

Instalando & Executando a Plataforma HPCC Systems®

Equipe de documentação de Boca Raton



Instalando & Executando o HPCC Systems® Platform

Equipe de documentação de Boca Raton

Copyright © 2023 HPCC Systems®. All rights reserved

Sua opinião e comentários sobre este documento são muito bem-vindos e podem ser enviados por e-mail para <docfeedback@hpccsystems.com>

Inclua a frase **Feedback sobre documentação** na linha de assunto e indique o nome do documento, o número das páginas e número da versão atual no corpo da mensagem.

LexisNexis e o logotipo Knowledge Burst são marcas comerciais registradas da Reed Elsevier Properties Inc., usadas sob licença.

SSystems® HPCC Systems® é uma marca registrada da LexisNexis Risk Data Management Inc.

Os demais produtos, logotipos e serviços podem ser marcas comerciais ou registradas de suas respectivas empresas. Todos os nomes e dados de exemplo usados neste manual são fictícios. Qualquer semelhança com pessoas reais, vivas ou mortas, é mera coincidência.

2023 Version 9.0.0-1

Boas Vindas	4
Guia de Introdução	5
Instalação e Inicialização do HPCC System	7
Configuração Inicial-Nó único	9
Configurando um Sistema de Múltiplos Nós	21
Iniciando e Parando	28
Configurando HPCC para Autenticação	30
Manutenção de Segurança do Usuário	45
Configurando o Servidor ESP para utilizar HTTPS (SSL)	87
Configurando SSL para o Roxie	95
Mais Exemplos	98
Exemplos de Anagrama	98
Próximos passos	113
Anexo	114
Scripts de exemplo	114
Desinstalando a plataforma HPCC	122
Aplicações Auxiliares	123
hpcc-init	124
Unity Launcher Icon (Inicializador de Unidade)	126
Executando o ECL IDE pela primeira vez	129
Suporte a Linguagem Externa	130

Boas Vindas

Estas instruções servem como orientação durante a instalação e execução do HPCC¹ Community Edition em um único nó para iniciar e, em seguida, opcionalmente, expandi-lo para um cluster maior de nós.

A tecnologia Thor do HPCC System foi projetada para processar, analisar e localizar links e associações em grandes volumes de dados complexos de forma eficaz. Ela é capaz de detectar relações não óbvias, fazer ajustes para suportar petabytes de dados, e é significativamente mais rápida do que as tecnologias concorrentes – embora exija menos hardware e recursos.

A tecnologia Roxie do HPCC Systems – também conhecida como Rapid Data Delivery Engine or RDDE – usa uma combinação de tecnologias e técnicas que produzem resultados extremamente rápidos para consultas em dados indexados.

Isso é convertido na obtenção de respostas de melhor qualidade e em menos tempo para que as organizações possam lidar com uma quantidade massiva de dados e transformar a informação em conhecimento de maneira eficaz.



Sugerimos a leitura completa deste documento antes de começar. O processo deve levar de uma a duas horas para ser concluído, dependendo da velocidade do seu download.

¹High Performance Computing Cluster (HPCC) é uma plataforma de computação de processamento massivo em paralelo que soluciona problemas de big data. Acesse [o link http://hpccsystems.com/Why-HPCC/How-it-works](http://hpccsystems.com/Why-HPCC/How-it-works) para obter mais detalhes.

Guia de Introdução

Recomendamos dedicar tempo para a leitura completa deste manual; porém, segue abaixo um guia rápido com o resumo das etapas. A plataforma do HPCC System abrange vários aspectos e este guia foi criado para ajudá-lo a usufruir ao máximo de todas as vantagens que o sistema oferece. Esta seção não deve substituir conteúdos mais abrangentes contidos na parte restante deste livro.

1. Instalar o HPCC.

Faça o download o pacote de instalação em <http://hpccsystems.com/download/free-community-edition>.

No CentOS/Red Hat:

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

No Ubuntu/Debian:

```
sudo dpkg -i <deb filename>
```

Então, atualize as dependências:

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

2. Inicie sua plataforma do HPCC Systems

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

NOTA: Nós fornecemos script de exemplos (veja Anexo:Script de Exemplos) para iniciar sistemas maiores com vários nós facilmente.

Usuários de System V, por favor, veja o anexo: hpcc-init.

3. Execute o **ECL Watch**. Valide o seu sistema.

Usando um navegador, vá para o **ECL Watch** executado na porta 8010 do seu Nó do HPCC.

Por exemplo, <http://nnn.nnn.nnn.nnn:8010>, onde nnn.nnn.nnn.nnn é o endereço IP do seu nó.

4. Crie e execute alguns códigos ECL.

Você pode fazer isso diretamente no ECL Watch. No ECL Watch, clique no ícone **ECL** e depois clique no link **Playground**.

5. Acesse <https://hpccsystems.com/download> para obter e instalar o ECL IDE e o Client Tools.

E agora?

Agora que seu HPCC já foi inicializado e está em execução, o que você deseja fazer? Talvez avalie suas necessidades e crie uma configuração customizada que atenda essas necessidades. Talvez você queira expandir seu sistema e adicionar nós. Esses tópicos e muitos outros serão abordados nas seções seguintes.

Para se familiarizar com o que o seu sistema é capaz de fazer, recomendamos realizar as seguintes etapas:

- O **Tutorial de dados do HPCC System**:
- **Exemplo** da Teoria dos seis graus de Kevin Bacon
- Leia **Como usar o Gerenciador de Configurações** para aprender como configurar uma plataforma do HPCC usando o Advanced View.

- Use suas novas habilidades para processar seu próprio dataset massivo!

Instalação e Inicialização do HPCC System

Para começar, siga essas etapas para instalar os pacotes e os componentes de inicialização em uma configuração de nó único. Após ter sido instalado com sucesso, o Gerenciador de Configurações será usado para customizar ou expandir seu sistema.

O Configuration Manager é o utilitário no qual configuramos a plataforma HPCC. Ele é executado em seu Linux Server (servidor Linux) e o acesso à sua interface é feito através de um navegador.

