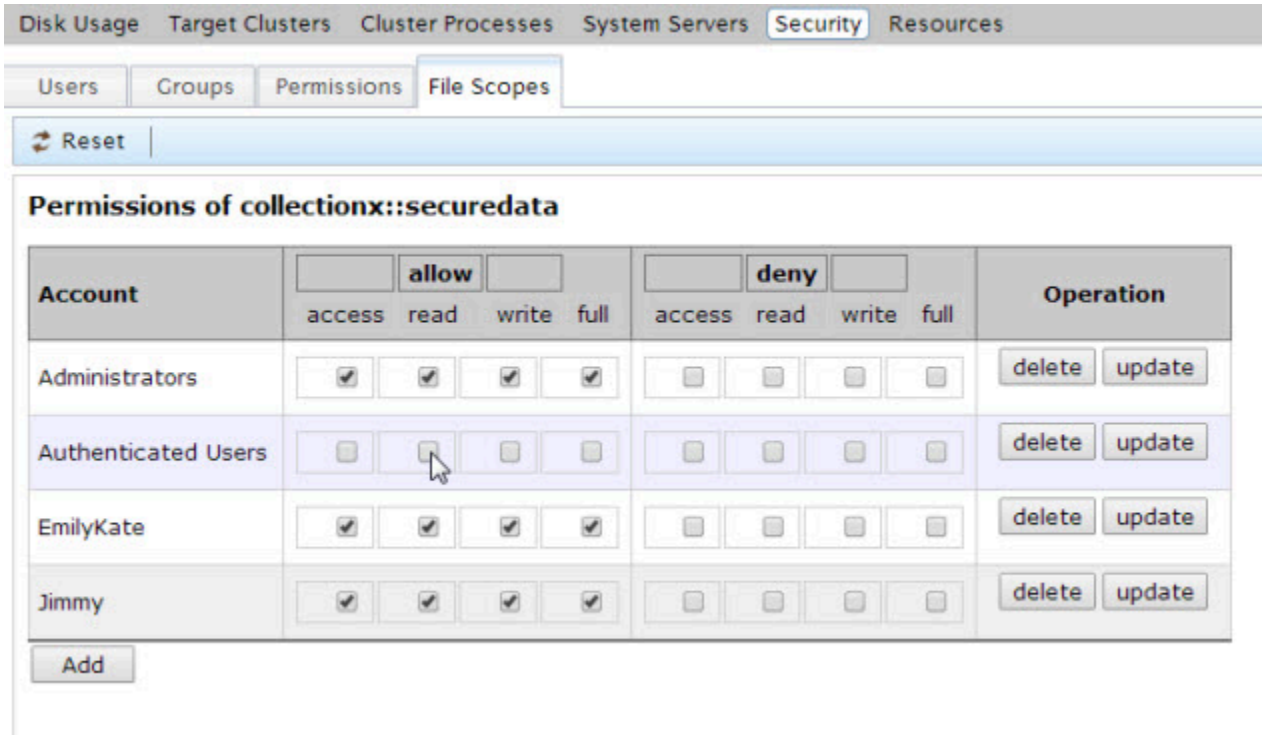
To set the file scope permissions click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Select the **File Scopes** tab.

2. Choose the scope to modify. Click the **Permissions** link for that scope.



3. The permissions defined for users and groups for that scope display.

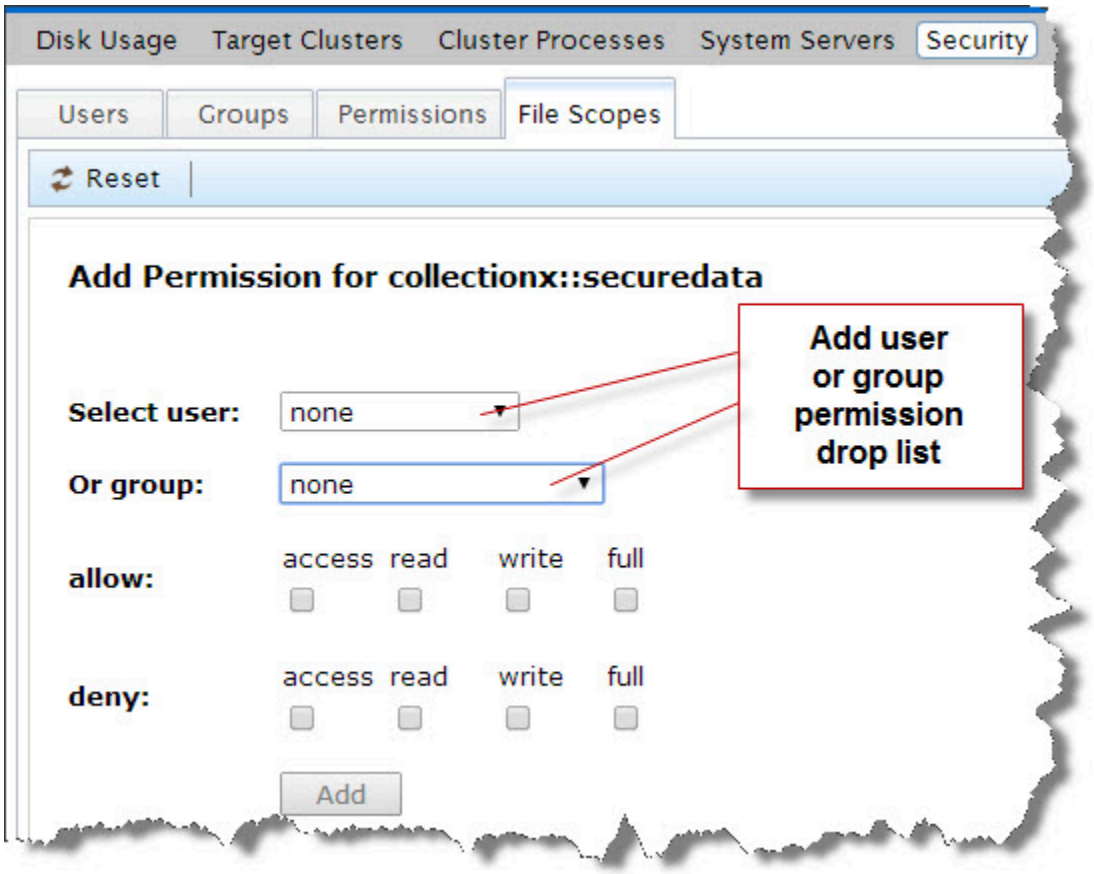


4. Check (or clear) the checkbox(es) in the **allow** and **deny** columns as appropriate for the users or groups displayed.

5. To add users or groups to the scope, press the **Add** button.

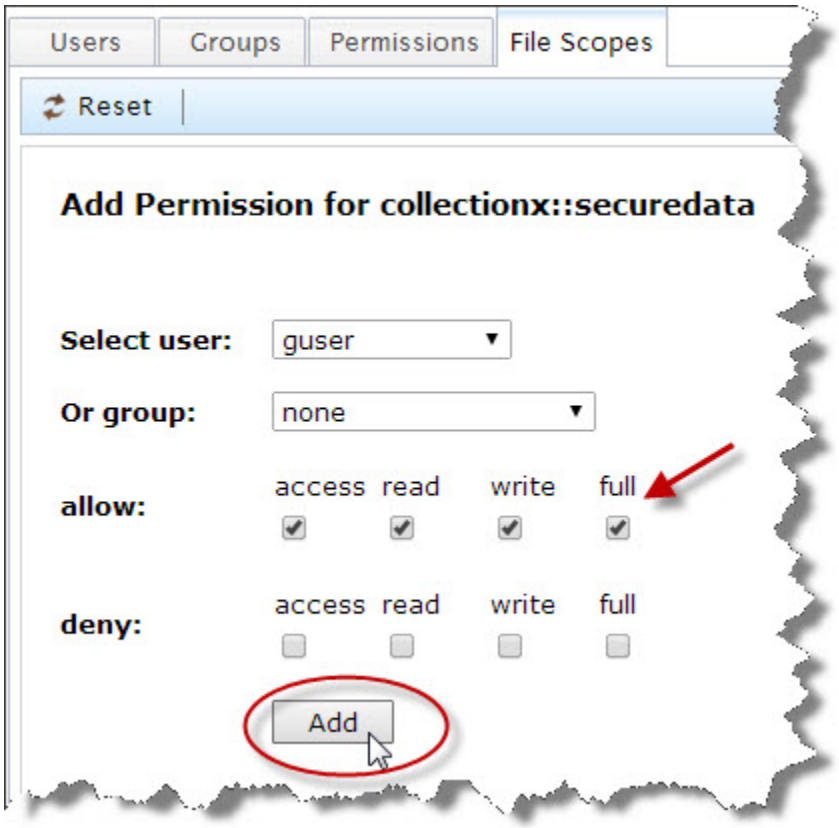
   The Add Permission dialog displays.

6. Select the user or the group to add from the drop list(s).



Once a user or group is selected, the Add button and the allow and deny checkboxes are active

7. Check the boxes for allow and deny as appropriate to set the permissions for this scope.



8. Press the **Add** button.

9. The changes are automatically saved. Close the tab(s).

File scope features

Below the List of File Scopes, there are buttons that allow you to:

- Reset **Default Permissions** to selected file(s)

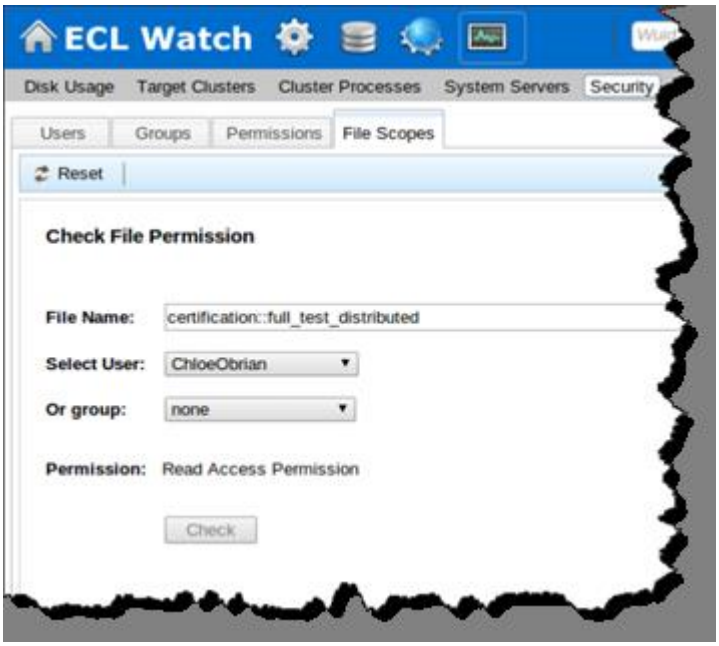
  This allows you to quickly remove any added permission settings for a file and reset to the default access.

- Allow or Deny Access to physical files on Landing Zone

  This provides a way to grant or deny access to the top level file scope. By default, only administrators have access to this scope.

- Check File Permissions for a user or group

  This provides a way to check a user or group's access to a logical file.



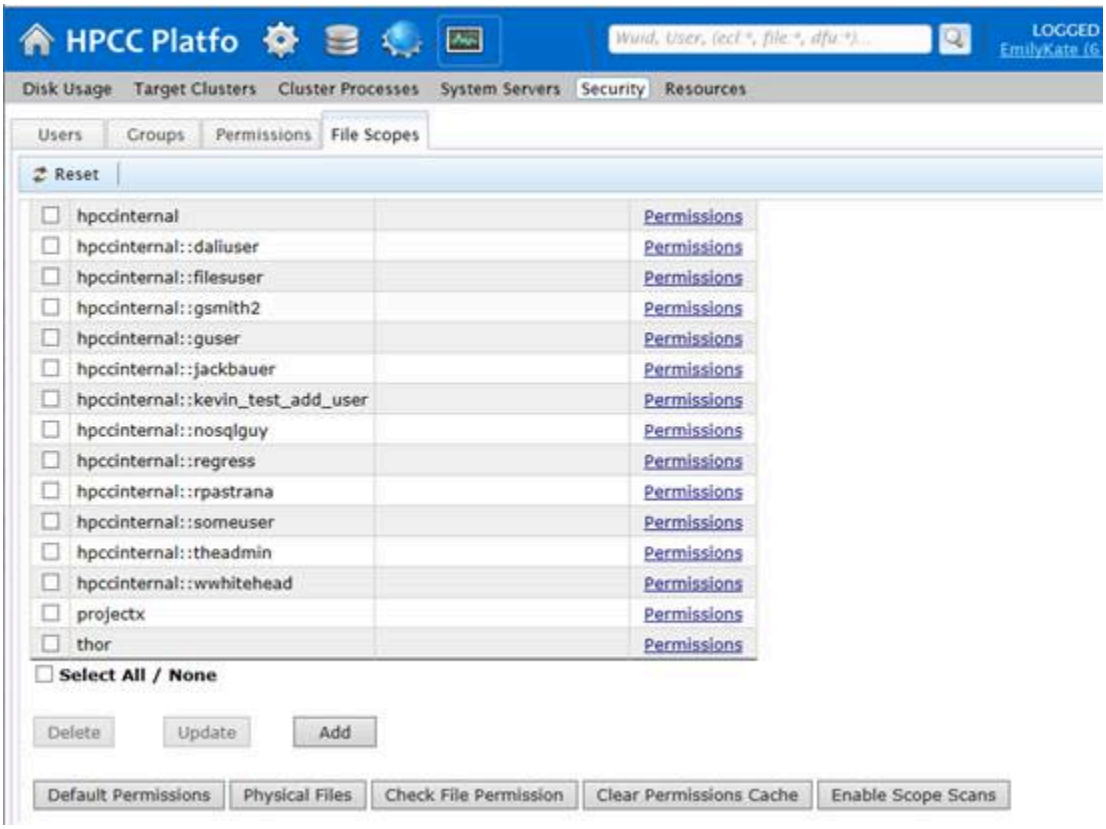
- Clear the Permissions Cache

  This clears the permissions cache and allowing any new permission settings to take effect immediately.

- Enable/Disable Scope Scans

  This provides a means to enable or disable Scope scans. Enable scope scans to check permissions for users to access scopes. This will impact performance. Disable scope scans ignores any scope permissions and removes all access control, but improves performance. Disabling access control is not recommended.

  Changing this setting through ECL Watch, as described here, is only a temporary override. When Dali restarts this setting will revert to what is defined in the configuration environment.xml.



Landing Zone Security

You can set additional security options on Landing Zone(s). Feature level security allows you to set permissions on access to your Landing Zone and what users or groups can do there. Landing Zone Scope Security allows you to set permissions on sub-folders in a Landing Zone. This provides a means to grant and deny users permission to areas within a Landing Zone.

Landing Zone Feature Authorization

This lists the HPCC Systems Landing Zone using Feature Level Authorization:

List/search Dropzone files	FileSprayAccess - SecAccess_Read
Spray a file from a Dropzone	FileSprayAccess - SecAccess_Write
Despray a file to a Dropzone	FileDesprayAccess - SecAccess_Write
Read the content of a Dropzone file	FileIOAccess - SecAccess_Read
Write the content of a Dropzone file	FileIOAccess - SecAccess_Write
Upload a file to a Dropzone using ECLWatch:	FileUploadAccess - SecAccess_Full
Download a file from a Dropzone using ECLWatch	FileSprayAccess - SecAccess_Full

To enable access to a feature, set the permission accordingly.