Figure 1. Visão geral do sistema: Thor

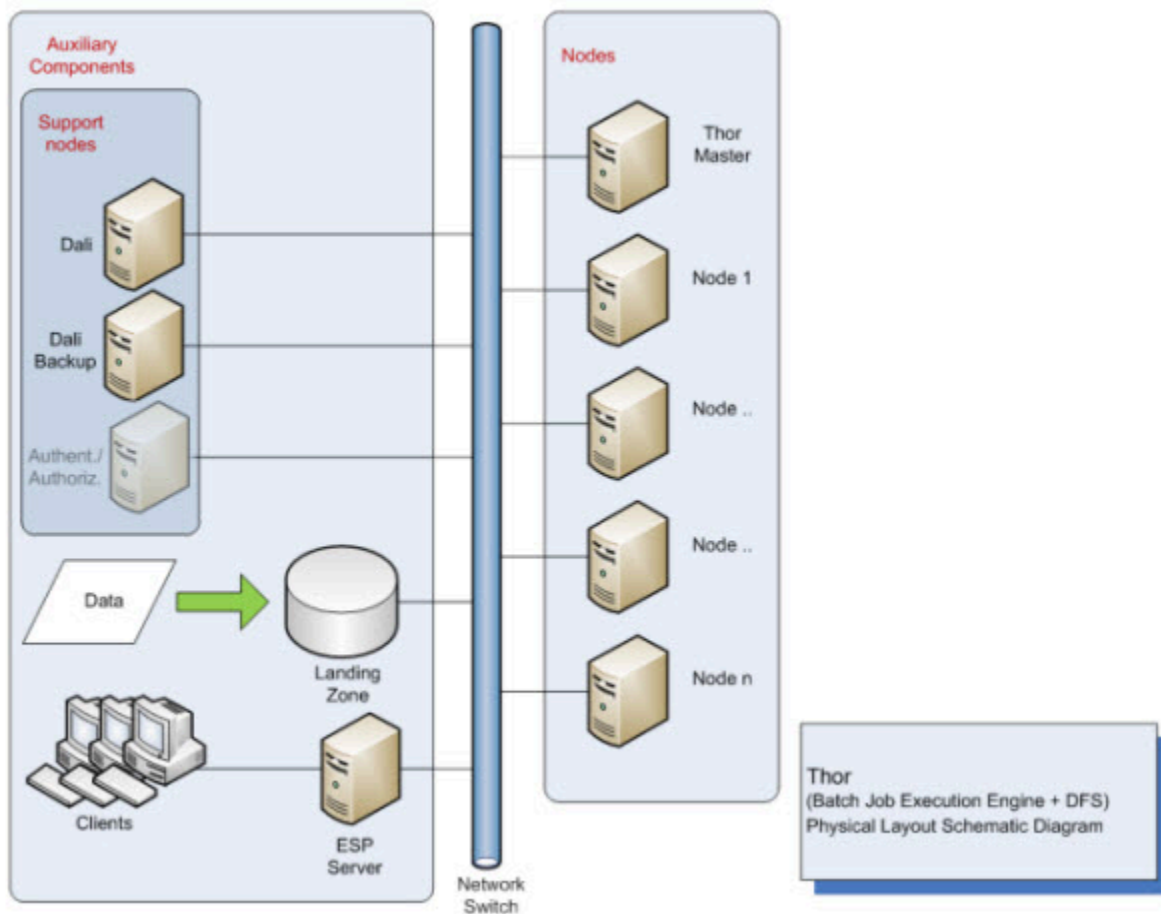
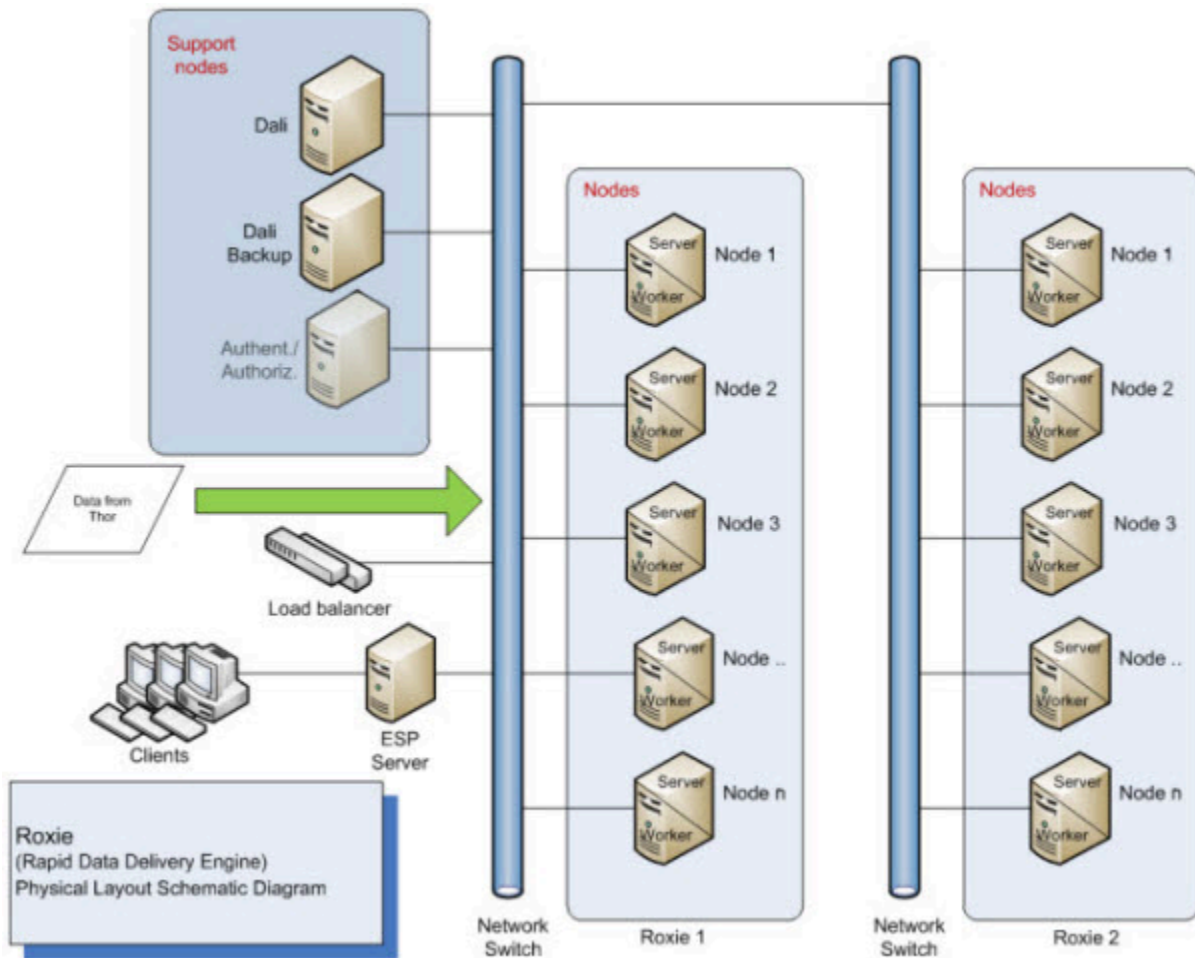