This may be sufficient level security in some cases, however, additional restrictions may be needed to secure certain files, from certain users or groups. You can use Landing Zone File Scope security to accomplish this. .

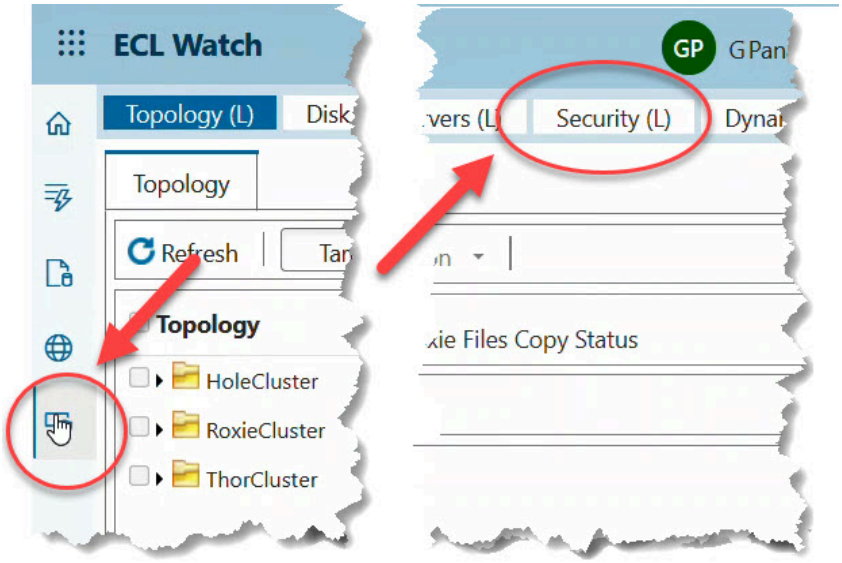
Landing Zone File Scopes

File Scope Level Authorization provides a means to secure access to folders within a Landing Zone.

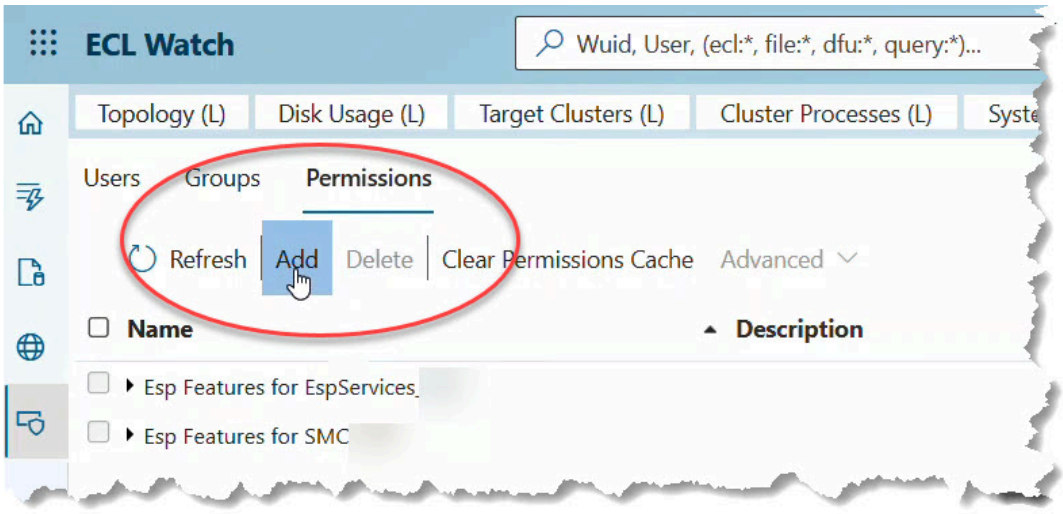
An HPCC Administrator can define the Landing Zone scopes for each folder in an HPCC Landing Zone.

Each scope is a file folder of an HPCC Landing Zone. Each Landing Zone scope is one HPCC file scope.

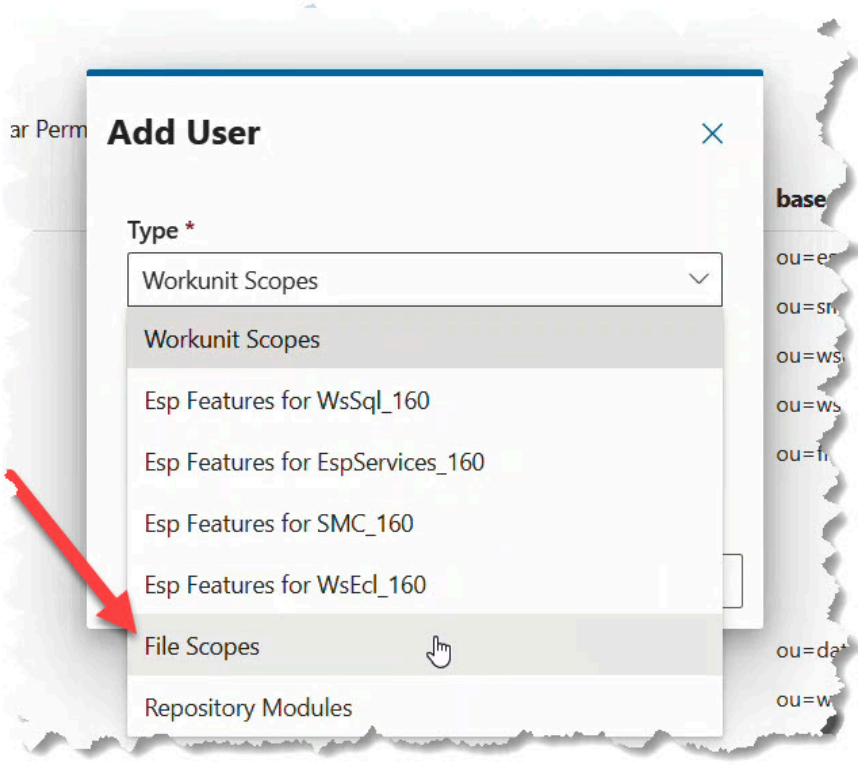
The Landing Zone file scopes can be defined using ECLWatch for security enabled systems.



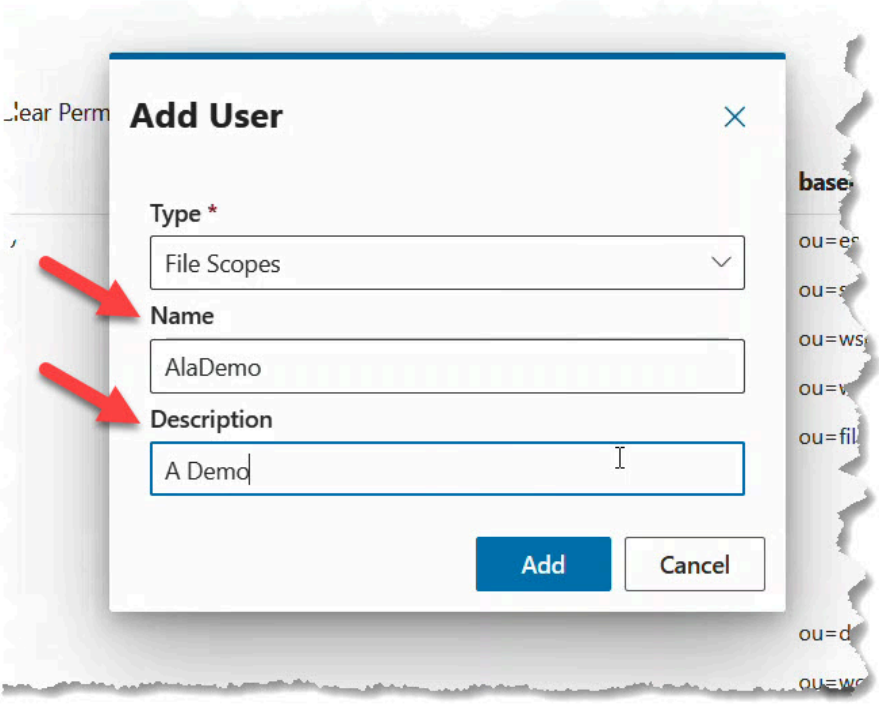
To create a new Landing Zone scope, go to the Security page of ECL Watch, and click on Permissions.



On the Permissions tab press the Add button.



Choose File Scopes on the drop down option box, then provide a name and optionally a description.



Landing Zone File Permissions

You can set the Landing Zone file permissions according to your requirements. Access your new Landing Zone using the following annotation:

```
plane::{dropzone_name}::{folder_name}::{subfolder_name}::{subfolder_name}...
```

Your HPCC Administrator can define access rights to each Landing Zone scope for each HPCC user or user group.

Workunit Access Control

There are 2 aspects of workunit (WU) security:

- Feature Authentication for workunits allows you to set permissions to control whether users can view their own WUs and/or other users' WUs.
- Workunit Scope security provides the ability to set permissions for individual WU scopes. All new workunits have a scope value.

Both methods are valid to use (either separately or together), and the strictest restriction always applys.

In other words, if someone is granted permission to see WUs in the scope *johndoe* but is denied permission to see other users' WUs in the Feature Authentication permissions, this user would be denied access to see the WUs in the *johndoe* scope.

Conversely, if the user is allowed access to see other people's WUs but is denied access to the *johndoe* WU scope, this user will be able to see other WUs in that scope.

Note: If you do not have access to a WU, you will never be able to view it or even know of its existence.

By default, a submitted WU has a scope of the user's ID. For example, a WU JohnDoe submits has *scope=johndoe* in the WU. This value in a WU allows ESP and its services to use LDAP to check for permissions and enforce those permissions.

You can override the default scope using ECL Code:

```
#workunit('scope','MyScopeValue');
```

Securing workunit scopes

ESP (on startup) automatically creates an LDAP OU called **Workunits** (unless it already exists). If this OU is automatically created, the OU is made with full permissions granted to all authenticated users. All WU scopes are below the *workunits* OU either implicitly or explicitly.

If a specific scope OU does not exist in LDAP (e.g., the scope johndoe used in earlier example), then the parent OU's permissions are used. In other words, the scope of *johndoe* is implicitly under the *workunits* OU even though it might not be explicitly listed in the LDAP structure and therefore it would use the permissions granted for the parent, *workunits* .

Workunits feature permissions

Using the **Workunit Scopes** feature in the **Permissions** area of ECL Watch the permissions for any scope can be reset to the default permissions settings for your system. Permission settings for Workunit Scopes may be set as follows:

Description	Access
View WUs in that scope	Read
Create/modify a WU in that scope	Write
Delete a WU in that scope	Full

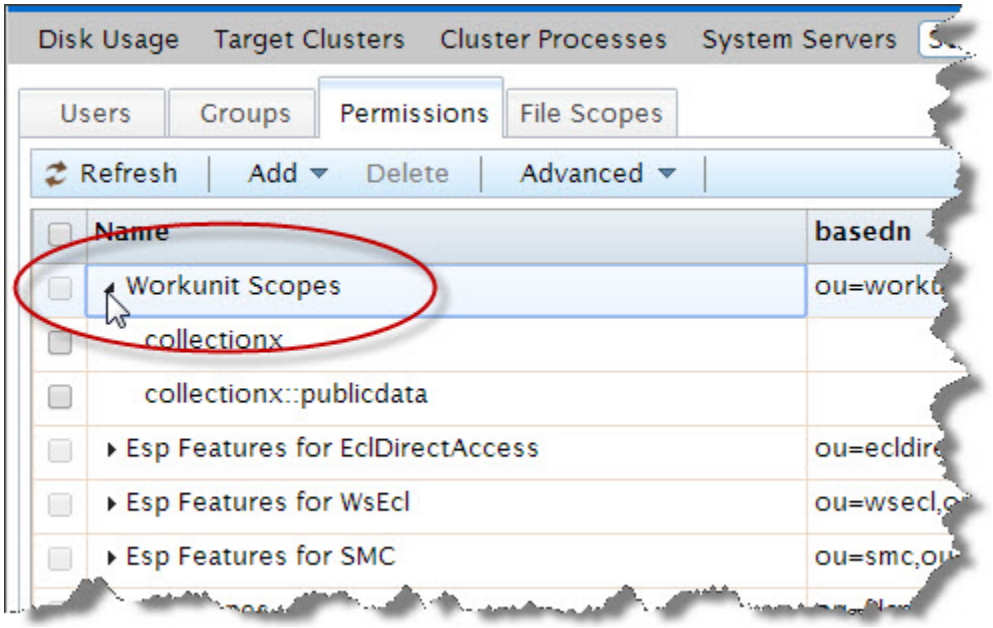
Adding workunit scopes

To add workunit scope permissions click on the **Operations** icon, then click the **Security** link from the navigation sub-menu.

1. Click the **Permissions** tab.

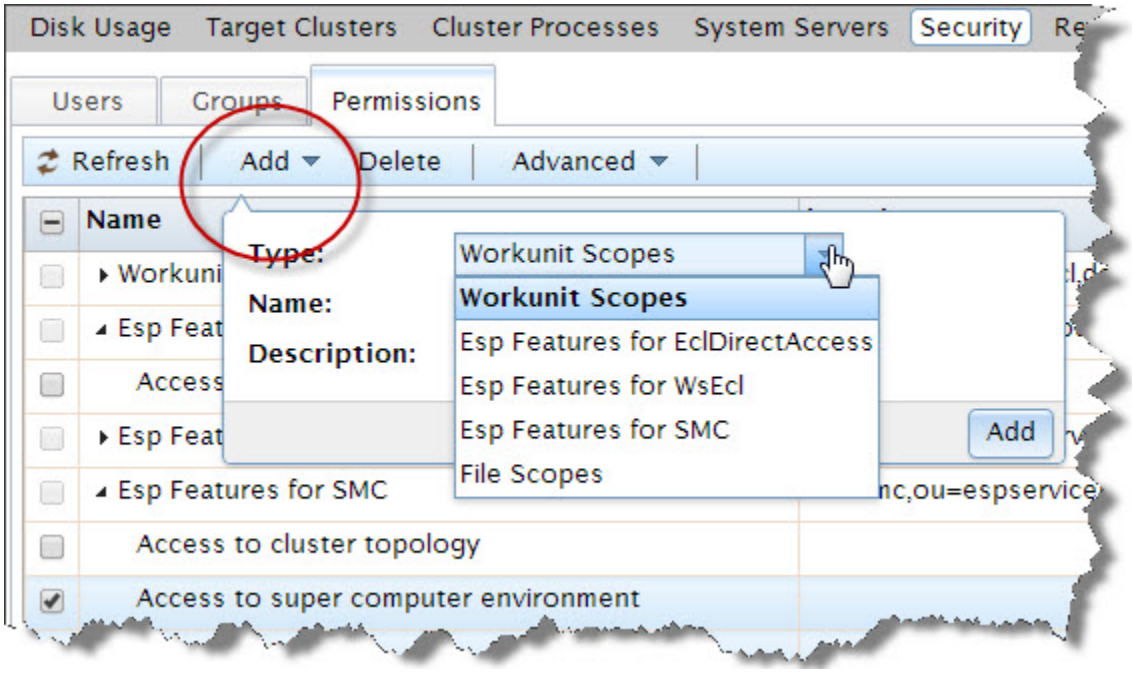
   The feature resources display.