Figure 2. Visão geral do sistema: Roxie



Configuração Inicial-Nó único

Essa seção abrange a instalação do HPCC em um nó único. Isso permitirá que o HPCC System opere com sucesso; porém, a verdadeira força do HPCC é observada quando ele é executado em um ambiente com nós múltiplos e pode alavancar a capacidade de realizar operações usando o Processamento Massivamente Paralelo (MPP).

Além disso, em um sistema de produção, seria necessário dedicar um ou mais nós para cada processo do servidor. Consulte o manual *Como usar o Gerenciador de Configurações* para maiores detalhes.

Instalando o Pacote

A instalação e o pacote que você baixou podem variar conforme o sistema operacional que planeja utilizar. Os pacotes de instalação não serão instalados com sucesso se suas dependências não estiverem presentes no sistema de destino.

Os pacotes estão disponíveis no site do HPCC Systems®: <http://hpccsystems.com/download/>

Para instalar o pacote, siga as instruções apropriadas de instalação:

CentOS/Red Hat

Para instalar a plataforma, você precisa ter a permissão adequada para a instalação de pacotes. Caso tenha perfil de administrador, você poderá instalar as plataformas usando yum.

```
sudo yum install <hpccsystems platform rpm package>
```

Opcionalmente você pode instalar o pacote com rpm (recomendamos utilizar as opções -Uvh); porém, será necessário negociar a instalação de quaisquer dependências adicionais.

Ubuntu/Debian

Um pacote Debian é disponibilizado para instalações Ubuntu. Você deve instalar o pacote, usando o comando:

```
sudo dpkg -i <deb filename>
```

Após instalar o pacote, execute o seguinte para atualizar quaisquer dependências.

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

Plugins

Há vários plugins opcionais que você pode escolher para adicionar à sua instalação.

Para sistemas baseados em RPM, pode ser instalar utilizando yum.

```
sudo yum install <hpccsystems plugin plugin_name>
```

Para instalar plugins opcionais em um pacote Ubuntu/Debian, use:

```
sudo dpkg -i <hpccsystems plugin plugin_name>
```

Os plugins opcionais são:

<ul style="list-style-type: none">• JAVA : javaembed• JavaScript : v8embed• R : rembed• MySql : mysqlembed	<ul style="list-style-type: none">• Kafka : kafka• MemCache : memcached• Redis : redis• SQL Lite : sqlite3embed
---	--

Outras tecnologias, como suporte ao Cassandra e Python estão incluídas no pacote da plataforma.

Primeira Inicialização

1. Inicie o sistema utilizando a configuração padrão.

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



Há arquivos de log para cada componente nos diretórios abaixo **/var/log/HPCCSystems** (local padrão), incluindo o log hpcc-init log para o processo de inicialização. Em caso de falha de inicialização de qualquer componente, esses logs podem ajudar na solução de problemas.

*Informações adicionais sobre o sistema hpcc-init e logs estão na seção Anexos do hpcc-init .

Observação: Se você estiver usando Cent OS 6, Ubuntu 14.04, ou outro sistema baseado em System V, por favor veja Anexo: System V.

Executado um Consuta ECL em seu sistema Nó-Único

Agora que o sistema de nó único está em execução, você pode criar e executar alguns ECL¹ Codifique usando o ECL IDE, o compilador ECL da linha de comando, ou a ferramenta de linha de comando ECL.

Instalar o ECL IDE e o HPCC Client Tools

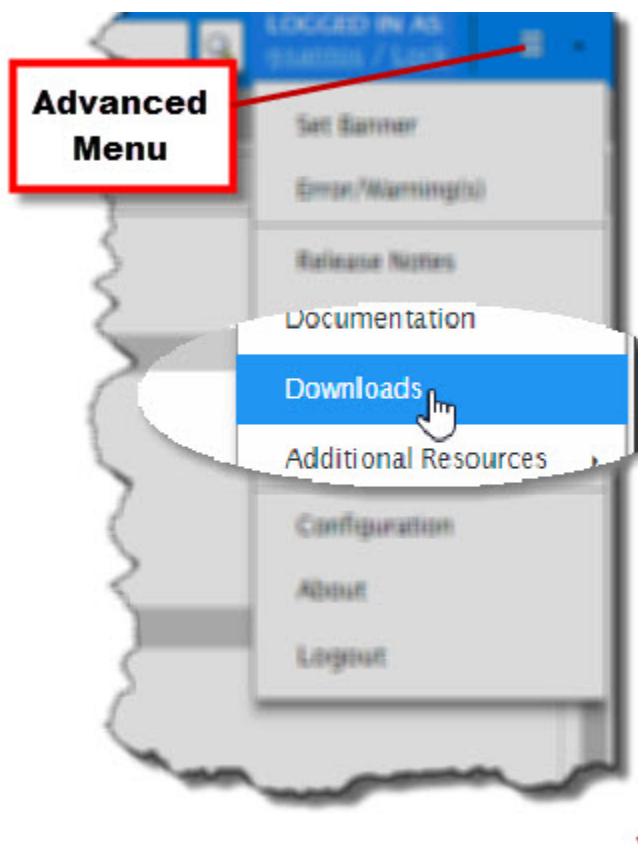
1. Em seu navegador, acesse o URL do **ECL Watch**. Por exemplo, <http://nnn.nnn.nnn.nnn:8010>, onde nnn.nnn.nnn.nnn é o endereço IP do seu nó.



Poderá ser diferente dos endereços fornecidos nas imagens de exemplo. Favor usar o endereço IP do **seu** nó.

2. No menu Avançado do ECL Watch, selecione o link **Download**.

Figure 3. Página de Recursos do ECL Watch



Siga o link para a página do portal de download do HPCC Systems.