2. Click on the arrow to the left of the **Workunit Scopes** resource to display the file scopes.

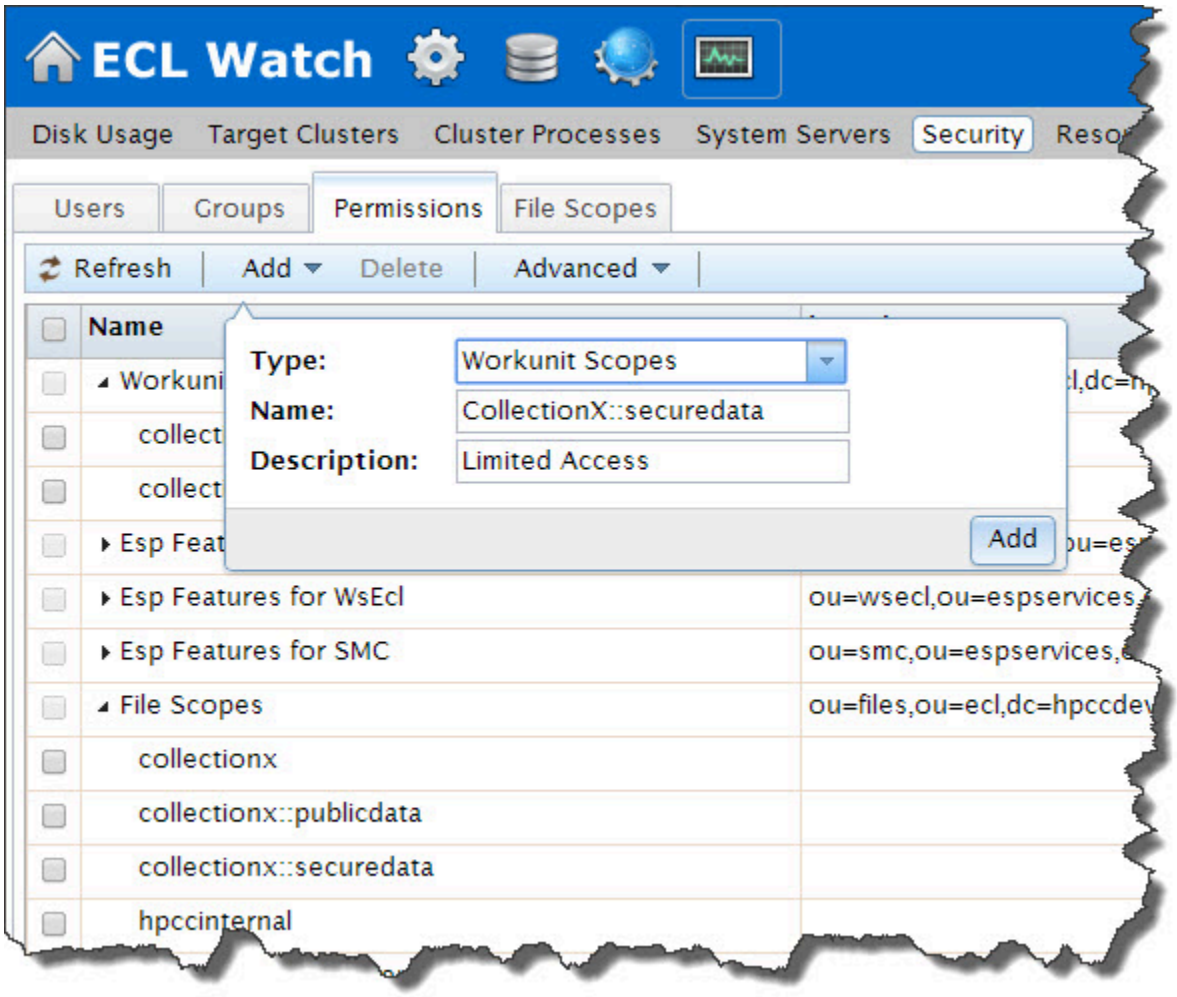


3. Press the **Add** button.

4. Choose **Workunit Scopes** from the drop list.



5. Enter the exact name of the scope you want to add in the **Name** field.



Enter a short description in the **Description field.**

6. Press the **Add** button.

   The new scope displays in the list.

Set permissions to the scope.

You apply the workunit scopes to a group. If you want to apply the scope to a new group, create the group(s) as required.

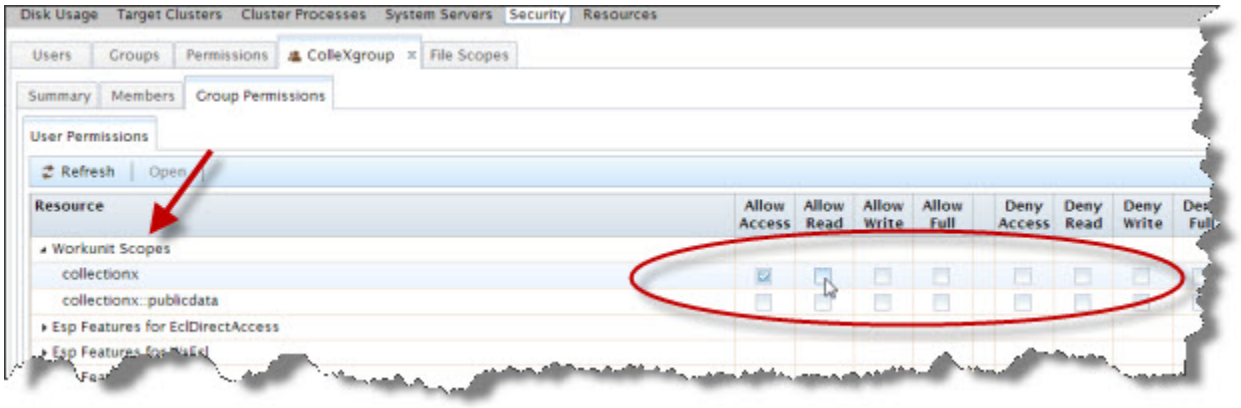
1. Go to the **Groups** tab.

2. Select a group to apply the scope to by checking the box next to the group name.

   Press the **Open** action button. You can select multiple groups, a tab opens for each group.

3. Select the **Group Permissions** tab of that group. (if multiple groups selected, you must repeat for each group)

4. Click on the arrow to the left of the Workunit Scopes to display the available scopes.



The Workunit scopes display. Check the boxes as appropriate to set the permissions for this scope.

5. To set permissions in this scope for another group, open and go to that groups tab.
6. To set permissions in this scope for a user, select the tab.
7. Select the user and press the Edit action button.

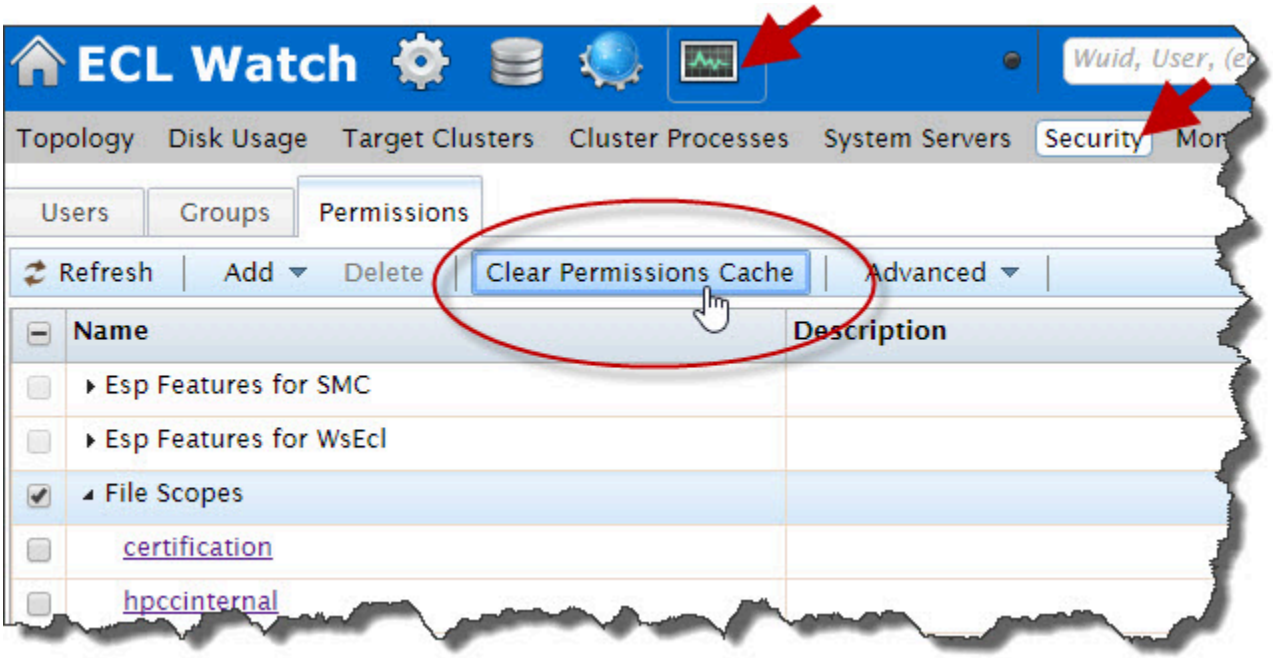
   A new tab for that user opens.
8. On that tab, click on the **User Permissions** sub-tab.
9. Locate the new scope listed under the appropriate Resource.

   Set the access permissions as appropriate for that user.
10. The changes are automatically saved. Close the tab(s).

Permission Caching

A helpful feature found on the Permissions tab is the *Clear Permissions Cache* button. The *Clear Permissions Cache* button clears the cached permissions from Dali and ESP.

When you change a permission in ECL Watch, the settings are cached in the ESP server and stored in the Dali server. The information in the cache is updated at a configurable interval. This value can be set in the Configuration Manager under the *LDAP Server settings Attributes* tab. The default cacheTimeout is 5 minutes.

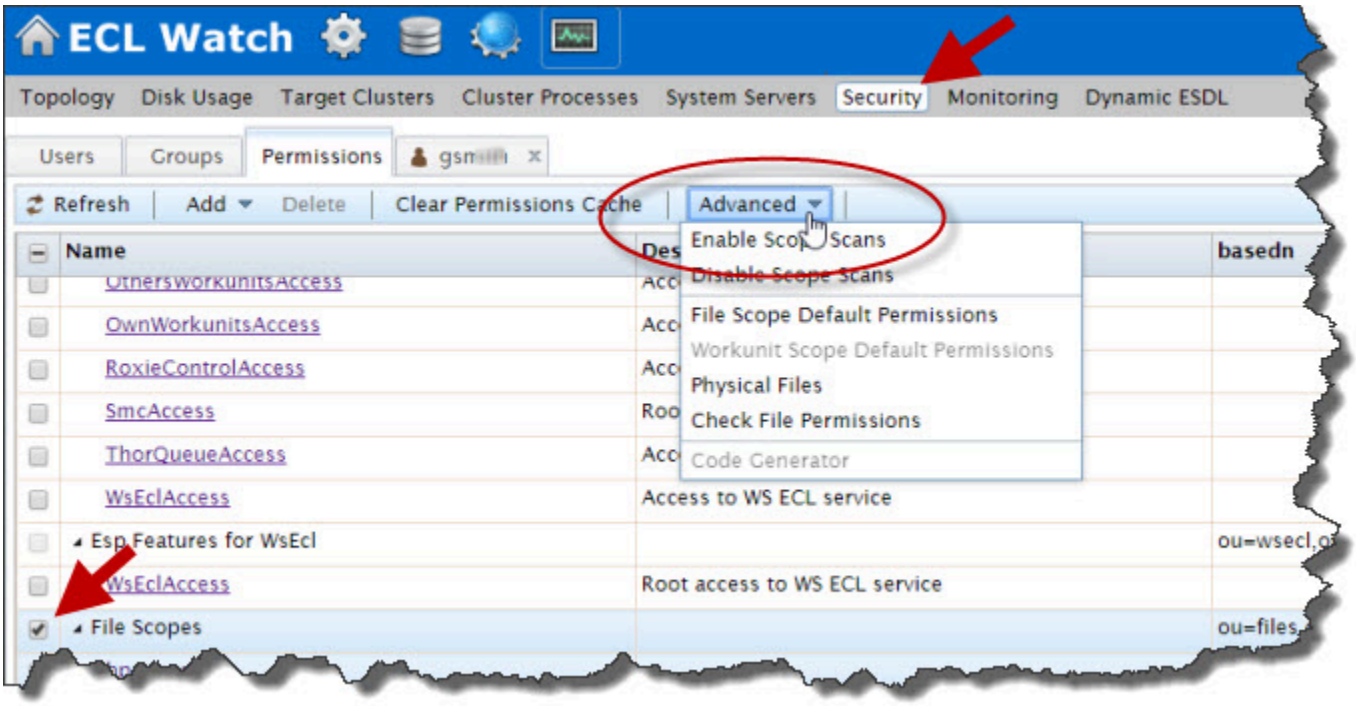


The Permissions Cache can be cleared from anywhere on the permissions tab in ECL Watch.

When you want a permission change to take effect immediately, you can clear the cache and force Dali to update the permission settings by pressing the **Clear Permissions Cache** button. This action transfers the settings when you press the button. Use this feature judiciously as overall system performance is affected temporarily while the LDAP settings in the Dali System Data Store repopulate.

Advanced Permissions

On the Permissions tab is the **Advanced** (Permissions) button. The Advanced menu/button provides access to manage file and workunit scope security. The Advanced button is only enabled when you select either File or Workunit Scopes on the Permissions tab.

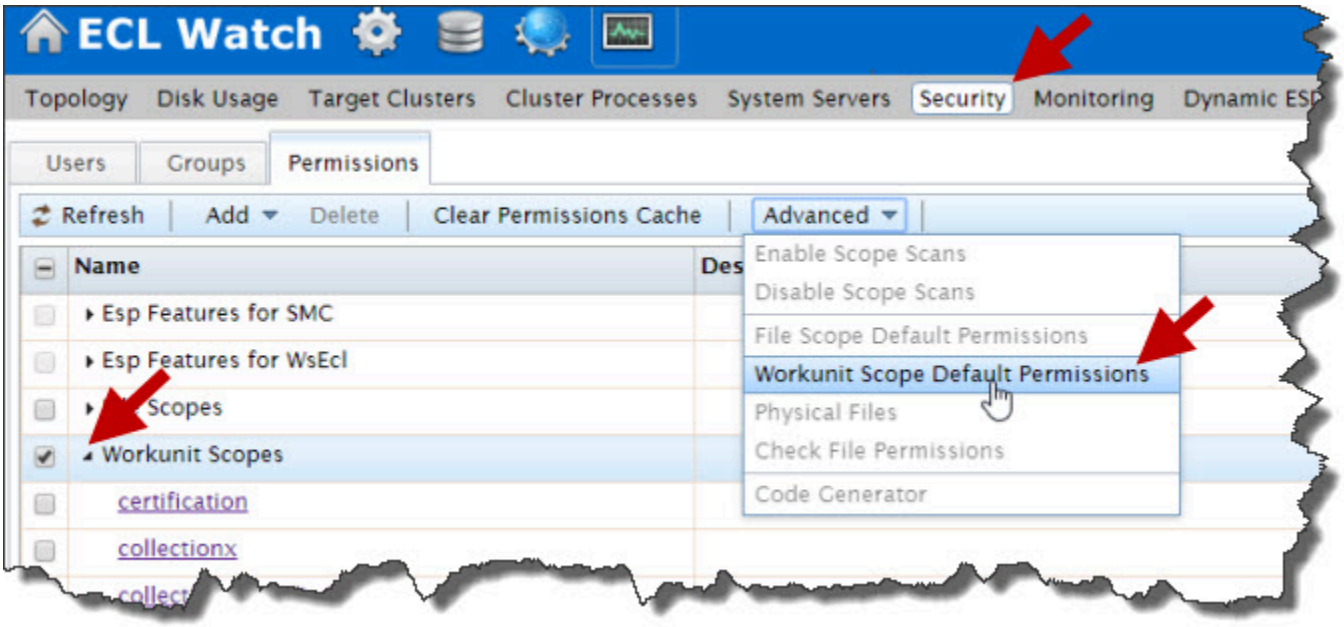


Press the Advanced button to display the Advanced permissions menu. The Advanced menu is context aware, so if you select File Scopes from the Permissions tab, then you can only choose to apply the relevant file scope permissions, likewise if you selected workunits scopes.

File Scans

Using the Advanced Menu with File Scopes selected:

- Enable or disable file scope security
- Access the file scope default permission page
- Access the Physical Files permission page. The Physical Files settings specify the default permissions for files that do not have a scope explicitly specified.
- Check the file permissions - This option opens a dialog where you can input a File name and select Users and Groups for the File security scope.



Workunit scans

Using the Advanced Menu with the Workunit Scopes selected opens only the Default Permissions tab for the Workunit Scope (Default) Permissions.

NOTE: File or Workunit Scope security needs to be enabled in your system configuration in order to use File or Workunit Scope security on your system.

Configuring ESP Server to use HTTPS (SSL)

The HPCC Systems Enterprise Services Platform server (ESP) supports Secure Sockets Layer (SSL), a protocol used to send and receive private data or documents.

SSL works by using a private key to encrypt and decrypt data transferred over the SSL connection. By convention, URLs using an SSL connection start with HTTPS instead of HTTP.

The SSL option in the ESP Server allows secure and encrypted communication between a browser or SOAP client application and the HPCC Systems platform.

SSL capabilities are configured in the Configuration Manager, but require a certificate be installed on the ESP server. The OpenSSL libraries provide a means to create the necessary certificate files in one of two ways.

- You can use the OpenSSL libraries to create a private key and a Certificate Signing Request (CSR) to purchase a certificate from a Certificate Issuing Authority (such as, VeriSign).
- You can use that CSR to generate your own self-signed certificate and then install the certificate and private key to your ESP Server.

In either case, once installed and configured, the network traffic is encrypted and secure. The Public and Private Keys use 2048-bit RSA encryption.

These server keys are read at runtime by the ESP process. It is important the installed keys have correct ownership and permissions. Typically, it is the HPCC user and their public key (certificate.cer) with read permissions such as 0444 (or 0644), along with the private key (privatekey.cer) with more restrictive permissions of 0400 (or 0600).

Generate an RSA Private Key

Use the OpenSSL toolkit to generate an RSA Private Key and a Certificate Signing Request (CSR). This can also be the basis for a self-signed certificate. Self-signed certificates are useful for internal use or testing.

The following example, creates a 2048-bit RSA Private Key which is encrypted using Triple-DES encryption and stored in Privacy Enhanced Mail (PEM) format.

```
openssl genrsa -des3 -out server.key 2048
```

When prompted, provide a passphrase. This is used as the basis for the encryption.

Remember this passphrase as you will need to enter it into the Configuration Manager later.

Generate a CSR (Certificate Signing Request)

After you have a private key, you can use it to create a Certificate Signing Request (CSR). You can use your CSR to request a signed certificate from a Certificate Authority (such as Verisign or Network Solutions). You can also use the CSR to create a self-signed certificate.

```
openssl req -new -key server.key -out server.csr
```

Answer the questions when prompted:

Country Name (2 letter code):	
State or Province Name (full name):	
Locality Name (eg, city) :	
Organization Name (eg, company) :	
Organizational Unit Name (eg, section) :	
Common Name (e.g., server's hostname):	
Email Address :	
A challenge password (optional):	
An optional company name (optional):	

Generate a Self-Signed Certificate

To generate a temporary certificate, which is good for up to 365 days, issue the following command:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

When prompted, enter the passphrase you used earlier when creating your CSR.

Installing the Private Key and Certificate to your ESP Server

You must install the certificate and private key on **all** ESP server node(s) that will host a service binding using SSL. Copy the keys and certificates to the correct locations and set the appropriate ownership and permissions

Your Private Key and certificate must be copied to /var/lib/HPCCSystems/myesp/ as illustrated in the following example.

1. Copy the certificate (crt) file to the required location on the ESP server(s) :

   ```
   sudo cp server.crt /var/lib/HPCCSystems/myesp/server.crt
   ```

2. Change the owner of the file to be HPCC:

   ```
   sudo chown hpcc:hpcc /var/lib/HPCCSystems/myesp/server.crt
   ```

3. Set the file permissions:

   ```
   sudo chmod 644 /var/lib/HPCCSystems/myesp/server.crt
   ```

4. Copy the private key to the ESP server(s):

   ```
   sudo cp server.key /var/lib/HPCCSystems/myesp/private.key
   ```

5. Change the owner of the file to be HPCC:

```
sudo chown hpcc:hpcc /var/lib/HPCCSystems/myesp/private.key
```

6. Set the file permissions:

```
sudo chmod 600 /var/lib/HPCCSystems/myesp/private.key
```

Configure HTTPS on your ESP Server

Start Configuration Manager in Advanced Mode

1. Start the Configuration Manager Service on one node (usually the first node is considered the head node and is used for this task, but this is up to you).

```
sudo /opt/HPCCSystems/sbin/configmgr
```

2. Using a Web browser, go to the Configuration Manager's interface.

   Use the url of http://nnn.nnn.nnn.nnn:pppp, where nnn.nnn.nnn.nnn is the IP address of the node running Configuration Manager and pppp is the port (default is 8015).

   The Configuration Manager startup wizard displays.

3. Select **Advanced View**.

4. Select an XML file from the drop list.

   This list is populated from versions of an environment XML file in your server's **/etc/HPCCSystems/source/** directory.

   Tip: The XML file that matches the active environment.xml is highlighted.

5. Press the **Next** button.

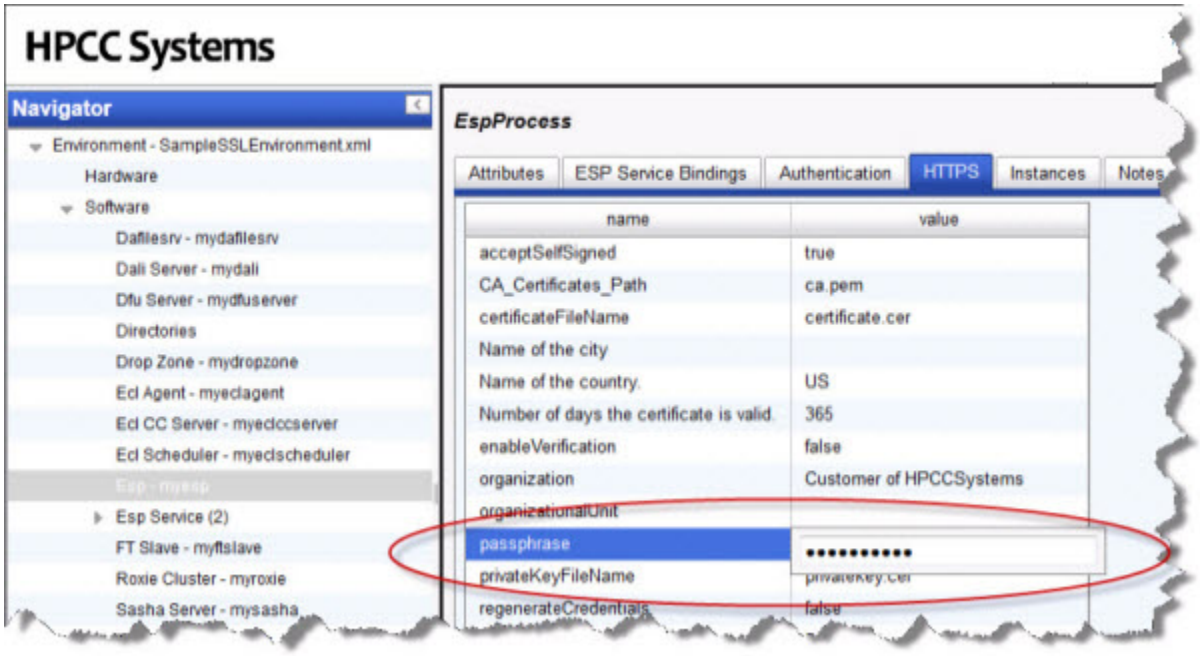
   The Configuration Manager Advanced View interface displays.

6. Check the **Write Access** box at the top of the page.

Configure ESP

1. Select ESP - MyEsp in the Navigator panel on the left side.
2. Select the **HTTPS** tab.

Figure 11. Select HTTPS Tab

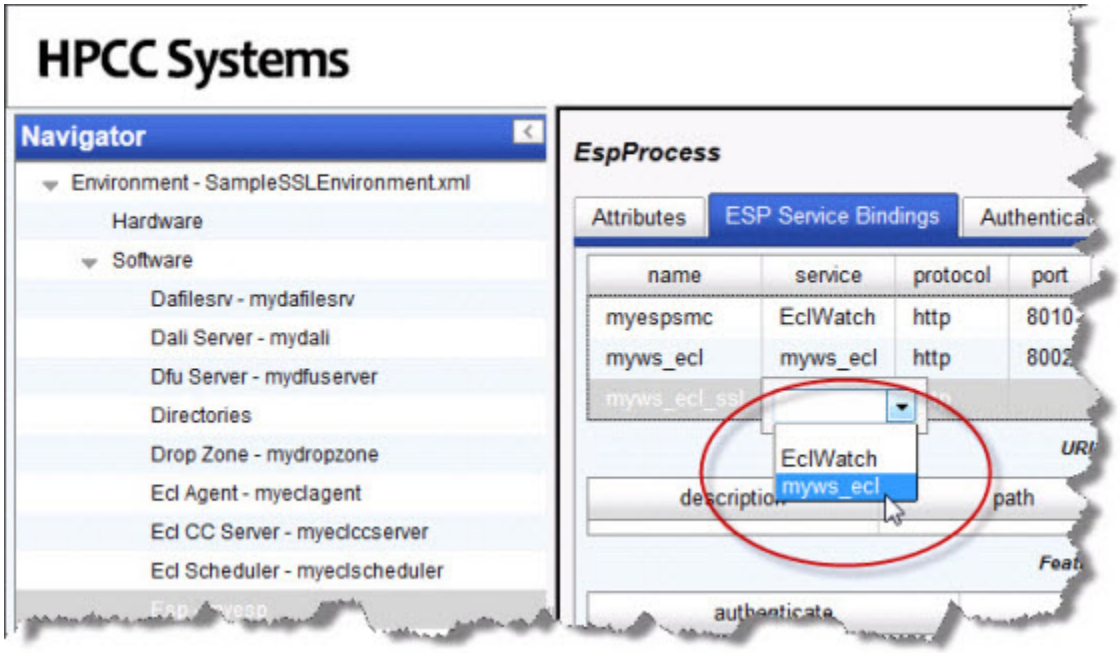


3. In the **passphrase** entry control, enter the passphrase you used earlier when you created the private key.
4. When prompted, provide the passphrase again.
5. Click the disk icon to save.

Configure one or more SSL-Enabled Service Bindings

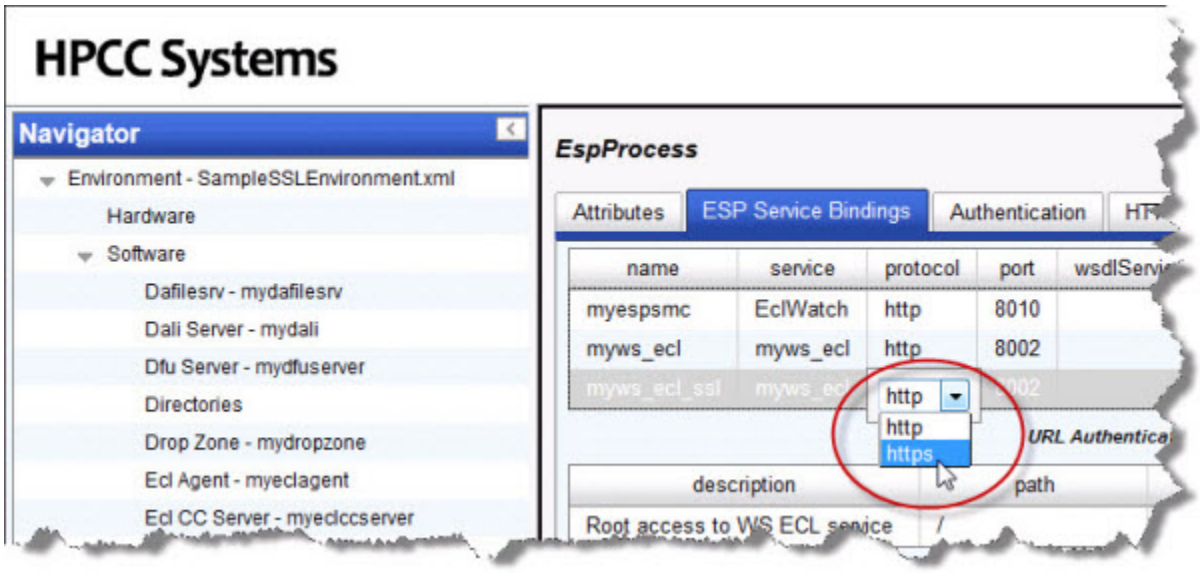
1. Select the ESP Service Bindings tab.
2. Right-click on the list of services, then select **Add**.
3. Provide a name for the binding (e.g., myws_ecl_ssl)
4. Select myws_ecl from the service drop-list.

Figure 12. myws_ecl



5. Select https from the protocol drop-list.

Figure 13. Select HTTPS



Note: If you have not previously edited the port, the change from http to https triggers Configuration Manager to automatically change the port to the default port for https (18002). It only updates automatically if the port has not been edited.

6. Click the disk icon to save

To ensure security, once you have confirmed access to your secure service via https, you delete the service binding which uses http. You should then repeat the process for **all** other service bindings.

Distribute the environment configuration file to all nodes, Restart, and Certify

Once your environment is set up as desired, you must copy the configuration file out to the other nodes.

1. If it is running, stop the system.

   Make sure system is stopped before attempting to move the environment.xml file.

2. Back up the original environment.xml file

   ```
   # for example
   sudo cp /etc/HPCCSystems/environment.xml /etc/HPCCSystems/environment.bak
   ```

   Note: the "live" environment.xml file is located in your **/etc/HPCCSystems/** directory. ConfigManager works on files in **/etc/HPCCSystems/source** directory. You must copy the XML file from this location to make an environment.xml file active.