Alternativamente, você pode usar seu navegador ou diretamente em <https://hpccsystems.com/download>

3. Siga as instruções na página para fazer o download **ECL IDE e Client Tools para Windows**.

¹Enterprise Control Lenterprise Control Language (ECL) é uma linguagem de programação declarativa e centrada em dados usada para gerenciar todos os aspectos da junção, classificação e compilação de dados massivos que realmente diferenciam o HPCC das demais tecnologias na sua capacidade de fornecer análise de dados flexíveis em escala massiva.

4. Instalar o **ECL IDE e Client Tools para Windows**.

Observação: O ECL IDE funciona somente no sistema operacional Windows.

5. Uma vez o ECL IDE instalado com sucesso, você pode prosseguir.

Executando um programa básico ECL

Agora que o pacote está instalado em seu nó do Linux e o ECL IDE está instalado em sua estação de trabalho Windows, você pode executar seu primeiro programa do ECL. Os programas do ECL podem ser executados localmente ou remotamente. Para tarefas ECL maiores, será preciso segmentar um cluster de máquinas, já que não se pode executar o SO na mesma que a máquina em que você está trabalhando.

Nesta seção, nós usaremos **interface de linha de comando ECL** para que o compilador possa compilar e executar o código ECL localmente.

O compilador ECL (eclcc) é instalado no nós do servidor eclcc quando o pacote é instalado. Isso deve estar em seu "path", para que possa ser executado em qualquer local no servidor. Também é instalado em uma máquina Windows no momento da instalação do ECL IDE. Para compilar e executar no Windows, você também precisará do compilador Visual Studio 2008 C++ (consulte a seção *Requisitos da estação de trabalho do usuário* para obter mais detalhes).

1. Crie um arquivo denominado hello.ecl e digite o texto a seguir (incluindo as aspas):

```
output('Hello world');
```

Você pode usar o editor de sua preferência ou a linha de comando digitando o seguinte

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

2. Compile seu programa usando eclcc adicionando o seguinte comando:

```
eclcc hello.ecl
```

3. Um arquivo executável será criado e poderá ser executado da seguinte maneira:

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

Isso gera o resultado "Hello world" (sem as aspas) para a saída padrão, sua janela de terminal neste exemplo. Você pode redirecionar ou transferir o resultado para um arquivo ou programa desejado. Isso confirma que o compilador está funcionando adequadamente.

Executando Remotamente utilizando as linhas de comando ECL

A aplicação **ECL Command Line Interface (CLI)** aceita parâmetros de linha de comando para enviar diretamente a um mecanismo de execução ECL. Esse utilitário pode ser usado para controlar a criação e execução de jobs ECL maiores que visam um sistema remoto. Para compilar jobs em um sistema remoto, o eclcc é usado para criar um arquivo do código ECL a ser compilado e o ECL CLI é usado para enviá-lo a um cluster de destino, onde será a compilação pelo servidor do compilador remoto (eclccserver).

Para enviar um job usando o ECL CLI, verifique se a plataforma HPCC Systems foi inicializada e use a seguinte sintaxe:

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

O resultado² da workunit é retornado à linha de comando.

Veja detalhes completos da workunit usando a interface do ECL Watch em seu HPCC acessando <http://nnn.nnn.nnn.nnn:8010>, onde nnn.nnn.nnn.nnn é o IP do nó do seu servidor ESP. Busque por uma workunit usando o ID dela ou selecione ECL Workunits/Browse e localize sua tarefa na lista fornecida.

²Uma Workunit é um registro de um trabalho enviado ao HPCC. Ela contém um identificador-- ID da workunit, o código ECL, resultados, e outras informações sobre o job

Definir um arquivo **ecl.ini** facilita a execução da tarefa quando as mesmas configurações são usadas todas as vezes que uma tarefa é enviada dessa forma. Consulte o manual *Ferramentas de cliente do HPCC* para obter mais detalhes.

Se o seu ECL for mais complexo do que um único arquivo de fonte, você pode usar o compilador eclcc localmente para criar um arquivo que será enviado para o eclccServer:

```
eclcc hello.ecl -E | ecl run - --target=thor --server=<Endereço IP do ESP>:8010
```

O parâmetro de destino precisa designar o nome do cluster de destino válido como listado na seção topologia do seu ambiente.

Executando um programa ECL básico do ECL IDE

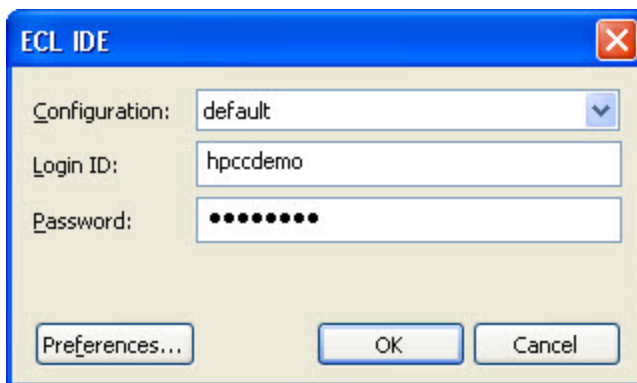
1. Abra o ECL IDE em sua estação de trabalho Windows, a partir do menu Iniciar. (Start >> All Programs >> HPCCSystems >> ECL IDE).



Você pode criar um atalho em sua área de trabalho para acessar rapidamente o ECL IDE.