3. Copy the NewEnvironment.xml file from the source directory to the /etc/HPCCSystems and rename the file to environment.xml

   ```
   # for example
   sudo cp /etc/HPCCSystems/source/NewEnvironment.xml /etc/HPCCSystems/environment.xml
   ```

4. Copy the **/etc/HPCCSystems/environment.xml** to the **/etc/HPCCSystems/** on every node.

   You might prefer to use a script to automate this step, especially if you have many nodes. See the Example Scripts section in the Appendix of the Installing and Running the HPCCPlatform manual.

5. Restart the HPCC system and certify the components as usual.

Configuring SSL for Roxie

Roxie can also be configured to use the Secure Sockets Layer (SSL) protocol. You may have already completed some of these steps if you configured your ESP Server to use SSL as described in the previous section. Please refer to the SSL For ESP section for more information on creating keys and certificates.

Configure HTTPS on your Roxie Cluster

Start Configuration Manager in Advanced Mode

1. Start the Configuration Manager Service on one node (usually the first node is considered the head node and is used for this task, but this is up to you).

   ```
   sudo /opt/HPCCSystems/sbin/configmgr
   ```

2. Using a Web browser, go to the Configuration Manager's interface.

   Use the url of http://nnn.nnn.nnn.nnn:pppp, where nnn.nnn.nnn.nnn is the IP address of the node running Configuration Manager and pppp is the port (default is 8015).

   The Configuration Manager startup wizard displays.

3. Select **Advanced View**.

4. Select an XML file from the drop list.

   This list is populated from versions of an environment XML file in your server's **/etc/HPCCSystems/source/** directory.

   Tip: The XML file that matches the active environment.xml is highlighted.

5. Press the **Next** button.

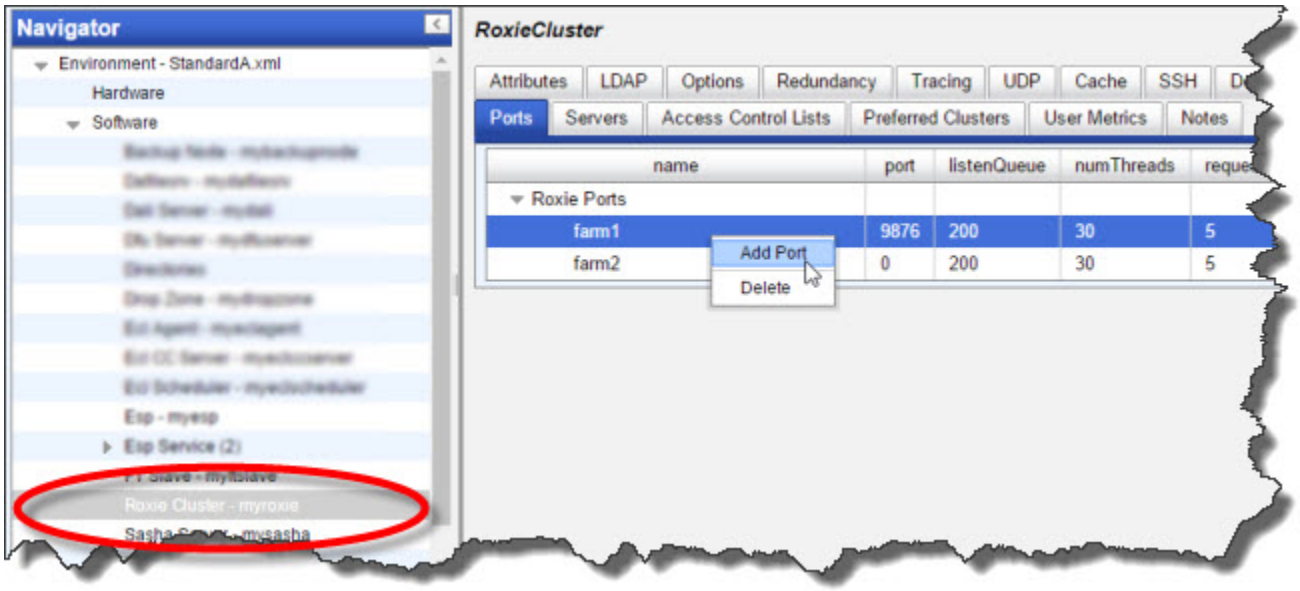
   The Configuration Manager Advanced View interface displays.

6. Check the **Write Access** box at the top of the page.

Configure Roxie SSL

1. Select your Roxie Cluster in the Navigator panel on the left side.
2. Select the **Ports** tab.
3. Right-click on the list of ports, then select **Add**.

Figure 14. Select Port Tab



4. The default port number is 9876. Change the default port number, for example, to 19876.
5. Change the protocol from *Native* to *SSL* from the drop menu (image).
6. In the **passphrase** entry control, enter the passphrase you used earlier when you created the private key. Leave this field empty if you did not use a passphrase.
7. When prompted, provide the passphrase again.
8. Enter the certificate filename.
9. Enter the key filename.
10. Click the disk icon to save.

The default lookup location for the certificate and key files is in */var/lib/HPCCSystems/myroxie*. You can specify a full path if you want these files in a different location. The certificate and key files must be available for each Roxie node.

Distribute the environment configuration file to all nodes, Restart, and Certify

Once your environment is set up as desired, you must copy the configuration file out to the other nodes. For more information about how to distribute your environment, please see the section Distribute the environment configuration file above.

More Examples

This section contains additional ECL examples you can use on your HPCC Systems cluster. You can run these on a single-node system or a larger multi-node cluster.

Anagram Examples

The following examples display some of things that HPCC Systems can do. Running through these examples will help your understanding of HPCC Systems and ECL.

ECL Example: Anagram1

This example takes a STRING and produces every possible anagram from it. This code is the basis for a second example which evaluates which of these are actual words using a word list data file.

1. Open the ECL IDE (Start **>>** All Programs **>>** HPCC Systems **>>** ECL IDE) and login to your HPCC Systems platform instance.

2. Open a new **Builder Window** (CTRL+N) and write the following code:

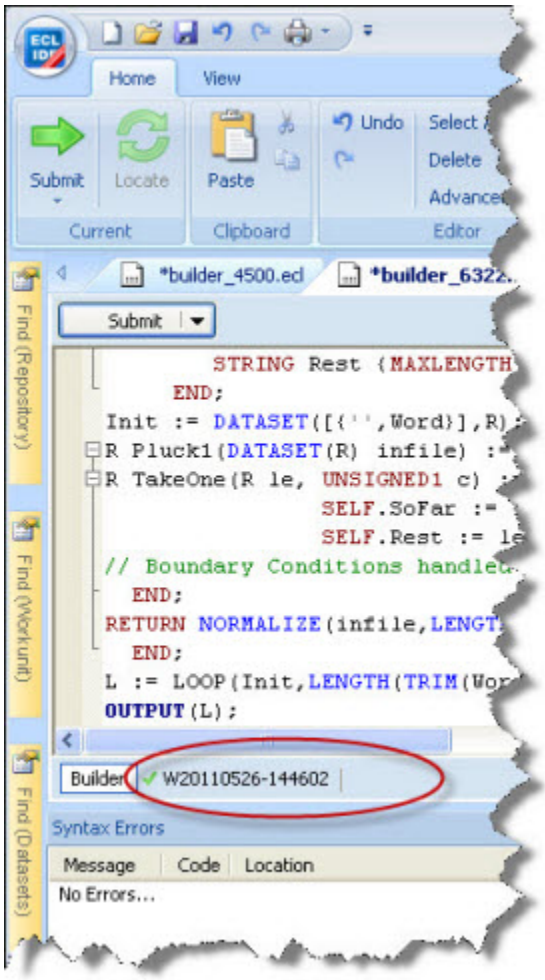
```
STRING Word := 'FRED' :STORED('Word');
R := RECORD
        STRING SoFar {MAXLENGTH(200)};
        STRING Rest {MAXLENGTH(200)};
     END;
Init := DATASET([{'',Word}],R);
R Pluck1(DATASET(R) infile) := FUNCTION
R TakeOne(R le, UNSIGNED1 c) := TRANSFORM
                SELF.SoFar := le.SoFar + le.Rest[c];
                SELF.Rest := le.Rest[..c-1]+le.Rest[c+1..];
// Boundary Conditions handled automatically
  END;
RETURN NORMALIZE(infile,LENGTH(LEFT.Rest),TakeOne(LEFT,COUNTER));
  END;
L := LOOP(Init,LENGTH(TRIM(Word)),Pluck1(ROWS(LEFT)));
OUTPUT(L);
```

3. Select **thor** as your target cluster.

4. Press the syntax check button on the main toolbar (or press F7)

5. Press the **Submit** button (or press ctrl+enter).

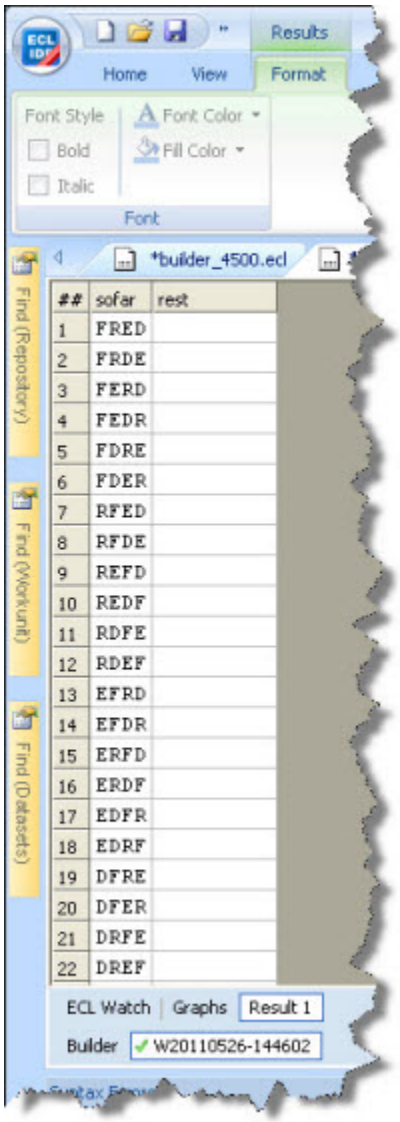
Figure 15. Completed job



The green check mark indicates successful completion.

6. Click on the workunit number tab and then on the Result 1 tab to see the output.

Figure 16. Completed job output



Roxie Example: Anagram2

In this example, we will download an open source data file of dictionary words, spray that file to our Thor cluster, then validate our anagrams against that file so that we determine which are valid words. The validation step uses a JOIN of the anagram list to the dictionary file. Using an index and a keyed join would be more efficient, but this serves as a simple example.

Download the word list

We will download the word list from http://wordlist.aspell.net/12dicts

1. Download the *Official 12 Dicts* Package. The files are available in tar.gz or ZIP format.

2. Extract the package contents and save the **2of12.txt** file (typically found in the American sub-folder) to a folder on your local machine.

Load the Dictionary File to your Landing Zone

In this step, you will copy the data files to a location from which it can be sprayed to your HPCC Systems cluster. A Landing Zone is a storage location attached to your HPCC Systems platform. It has a utility running to facilitate file spraying to a cluster.

For smaller data files, maximum of 2GB, you can use the upload/download file utility in ECL Watch. This data file is only ~400 kb.

Next you will distribute (or Spray) the dataset to all the nodes in the HPCC Systems cluster. The power of HPCC Systems comes from its ability to assign multiple processors to work on different portions of the data file in parallel. Even if your deployment only has a single node, the data must be sprayed to the cluster.

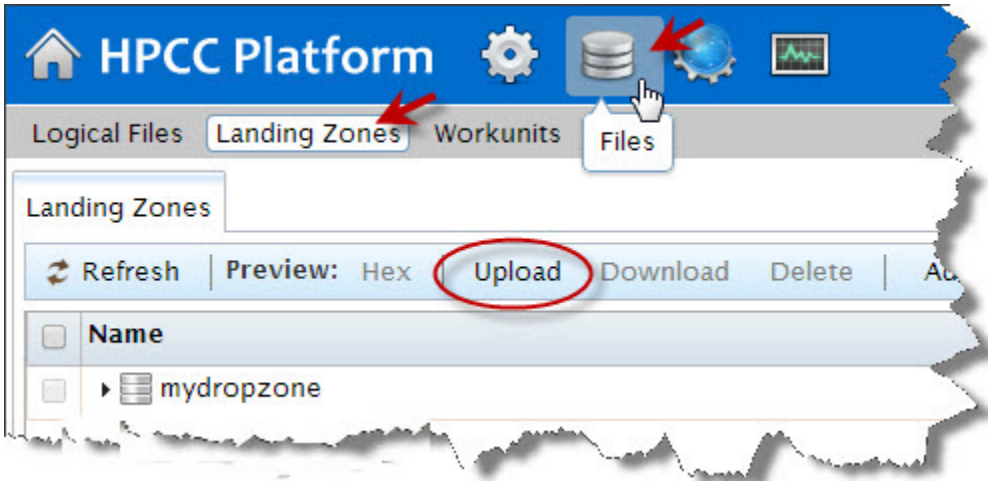
1. In your browser, go to the **ECL Watch** URL. For example, http://nnn.nnn.nnn.nnn:8010, where nnn.nnn.nnn.nnn is your ESP Server's IP address.

	Your IP address could be different from the ones provided in the example images. Please use the IP address provided by **your** installation.

2. From ECL Watch click on the **Files** icon, then click the **Landing Zones** link from the navigation sub-menu.

   Press the **Upload** action button.

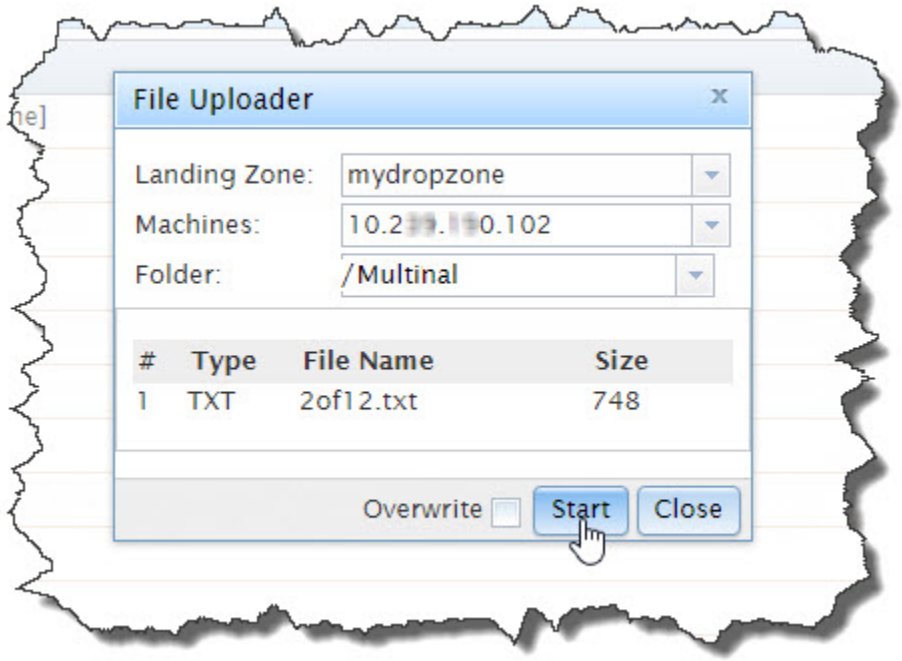
Figure 17. Upload



3. A dialog opens. **Browse** to and select the file to upload and then press the **Open** button.

   The file you selected should appear in the **File Name** field. The data file is named: **2of12.txt**.