2. Insira o **ID de Login** e a **Senha** fornecida na caixa de diálogo Login.

Figure 4. Janela de Login



3. Abra uma nova **Janela do compilador** (CTRL+N) e escreva o seguinte código:

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

Isso também poderia ser escrito como:

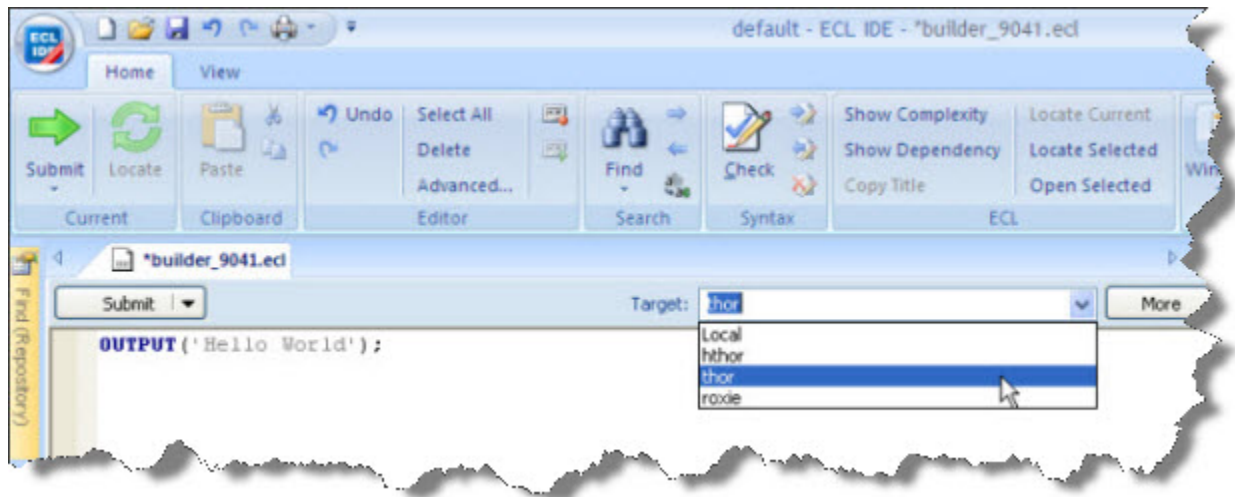
```
'Hello World';
```

Na segunda listagem de programa, a palavra-chave OUTPUT é ocultada. Isso ocorre possivelmente porque a linguagem é declarativa e a ação OUTPUT é implícita.

4. Selecione **thor** como seu cluster de destino.

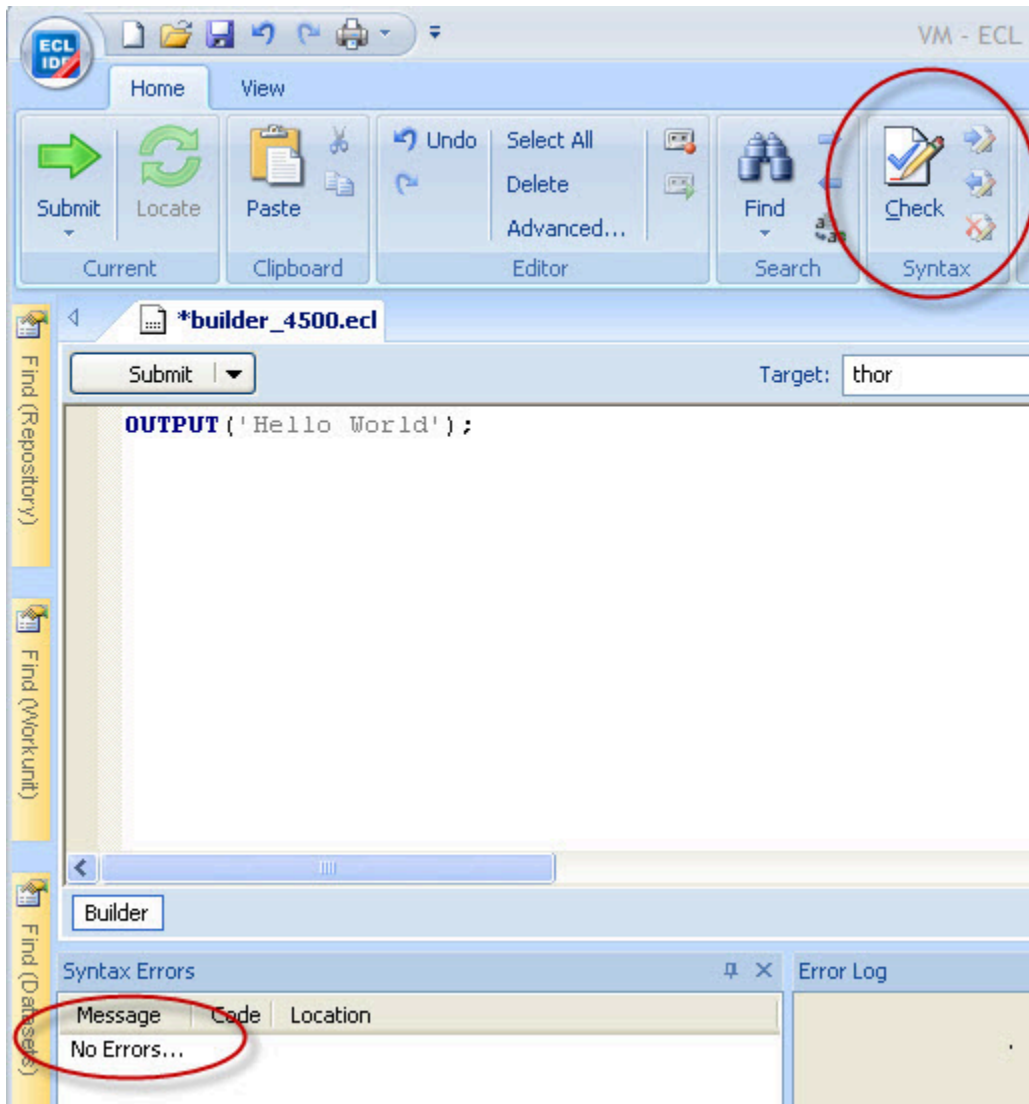
Thor é o componente da Refinaria de dados da plataforma HPCC System. Trata-se de um cluster de computador massivamente paralelo baseado em disco, otimizado para classificar, manipular e transformar uma quantidade massiva de dados.