4. ### Figure 18. Start File Upload



   Press the **Start** button to complete the file upload.

Spray the Data File to your *Data Refinery (Thor) Cluster*

To use the data file in our HPCC Systems cluster, we must "spray" it to all the nodes. A *spray* or *import* is the relocation of a data file from one location (such as a Landing Zone) to multiple file parts on nodes in a cluster.

The distributed or sprayed file is given a *logical-file-name* as follows**: ~thor::word_list_csv** The system maintains a list of logical files and the corresponding physical file locations of the file parts.

1. Open ECL Watch using the following URL:

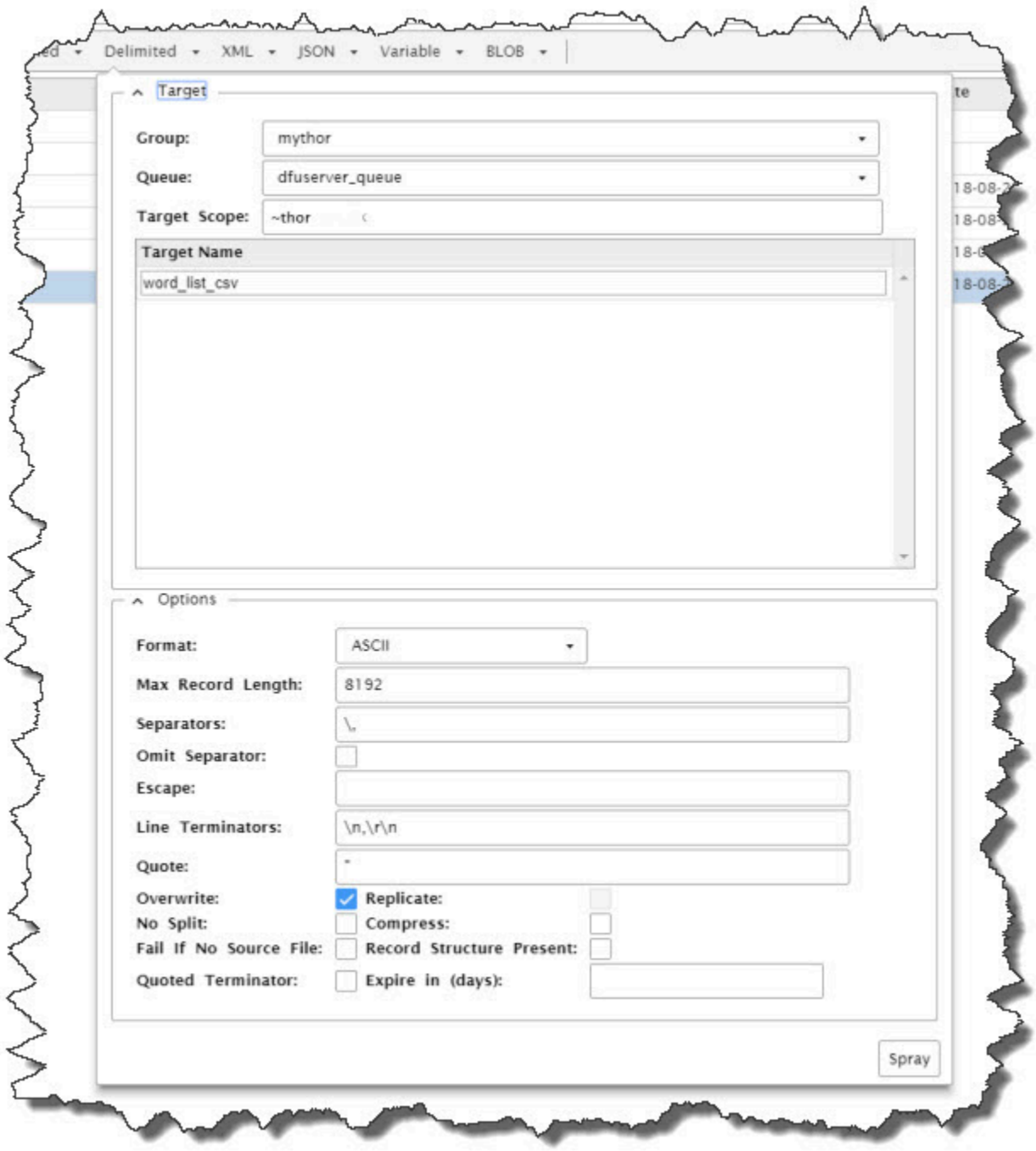
   http://nnn.nnn.nnn.nnn:pppp(where nnn.nnn.nnn.nnn is your ESP Server's IP Address and pppp is the port. The default port is 8010)

2. Click on the **Files** icon, then click the **Landing Zones** link from the navigation sub-menu. Select the appropriate landing zone (if there are more than one landing zones). Click the arrow to the left of your landing zone to expand it.

3. Select the file from your drop zone by checking the box next to it.

4. Check the box next to 2of12.txt, then press the **Delimited** button.

Figure 19. Spray Delimited



The **DFU Spray Delimited** page displays.

5. Select mythor in the Target Group drop list.

6. Complete the Target Scope as *thor*.

7. Fill in the rest of the parameters (if they are not filled in already).
   - Max Record Length 8192
   - Separator \,
   - Line Terminator \n,\r\n
   - Quote: '
8. Fill in the Target Name using the rest of the Logical File name desired: word_list_csv
9. Make sure the **Overwrite** box is checked.

   If available, make sure the **Replicate** box is checked. (The Replicate option is only available on systems where replication has been enabled.)
10. Press the **Spray** button.

    A tab displays the DFU Workunit where you can see the progress of the spray.

Run the query on Thor

1. Open a new **Builder Window** (CTRL+N) and write the following code:

```
IMPORT Std;
layout_word_list := record
  string word;
end;
File_Word_List := dataset('~thor::word_list_csv', layout_word_list,
                          CSV(heading(1),separator(','),quote('')));
STRING Word := 'teacher' :STORED('Word');
STRING SortString(STRING input) := FUNCTION
  OneChar := RECORD
    STRING c;
  END;
  OneChar MakeSingle(OneChar L, unsigned pos) := TRANSFORM
    SELF.c := L.c[pos];
  END;
  Split := NORMALIZE(DATASET([input],OneChar), LENGTH(input),
  MakeSingle(LEFT,COUNTER));
  SortedSplit := SORT(Split, c);
  OneChar Recombine(OneChar L, OneChar R) := TRANSFORM
    SELF.c := L.c+R.c;
  END;
  Recombined := ROLLUP(SortedSplit, Recombine(LEFT, RIGHT),ALL);
  RETURN Recombined[1].c;
END;

STRING CleanedWord := SortString(TRIM(Std.Str.ToUpperCase(Word)));

R := RECORD
  STRING SoFar {MAXLENGTH(200)};
  STRING Rest {MAXLENGTH(200)};
END;
Init := DATASET([{'',CleanedWord}],R);
R Pluck1(DATASET(R) infile) := FUNCTION
  R TakeOne(R le, UNSIGNED1 c) := TRANSFORM
    SELF.SoFar := le.SoFar + le.Rest[c];
    SELF.Rest := le.Rest[..c-1]+le.Rest[c+1..];
    // Boundary Conditions
    // handled automatically
```

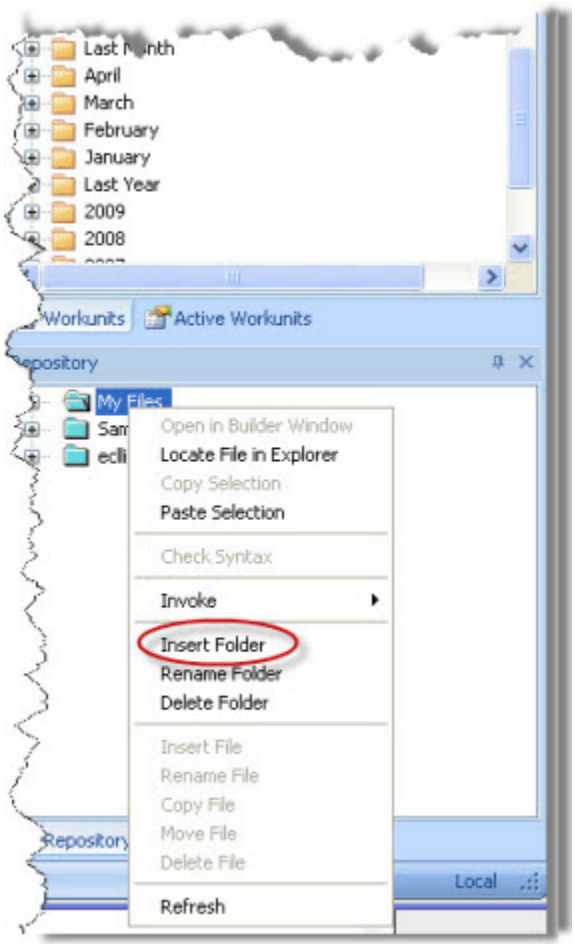
```
  END;
  RETURN DEDUP(NORMALIZE(infile,LENGTH(LEFT.Rest),TakeOne(LEFT,COUNTER)));
END;
L := LOOP(Init,LENGTH(CleanedWord),Pluck1(ROWS(LEFT)));
ValidWords := JOIN(L,File_Word_List,
LEFT.SoFar=Std.Str.ToUpperCase(RIGHT.Word),TRANSFORM(LEFT));
OUTPUT(CleanedWord);
COUNT(ValidWords);
OUTPUT(ValidWords)
```

2. Select **thor** as your target cluster.
3. Press the syntax check button on the main toolbar (or press F7)
4. Press the **Submit** button.
5. When it completes, select the Workunit tab, then select the Result tab.
6. Examine the result.

Compile and Publish the query to Roxie

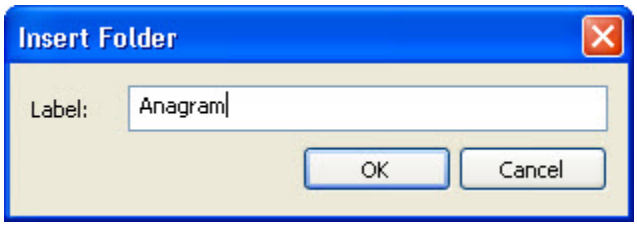
1. Right-click on the **My Files** folder in the Repository window, and select **Insert Folder** from the pop-up menu.

Figure 20. Insert Folder



2. Enter **Anagram** for the label, then press the OK button.

Figure 21. Enter Folder Label

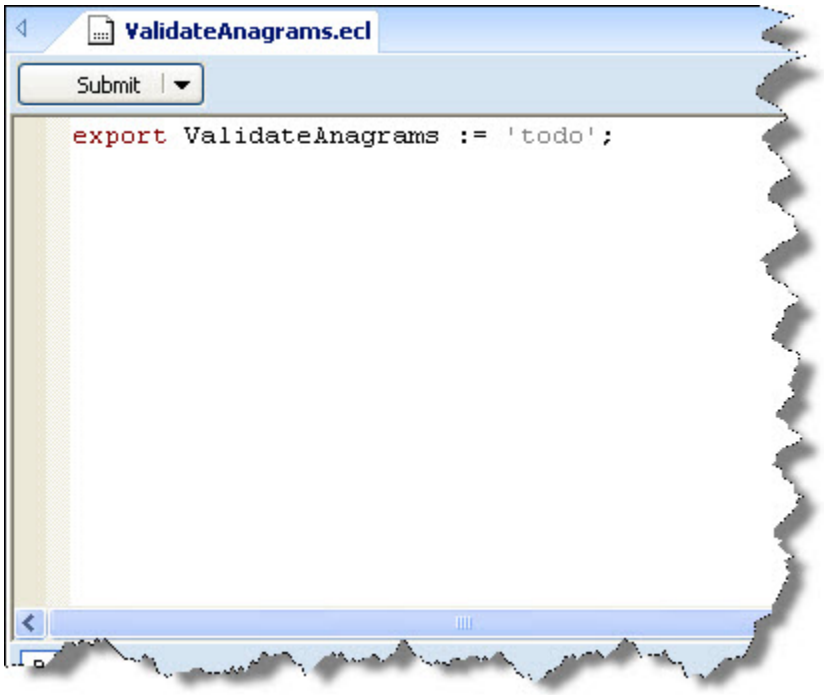


3. Right-click on the **Anagram** Folder, and select **Insert File** from the pop-up menu.

4. Enter **ValidateAnagrams** for the label, then press the OK button.

   A Builder Window opens.

Figure 22. Builder Window



5. Write the following code (you can copy the code from the other builder window):

```
IMPORT Std;
layout_word_list := record
  string word;
end;
File_Word_List := dataset('~thor::word_list_csv', layout_word_list,
                          CSV(heading(1),separator(','),quote('')));
STRING Word := 'teacher' :STORED('Word');
STRING SortString(STRING input) := FUNCTION
  OneChar := RECORD
    STRING c;
  END;
  OneChar MakeSingle(OneChar L, unsigned pos) := TRANSFORM
```

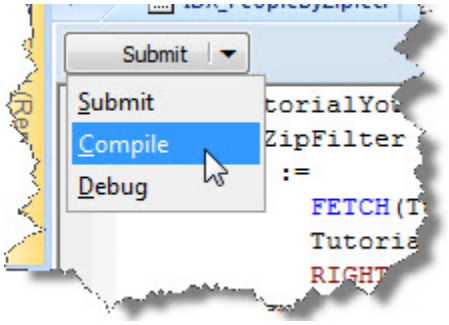
```
    SELF.c := L.c[pos];
  END;
  Split := NORMALIZE(DATASET([input],OneChar), LENGTH(input),
  MakeSingle(LEFT,COUNTER));
  SortedSplit := SORT(Split, c);
  OneChar Recombine(OneChar L, OneChar R) := TRANSFORM
    SELF.c := L.c+R.c;
  END;
  Recombined := ROLLUP(SortedSplit, Recombine(LEFT, RIGHT),ALL);
  RETURN Recombined[1].c;
END;

STRING CleanedWord := SortString(TRIM(Std.Str.ToUpperCase(Word)));

R := RECORD
  STRING SoFar {MAXLENGTH(200)};
  STRING Rest {MAXLENGTH(200)};
END;
Init := DATASET([{'',CleanedWord}],R);
R Pluck1(DATASET(R) infile) := FUNCTION
  R TakeOne(R le, UNSIGNED1 c) := TRANSFORM
    SELF.SoFar := le.SoFar + le.Rest[c];
    SELF.Rest := le.Rest[..c-1]+le.Rest[c+1..];
    // Boundary Conditions
    // handled automatically
  END;
  RETURN DEDUP(NORMALIZE(infile,LENGTH(LEFT.Rest),TakeOne(LEFT,COUNTER)));
END;
L := LOOP(Init,LENGTH(CleanedWord),Pluck1(ROWS(LEFT)));
ValidWords := JOIN(L,File_Word_List,
LEFT.SoFar=Std.Str.ToUpperCase(RIGHT.Word),TRANSFORM(LEFT));
OUTPUT(CleanedWord);
COUNT(ValidWords);
OUTPUT(ValidWords)
```

6. Select **Roxie** as your target cluster.

7. Press the syntax check button on the main toolbar (or press F7)

8. In the Builder window, in the upper left corner the **Submit** button has a drop down arrow next to it. Select the arrow to expose the **Compile** option.

Figure 23. Compile

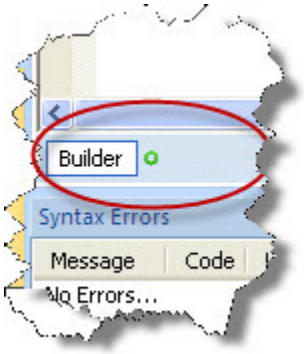


9. Select **Compile**

10. When it completes, select the Workunit tab, then select the Result tab.

11.When the workunit finishes, it will display a green circle indicating it has compiled.

Figure 24. Compiled

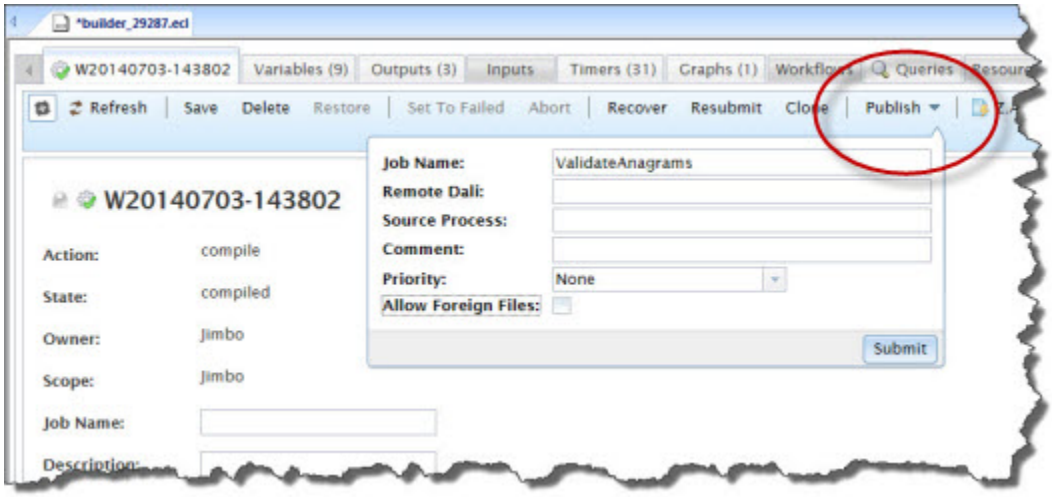


Publish the Roxie query

Next we will publish the query to a Roxie Cluster.

1. Select the workunit tab for the ValidateAnagrams that you just compiled.
2. Select the ECL Watch tab.
3. Press the **Publish** button, complete the dialog, and press **Submit**.

Figure 25. Publish Query



When it successfully publishes, a confirmation message displays.

Run the Roxie Query in WsECL

Now that the query is published to a Roxie cluster, we can run it using the WsECL service. WsECL is a web-based interface to queries on an HPCC Systems platform. Use the following URL:

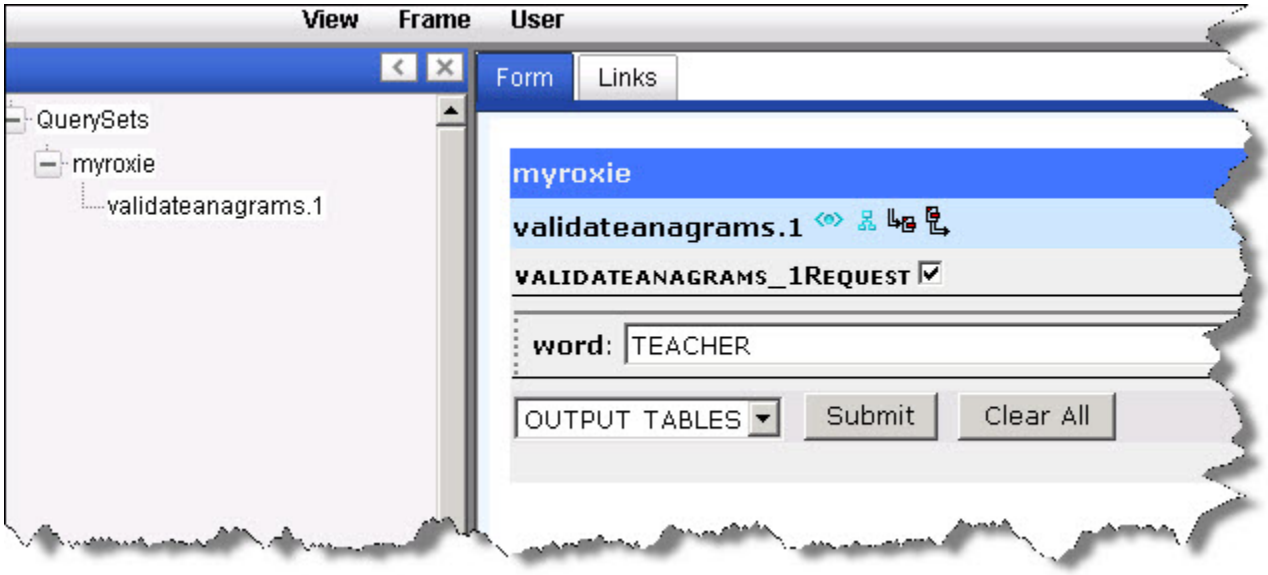
http://nnn.nnn.nnn.nnn:pppp (where nnn.nnn.nnn.nnn is your ESP Server's IP address and pppp is the port. The default port is 8002)

1. Click on the + sign next to **myroxie** to expand the tree.

2. Click on the **ValidateAnagrams.1** hyperlink.

   The form for the service displays.

Figure 26. RoxieECL

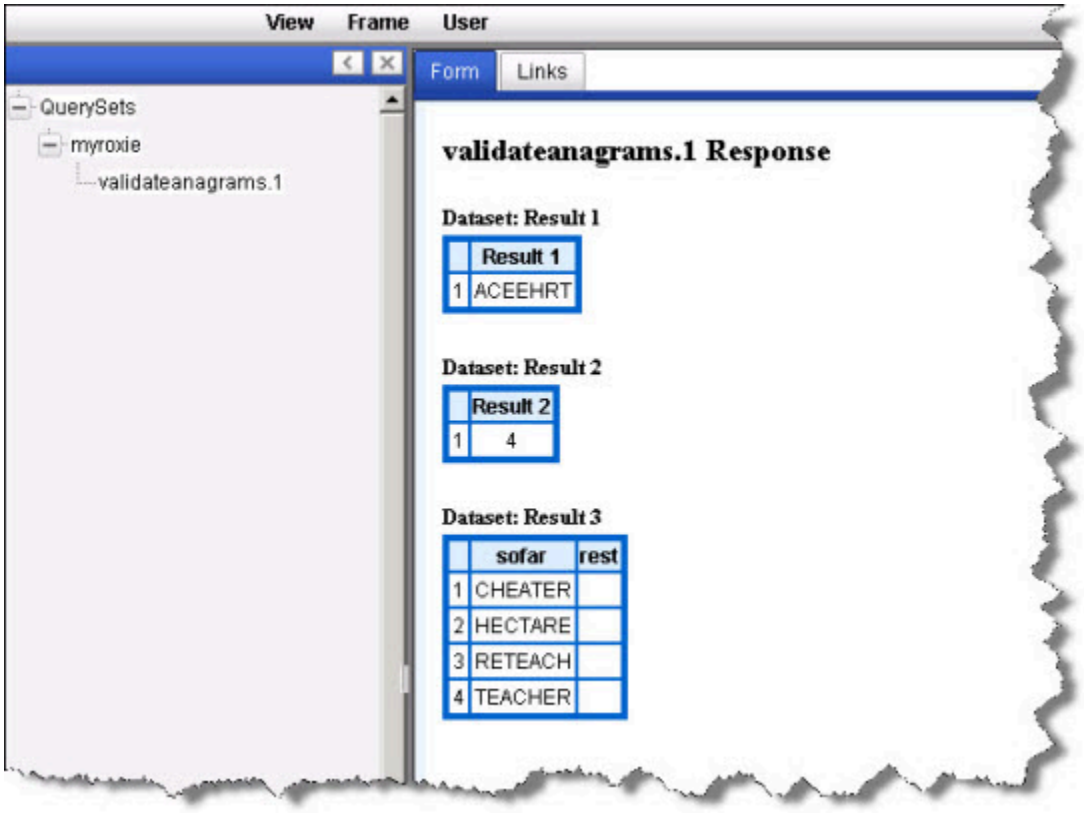


3. Select Output Tables in the drop list.

4. Provide a word to make anagrams from (e.g., TEACHER), then press the Submit button.

   The results display.

Figure 27. RoxieResults

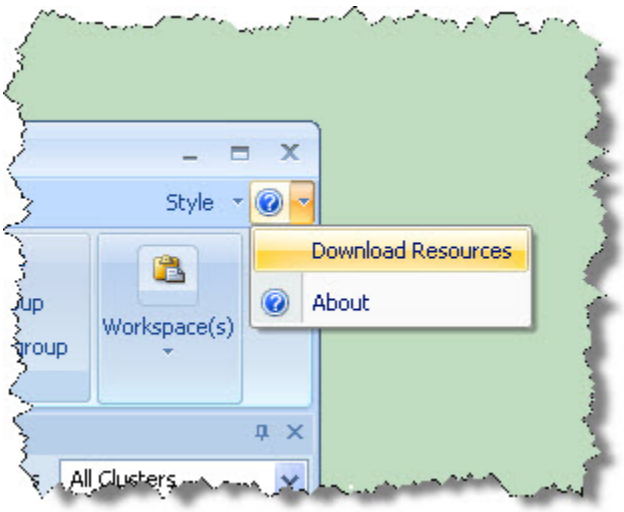


Next Steps

Available from the menu in the ECL IDE there are several documents which provide details on various aspects of the HPCC Systems.

You can access them from the help menu: Help **>>** Documentation.

Figure 28. Help Menu



You can also find these from the **Start** menu :

Start **>>** All Programs **>>** HPCC Systems **>>** ECL IDE **>>** Docs

To familiarize yourself with what your system can do we recommend following the steps in

- The **HPCC Systems Data Tutorial**
- Read **Using Config Manager** to learn how to configure an HPCC Systems platform using Advanced View.
- Use your new skills to process your own massive dataset!

The HPCC Systems® Portal is also a valuable resource for more information including:

- Video Tutorials
- Additional examples
- White Papers
- Documentation

Appendix

Example Scripts

For a multi-node configuration, you must install the packages on each node. You can install each one manually or use scripts to copy and install the packages. On a large system where you have many nodes copying and installing on every node is not practical, therefore we provide some scripts you can use or to serve as examples to give you a start in making your own.

Scripts are installed to the **/opt/HPCCSystems/sbin** directory. Scripts should be run as sudo or as a user with appropriate privileges on all nodes. The scripts have the ability to multi-thread.

Make sure that you have the sufficient privileges to sudo as an administrator to use the install-cluster.sh script. To use the hpcc-push.sh or hpcc-run.sh scripts, you must sudo as user **hpcc**.

install-cluster.sh

install-cluster.sh [-k | -p <directory>] [-n <value>] <package-name>

<package-name>	Name of the HPCC Systems package to install. Required
-h	Help. Optional.
-k, --newkey	When specified, the script generates and distributes ssh keys to all hosts. Optional.
-p, --pushkeydir	Push existing ssh key to remote machine. Optional. Use either -k or -p, not both.
-n, --concurrent	When specified, denotes the number of concurrent executions. Default is 5. Optional.

You can run this script as any user with sufficient permissions to execute it; however, when prompted for username/password, you must provide credentials for a user with sufficient sudo rights to run commands as an administrator on all nodes.

Before you can use this script, you must have already defined and generated an environment.xml file (using ConfigMgr's wizard or advanced mode). This script:

- reads the active environment.xml file and gathers a list of nodes upon which to act.
- installs the HPCC Systems platform package(s) on all nodes specified.
- pushes out and deploys the environment file (environment.xml) to all nodes specified.
- optionally, if you specify the -k option it also generates the required ssh keys and deploys them as required to all nodes specified.
- optionally, if you specify the -p option it pushes out the existing ssh keys to all nodes specified. Use either the -k or the -p option, but not both.
- optionally, if you specify the -n <value> option it spawns that many concurrent executions. Default is 5.

Examples:

This example installs the HPCC Systems platform packages to remaining nodes and pushes out the active environment.xml file to those nodes.:

```
sudo /opt/HPCCSystems/sbin/install-cluster.sh hpccsystems-platform-xxxx-n.n.nnnn
```

(where *n.n.nnnn* is the build number)

This example installs the HPCC Systems platform packages to all nodes and pushes out the active environment.xml file to those nodes. It also generates ssh keys and pushes them out to all nodes.

```
sudo /opt/HPCCSystems/sbin/install-cluster.sh -k hpccsystems-platform-xxxx-n.n.nnnn
```

(where *n.n.nnnn* is the build number)

This example installs the HPCC Systems platform packages and pushes out the active environment.xml file to 8 concurrent nodes.:

```
sudo /opt/HPCCSystems/sbin/install-cluster.sh -n 8 hpccsystems-platform-xxxx-n.n.nnnn
```

(where *n.n.nnnn* is the build number)

deploy-java-files.sh

deploy-java-files.sh [-c] [-e] [-H <value>] [-n <value>] [-r] [-s <value>] [-t <value>] [-u <value>] [-x]

-c	When specified, this option adds the target directory or jar file path to classpath in environment.conf.
-e	When specified, this denotes the target is to be removed from the classpath.
-H	Host IP list. When specified, will target the IP addresses specified, one IP address per line. If this option is not used will run on the IP list generated from the environment.xml
-n	When specified, denotes the number of concurrent execution threads. Default is 5. You must have python installed, otherwise this option will be ignored and the action will run on each host sequentially.
-r	Reset classpath. When specified, will reset the classpath to <install_directory>/classes. If used in conjunction with the -t adds the new entries to the classpath after reset.
-s	Source file or directory.
-t	Target directory. The default is <install_directory>/classes. If it is only for adding to classpath, the value can be the full path of the java jar file.
-u	The username to use for ssh access to remote system. Provide this option when the specified user does not use a password to run ssh/scp. Without specifying this option you will be prompted to supply a username and password. We strongly recommend not using <hpcc user> to avoid security issues.
-x	When specified, this option excludes execution on the current host.

The **deploy-java-files.sh** script, is used to deploy java files (source) to HPCC Systems cluster hosts and update the classpath variable in environment.conf.

This script runs a command on all IP addresses or host names in the active environment.xml. The IP addresses are defined when editing the environment in ConfigMgr.