Figure 5. Selecionar destino



5. Pressione o botão de verificação de sintaxe localizado na barra de ferramentas principal (ou pressione F7).

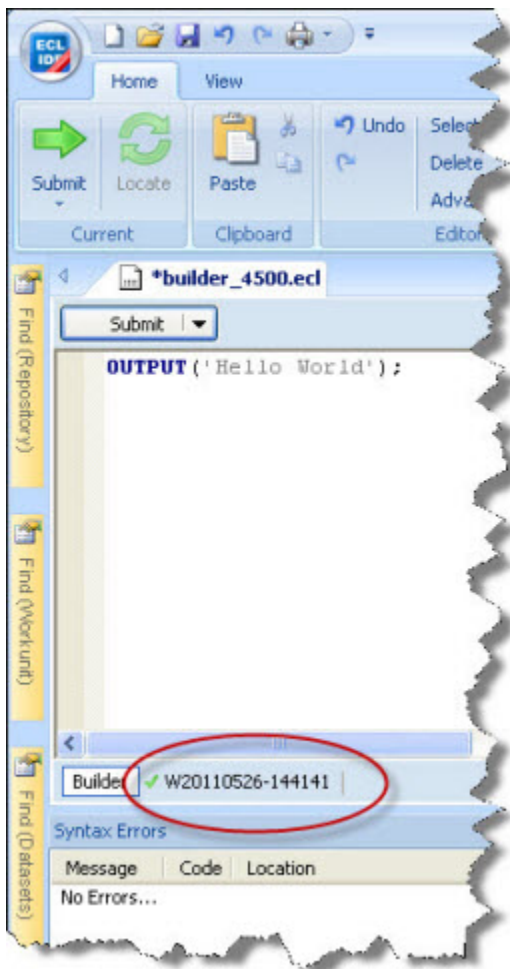
Figure 6. Verificação de sintaxe



Uma verificação de sintaxe bem-sucedida exibe a mensagem “No errors...”.

6. Pressione o botão **Go** (ou as teclas ctrl+enter).

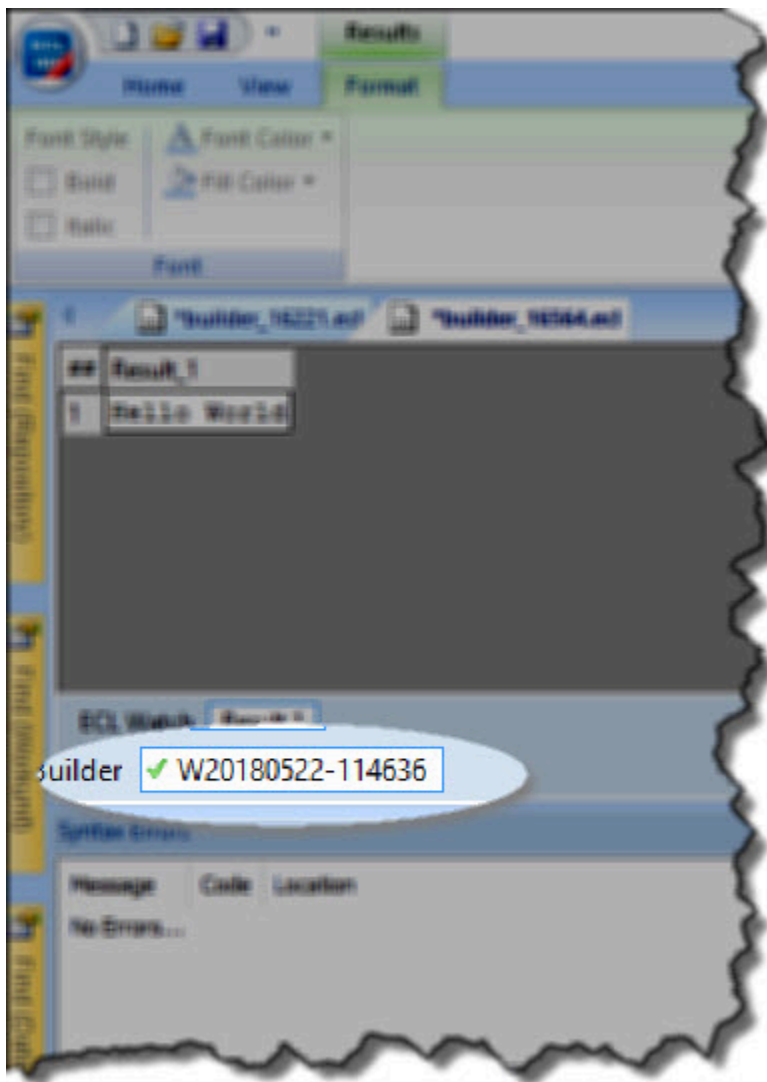
Figure 7. Job Concluído



A marcação na cor verde indica uma conclusão bem-sucedida.

7. Clique na aba do número da workunit para ver os resultados.

Figure 8. Resultado do job concluído



Configurando um Sistema de Múltiplos Nós

Embora o sistema de nó único seja completamente funcional, ele não se beneficia do verdadeiro poder de um HPCC--a capacidade de realizar operações usando o Processamento massivamente paralelo (MPP). Esta seção fornecerá as etapas para expandir seu sistema de nó único para um sistema de vários nós através do assistente do Gerenciador de Configurações.

Para executar um sistema de vários nós, certifique-se de que todos os mesmos pacotes estejam instalados em cada nó. Siga as etapas abaixo para configurar seu sistema de vários nós para obter todos os benefícios do poder de um Processamento massivamente paralelo.

Utilizando o Gerenciador de Configurações

Esta seção detalhará a reconfiguração do sistema para usar vários nós. Antes de iniciar essa seção, você precisa ter baixado os pacotes corretos para sua distro no site do HPCC Systems® website: <https://hpcc-systems.com/download>.

1. Caso esteja em execução, pare o HPCC Systems utilizando este comando:

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



Este comando pode ser usado para confirmar que os processos do HPCC foram interrompidos:

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

2. Inicie o serviço do Gerenciador de Configurações.

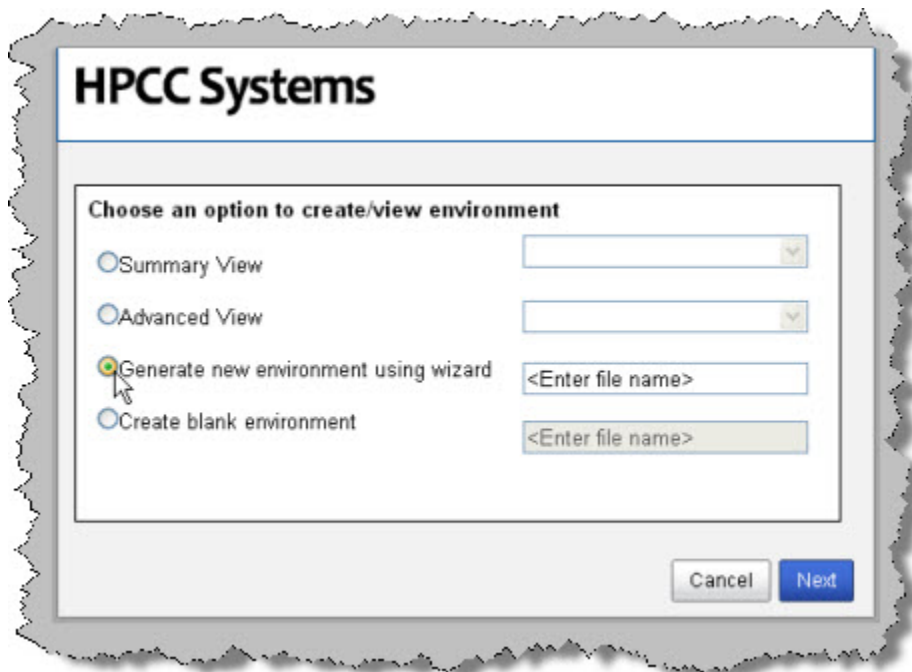
```
sudo /opt/HPCCSystems/sbin/configmgr
```

```
node219008 ~]$ sudo /opt/HPCCSystems/sbin/configmgr
Using default filename /etc/HPCCSystems/source/environment.xml and default port
"8015"
Validating environment file /etc/HPCCSystems/source/environment.xml using config
gen ... Success
Verifying configmgr startup... Success
Exit by pressing ctrl-c...
```

3. Deixe esta janela aberta. Se desejar, você pode minimizá-la.
4. Usando um navegador de Internet, acesse a interface do Gerenciador de Configurações:

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

5. O assistente de inicialização do Gerenciador de Configurações é exibido. Para usar o assistente, selecione o botão Generate novo ambiente usando o assistente.



6. Forneça um nome ao arquivo do ambiente.

Esse será então o nome do arquivo configuration.xml. Por exemplo, nomearemos como *NewEnvironment.xml*.

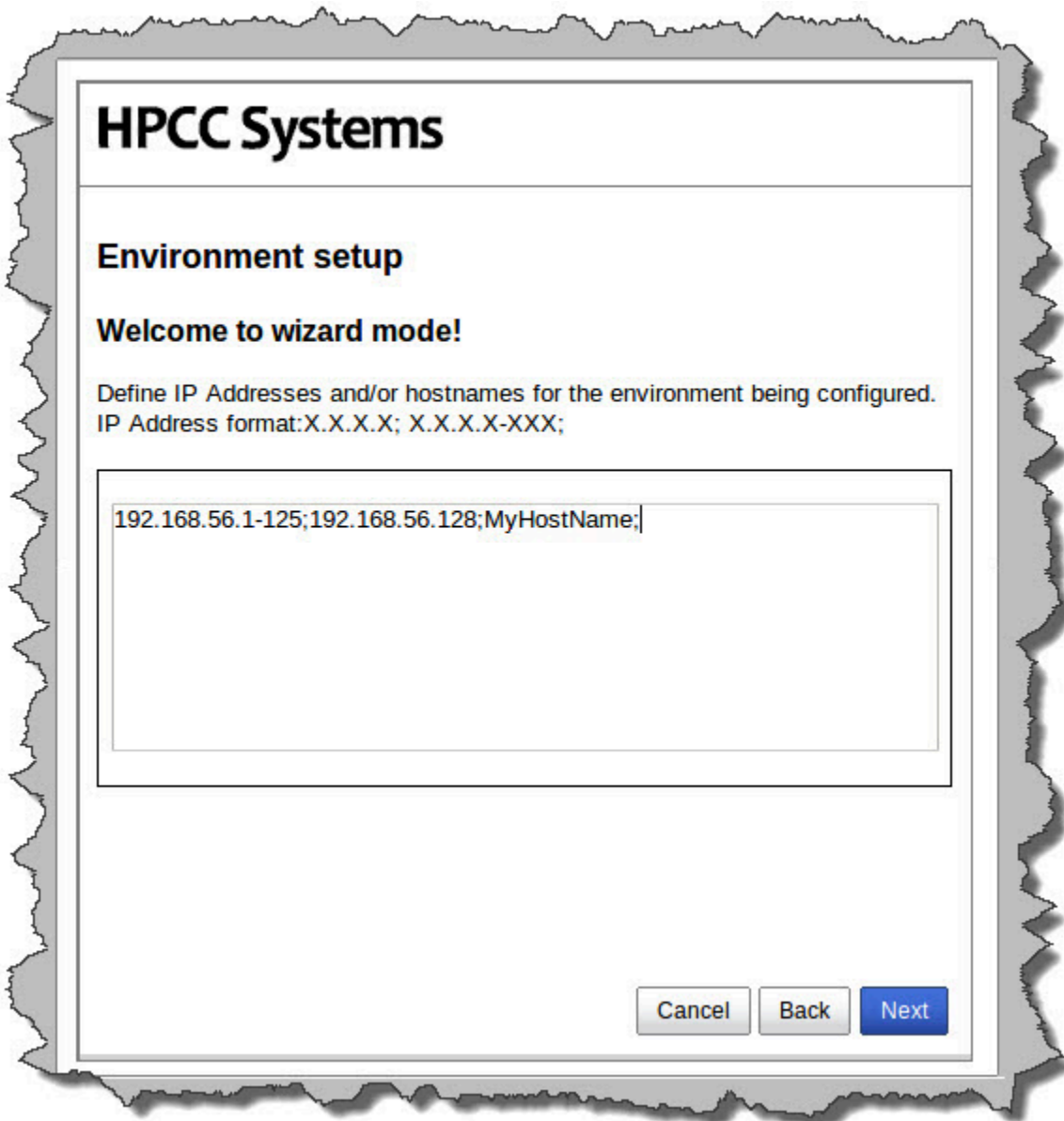
7. Pressione o botão **Next** .

Em seguida, você precisará definir os endereços IP que seu sistema usará.

8. Digite todos os endereços IP que deseja usar no HPCC. Também é possível digitar o(s) nome(s) do(s) host(s).

Os endereços IP não precisam ser contíguos. Na imagem abaixo, especificamos os endereços IP nn.nnn.nnn.1-125 e nn.nnn.nnn.128. Eles são separados com um ponto e vírgula.