This script writes to a log file:

/var/log/HPCCSystems/cluster/se_<action>_<commnd>_<pid>_yyyymmdd_HHMMSS.log

Examples:

To deploy java files from /home/hpcc/development/java/ on local system to /home/hpcc/java/ on all hosts in cluster and update classpath with 10 concurrent executions:

```
./deploy-java-files.sh -s /home/hpcc/development/java/* -t /home/hpcc/java/ -c -n 10
```

To deploy java files from /home/hpcc/java/ on local system to /home/hpcc/java on all hosts in cluster except local system:

```
./deploy-java-files.sh -s /home/hpcc/java/* -t /home/hpcc/java -x
```

To update classpath for a cluster:

```
./deploy-java-files.sh -c -t /home/hpcc/develop/java:/home/hpcc/test/java/
```

To To deploy java files to a list of hosts :

```
./deploy-java-files.sh -H /home/hpcc/hosts.txt -s /home/hpcc/java/* -t /home/hpcc/java/
```

hpcc-push.sh

hpcc-push.sh [-s <source>] [-t <target>] [-n <concurrent>] [-x]

-s	Source file or directory.
-t	Target file or directory.
-n, --concurrent	When specified, denotes the number of concurrent executions. Default is 5. Optional.
-x	When specified, this option excludes execution on the current host.

This script "pushes" files from the source filename and path to the destination filename and path for all IP addresses in the active environment.xml.

To use this script, the ssh keys need to be properly configured on all nodes, and you must use sudo.

The IP addresses were defined when editing the environment in ConfigMgr.

```
sudo /opt/HPCCSystems/sbin/hpcc-push.sh -s <sourcefile> -t <destinationfile>
```

For example:

```
sudo /opt/HPCCSystems/sbin/hpcc-push.sh -x \
     -s /etc/HPCCSystems/environment.xml -t /etc/HPCCSystems/environment.xml
```

hpcc-run.sh

hpcc-run.sh [-c component] [-n concurrent] [-s] [-S] {start|stop|restart|status}

-c, --comp	HPCC Systems component. For example, dali@mydali.service, roxie@myroxie.service, etc.
-n, --concurrent	When specified, denotes the number of concurrent instances to run. The default is 5. Optional.
-S, --sequentially	When specified, the command runs sequentially, one host at a time.
-s, --save	When specified, saves the result to a file named <ip address>.

To use this script, the ssh keys need to be properly configured on all nodes, and you must sudo as user hpcc.

This script runs a command on all IP addresses in the active environment.xml.

The IP addresses were defined when editing the environment in ConfigMgr. This script supports all the parameters of hpcc-init and dafilesrv.

Examples:

This example starts all components on the nodes

```
sudo /opt/HPCCSystems/sbin/hpcc-run.sh start
```

This example starts all components on all the nodes, using 8 concurrent executions

```
sudo /opt/HPCCSystems/sbin/hpcc-run.sh start -n 8
```

This example starts all components of the dali type on the nodes

```
sudo /opt/HPCCSystems/sbin/hpcc-run.sh -c dali@mydali.service start
```

This example starts the dafilesrv helper application

```
sudo /opt/HPCCSystems/sbin/hpcc-run.sh -c dafilesrv@dafilesrv.service start
```

update-keys

update-keys [-s <secret_key> -p <public_key>] [-g] [-n <number of concurrent threads>]

-s	SSH Secret Key.
-p	SSH Public Key.
-g	Generates new id_rsa private/public keys and will overwrite any user supplied keys to use the new generated keys.
-n	Number of concurrent threads, default is 5.

This script is intended to assist administrators to deploy HPCC Systems SSH keys across their cluster. SSH keys are used primarily for component startup such as Thor and certain plug-ins such as Spark. SSH keys are more important in a physical bare-metal environment and less so in a cloud environment.

Examples:

```
sudo /opt/HPCCSystems/sbin/update-keys -g
```

This example generates new private/public SSH keys and overwrites any existing keys and distributes the keys to the components.

Uninstalling the HPCC Systems Platform

To uninstall the HPCC Systems platform, issue the appropriate commands for your system. If necessary, do so on each node that it is installed on.

Centos/Red Hat

```
sudo yum remove hpccsystems-platform
```

Ubuntu/Debian

```
sudo apt-get remove hpccsystems-platform
```

Helper Applications

There is a helper applications that runs on all nodes that you may need to stop or start manually.

Normally, this process is started automatically the first time the hpcc-init service executes.

Enter the following commands to stop or start the helper application:

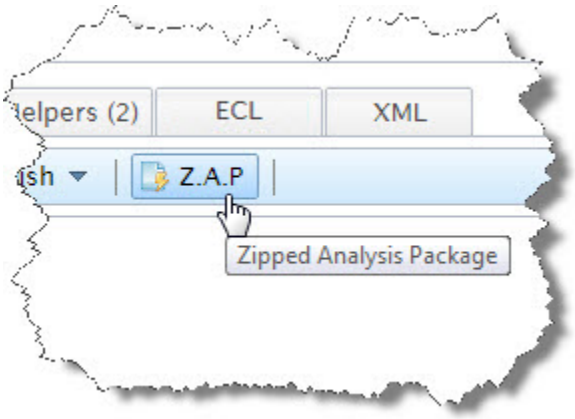
- dafilesrv

```
sudo systemctl dafilesrv@dafilesrv.service stop

sudo systemctl dafilesrv@dafilesrv.service start
```

Z.A.P. Utility

The Zipped Analysis Package (Z.A.P.) button is a utility for collecting system information and encapsulating it into a shareable package. It is a useful tool for reporting errors, inconsistencies, or other unexpected behavior. When there is such an occurrence, this utility packages up information to send for further analysis.

Figure 29. Z.A.P. Button



To use the Z.A.P. utility, press the Z.A.P. button on the workunit details page from the appropriate workunit. The button opens the Zipped Analysis Package dialog.

Some of the required fields are populated. Fill in the corresponding values under Description, History, and the other fields. Optionally, you can password protect the ZAP package and choose to include worker logs. Worker logs are not included by default. If there are worker logs, the option to include them is available. You must check that field when available to include the worker logs.

If your data contains sensitive information, such as personally identifiable information (PII), save the ZAP package, sanitize the data, then email it manually. If appropriate to share your data, you can take advantage of the Send Email field.

The Send Email field is only available if email is configured for the ESP service in the Configuration Manager. If available, check the Send Email box to email the ZAP report. Only an Administrator can configure the email. The (To) Email Address is also set by the Administrator and can only be changed in the configuration. The (From) Email Address can be set in the Configuration Manager, but can be changed if desired. The Email Subject is required, but the Email Body is optional.

Press the **Apply** button when all the dialog fields are completed. At that point if you checked the Send Email box, the Z.A.P. report gets sent. If email is not configured, the Z.A.P. utility generates a zip file with all the appropriate information for troubleshooting.

You can find the generated zip file in your browser's designated download directory. You can now manually send this file to the person handling your support request, or you can upload the file into the issue tracking system. Remember, you should only use the email feature if appropriate to share your data.

Configuration Options

The component logs are some of the most important artifacts included in these ZAP reports.

The logging behavior differs on bare metal and containerized deployments. In bare metal, some logs are always slated to be included (Thor Manager, ECLCC Server, and ECL Agent). The UI checkbox “Include worker logs” controls the inclusion of the Thor Worker log files.

In a containerized environment, you can choose to exclude all the logs. Deselect the UI check boxes for the inclusion of the logs. Containerized deployments allow this flexibility because logs require a remote log reader component which may not be configured on your system. Cloud-based logging can lead to additional expenses for data collection and downloads compared to traditional bare metal systems, which is why some cloud deployments may have logging disabled.

Including the Logs

To include the logs check the two UI check boxes:

Include related logs : Controls inclusion of the <wuid>.log file.

Include per-component logs: Controls inclusion of logs generated from at least these components (the list may be vary based on your deployment): ECLCC Server, Thor-ECL Agent, Thor Manager, Thor Agent, and Thor Worker.

In order for these logs to be included in the Z.A.P. the bare metal deployments require the ESP feature permission **Cluster Topology Access** value to be set to **READ**.

```
ClusterTopologyAccess:READ
```

A containerized deployment must have logging properly configured to be able to include logs. Additionally the user must have the feature permission *WsLogAccess:Read* or the logs will be excluded and instead contain an error message indicating which permission is required.

If a "no access" message is present in the ZAP file and there are no log files, the permission value specified in the error message must be set to ensure the logs are included in the ZAP report.

See the Containerized Logging section in the Containerized HPCC Systems Platform documentation for more information about configuring log processing.

hpcc-init

Systems utilizing System V based init systems do not support the systemd calls utilized by HPCC Systems. We will continue to support the old System V style init.d calls.

hpcc-init [*option*] *command*

option

- -c *componentname*, --component=*componentname*

  Specifies the component upon which to execute the command. If omitted, the default is **all** components on the machine.

  -c *componenttype*, --component=*componenttype*

  Specifies the component type upon which to execute the command. If more than one of this type is configured, all will be acted upon. If omitted, the default is **all** components on the machine.

- --componentlist

  Provides a list of all component names on the current node as specified in the environment file.

- --typelist

  Provides a list of all component types on the current node as specified in the environment file.

- -h, --help

  Displays a help page

command

- start:

  Starts component(s)

- stop

  Stops component(s)

- status

  Displays component(s) status

- restart

  Restarts component(s)

- setup

  Initializes component configuration files but does not start the component(s).

The **hpcc-init** function is used to start, stop, restart, setup, or check the status of any or all HPCC Systems components.

Examples:

```
sudo /etc/init.d/hpcc-init start
sudo /etc/init.d/hpcc-init stop

sudo /etc/init.d/hpcc-init -c myeclserver start
sudo /etc/init.d/hpcc-init --component=myeclserver start

sudo /etc/init.d/hpcc-init -c esp start
```

HPCC Systems systemd services

HPCC Systems is extending support and development to more systemd services. We intend to continue support for older System V based systems through the hpcc-init.

The hpcc-init system service will support "start", "stop" and "restart" options.

The reporting and logging for HPCC Systems systemd will differ from the previous hpcc-init type. The systemd logs do not have any output to STDOUT/STDERROR, instead it logs to /var/log/syslog. To view the output:

```
journalctl -u <service> -f
```

or

```
sudo systemctl <start|stop|restart> <full_service_name>
```

The systemd displays the service status in its own format.

```
sudo systemctl status <full_service_name>
```

This is different than the output from

```
/etc/init.d/hpcc-init status
```

HPCC Systems services started through systemd will be listed as active in systemd. They can be listed as "sudo systemctl list-units [PATTERN...]". To remove them from the systemd active service list, you must run the stop service from the "service" or "systemctl" commands (as shown above) even though it is already stopped by directly calling /etc/init.d/<hpcc-init|dafilesrv> stop.

HPCC Systems uninstall will automatically remove HPCC Systems services from active list and /etc/systemd/system/ directory.

External Language Support

This section covers the steps to add external language support to the HPCC Systems platform. HPCC Systems offers support for several programming languages, some have additional dependencies that must be installed. External language support is included with the platform installation package, however there are RPM-based HPCC Systems platform installation packages that explicitly state **with plugins**.

RPM-based systems:

If you are interested in using external languages for RPM-based systems (CentOS/Red Hat), you need to download and install the appropriate platform installation distribution **with plugins** option from the downloads site.

For RPM based systems, there are two different installation packages available. One package includes the optional plugins to support embedded code from other languages. If you want support for other languages, choose the package for your distro that begins with:

```
hpccsystems-platform_community-with-plugins-
```

Debian-based systems:

Optional plugin downloads are NOT needed for the Debian-based systems (Ubuntu) installation package, as the plugins are included in all the Debian installation packages.

The external languages currently supported include:

- C++ (full support is already built-in)
- Java
- Python (full support is already built-in)

The following sections detail what is required to utilize these languages in your HPCC Systems platform.

In addition to these languages, you can add support for additional languages by creating your own plugin. This is not very difficult to do. For example the Java plugin is about 500 lines of C++ code. You can use that as a template to write your own and, if desired, you can contribute it back to the open source initiative.

Java

You can run external Java code on the HPCC Systems platform. Compiled Java can be used either as a .class (or a .jar) and called from ECL just like any other ECL function.

To extract the JNI signatures:

```
javap -s
```

To set up Java to integrate with the HPCC Systems platform:

1. Install a Java development package, such as OpenJDK or Oracle Java SE Development Kit (JDK) on the server.
2. Set the Java CLASSPATH

   You can set the classpath several ways:

   - In your profile.
   - In your environment.
   - in your JVM Profile.
   - using classpath value in environment.conf

     The default configuration file for the HPCC Systems platform is **/etc/HPCCSystems/environment.conf** you will need to edit this file to point to your Java build directory.

     For example (on a Linux system):

     ```
     classpath=/opt/HPCCSystems/classes:/home/username/workspace/StreamAPI/bin
     ```

     The classpath should point to your Java build directory.
3. Start the HPCC Systems® platform (restart if it is already running) in order to read the new configuration.

   For example :

   ```
   sudo systemctl start hpccsystems-platform.target
   ```

   For more information see the Starting-and-stopping the HPCC Systems platform in the *Installing and Running The HPCC Systems Platform* document.
4. Test the Java integration.

   The HPCC Systems® platform comes with a Java example class. You can execute some Java code either in your ECL IDE or the ECL Playground.

   For example:

   ```
   IMPORT java;

   integer add1(integer val) := IMPORT(java, 'JavaCat.add1:(I)I');

   add1(10);
   ```

   If this successfully executes, you have correctly set up Java to work with your HPCC Systems platform.

   If you get a "unable to load libjvm.so" error you should reinstall or try a different Java package.

You can call Java from ECL just like any other ECL function. Java static functions can be easily prototyped using ECL types.

Additional examples of Java for HPCC Systems can be found at:

https://github.com/hpcc-systems/HPCC-Platform/tree/master/initfiles/examples/embed

Python

The HPCC Systems platform supports Python3 and the Python3 plug-in is present and enabled. Python2 is no longer supported.

To enable Python support within the HPCC Systems® Platform:

1. Install Python, if not already installed. Many distributions come with Python already installed.

2. You can embed Python natively inside an ECL Program, much like BEGINC++

3. Call Python from ECL as you would any other ECL function.

   Python does not multi-thread efficiently (Global Interpreter Lock). Effectively only one thread can be in the python code at once. Scripts are compiled every call (but with caching of most recent, per thread). The IMPORT case will avoid recompiles.

4. Test the Python integration.

   You can now execute some Python code either in your ECL IDE or the ECL Playground.

   For example:

```
IMPORT Python;

SET OF STRING split_words(STRING val) := EMBED(Python)
  return val.split()
ENDEMBED;

split_words('Once upon a time');
```

   If this successfully executes, you have correctly set up Python to work with your HPCC Systems platform. You can now embed Python anywhere you would use ECL within with your HPCC Systems platform.

   Additional examples of using Python with HPCC Systems code can be found at:

   https://github.com/hpcc-systems/HPCC-Platform/tree/master/initfiles/examples/embed

In order for Python to work properly it is important that the version of Python and HPCC Systems are set up correctly to support using the correct installed version of Python.

Python Scope Options

GLOBALSCOPE - This option allows independent EMBED attributes to share globals with each other if they specify the same name for the GLOBALSCOPE parameter.

PERSIST - This option controls how long such a shared global scope will persist and exactly how far it will be shared.

The value passed to GLOBALSCOPE can be any string you like, allowing you to share globals between related EMBED sections while keeping them distinct from unrelated ones.

PERSIST can take one of the following values:

global - The values persist indefinitely (until the process terminates) and are shared with any other embeds using the same GLOBALSCOPE value, even in other workunits.

query - The values persist until the query is unloaded, and are shared with other instances of the query that might be running at the same time in Roxie, but not with other queries.

workunit - The values persist until the end of the current workunit or the current instance of a Roxie deployed query, and are not shared with other instances.