Você pode especificar um intervalo de IPs usando um hífen (p.ex.,192.168.55.1-125). Os endereços IP podem ser especificados individualmente usando ponto e vírgula como separadores.



9. Pressione o botão **Next** .

Agora você vai definir quantos nós usar para os clusters Roxie e Thor.

10 Insira os valores adequados conforme indicado.

HPCC Systems

Environment setup

Enter number of nodes for Roxie and Thor clusters. No Roxie/Thor cluster will be generated for zero (0) number of nodes.

Number of support nodes	7
Number of nodes for Roxie cluster	20
Number of slave nodes for Thor cluster (A Thor Master will be added to the cluster and assigned to a support node)	100
Number of Thor slaves per node (default 1)	1
Enable Roxie on demand	<input checked="" type="checkbox"/>

Cancel Back Next

- | | |
|--|---|
| Número de nós de suporte. | Especifique o número de nós a serem usados para os componentes de suporte. O padrão é 1. |
| Número de nós do cluster Roxie: | Especifique o número de nós a serem usados para seu cluster Roxie. Insira zero (0) se você não quiser um cluster Roxie. |
| Número de nós slaves do cluster Thor | Especifique o número de nós slaves a serem usados para seu cluster Thor. Um nó master Thor será adicionado automaticamente. |
| Número de slaves Thor por nó (padrão 1) | Especifique o número de processos slaves Thor para instanciar em cada nó slave. Insira zero (0) se você não quiser um cluster Thor. |
| Ativar o Roxie sob demanda | Especifique se você deseja permitir ou não que as consultas sejam executadas imediatamente no Roxie.(O padrão é true) |

11 Pressione o botão Next

O Resumo do ambiente será exibido.

12. Clique em **Finish** para aceitar esses valores. Esse procedimento salvará o arquivo.

Lembre-se de que as configurações do HPCC podem variar de acordo com as suas necessidades. Por exemplo, você pode não precisar de um Roxie ou de vários clusters Roxie menores. Além disso, em um sistema de produção [Thor] seria necessário assegurar que os nós do Thor e Roxie sejam dedicados e que não contenham nenhum outro processo em execução. Este documento visa mostrar como usar as ferramentas de configuração. Planejamento de capacidade e design de sistema estão disponíveis em um módulo de treinamento.

HPCC Systems

Environment summary for New.xml

Component/Esp Services	BuildSet	Net Addresses/Po
myroxie	roxie	192.168.56.8,192.168.56.10,192.168.56.11,192.168.56.12,192.168.56.13,192.168.56.14,192.168.56.15,192.168.56.17,192.168.56.19,192.168.56.20,192.168.56.21,192.168.56.22,192.168.56.23,192.168.56.24,192.168.56.25,192.168.56.26,192.168.56.27
mydali	dali	192.168.56.2
mydfuserver	dfuserver	192.168.56.3
myeclccserver	eclccserver	192.168.56.5
myesp	esp	192.168.56.1
myeclagent	eclagent	192.168.56.4
		192.168.56.1,192.168.56.2,192.168.56.3,192.168.56.4,192.168.56.5,192.168.56.6,192.168.56.7,192.168.56.8,192.168.56.9,192.168.56.10,192.168.56.11,192.168.56.12,192.168.56.13,192.168.56.14,192.168.56.15,192.168.56.16,192.168.56.17,192.168.56.18,192.168.56.19,192.168.56.20,192.168.56.21,192.168.56.22,192.168.56.23,192.168.56.24,192.168.56.25,192.168.56.26,192.168.56.27

Cancel
Back
Finish
Advanced View

Click and drag to resize

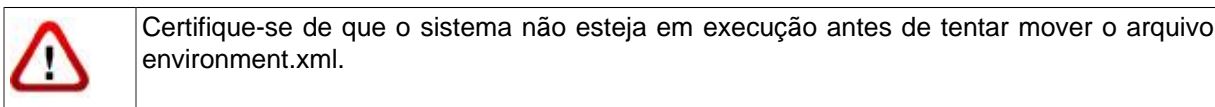
É possível redimensionar o Environment Summary clicando e arrastando o canto inferior direito.

13.Você agora será notificado de que concluiu o procedimento.



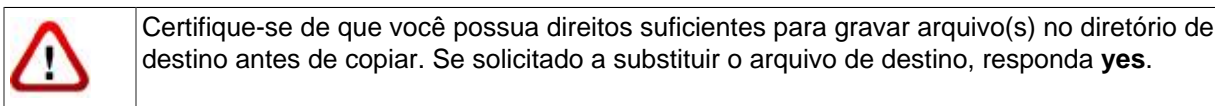
Neste ponto, o sistema criou um arquivo com o nome NewEnvironment.xml no diretório **/etc/HPCCSystems/source** :

14.Pare o Gerenciador de Configurações no terminal em que você o iniciou pressionando as teclas CTRL-C.



15.Copie o novo arquivo NewEnvironment.xml do diretório de origem para /etc/HPCCSystems e renomeie o arquivo para environment.xml

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



16.Se você adicionou novas máquinas no cluster, será necessário copiar e instalar o pacote do HPCC em todos os nós e gerar e clonar as chaves SSH. Isso pode ser feito usando o script install-cluster.sh fornecido com o HPCC. Use o comando a seguir:

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

Onde<package-file-name> é o nome do arquivo do pacote que você deseja instalar em cada nó – isso estará no formato hpccsystems-platform-xxxx-n.n.nnnn.rpm (ou .deb) dependendo da versão e da distribuição. A seção Anexos contém mais detalhes, incluindo outras opções que podem ser usadas com esse comando.

17.Copie o arquivo **/etc/HPCCSystems/environment.xml** para **/etc/HPCCSystems/** em **cada** nó.

Você pode criar um script para forçar o arquivo XML para todos os nós. Um script de amostra é fornecido com o HPCC. Os comandos a seguir copiam os arquivos XML para todos os nós como exigido:

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

Onde o <sourcefile> é o caminho absoluto para o arquivo que deseja copiar, e o <destinationfile> é o caminho absoluto para o arquivo que será gerado. Veja o anexo (Anexo:Scripts de Exemplo) para maiores informações utilizando esse script.

18 Reinicie o HPCC Systems em **todos** os nós. O comando a seguir inicia o HPCC System em um nó individual:

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



Você pode usar um script para lançar esse comando para todos os nós. Um script de amostra é fornecido com o HPCC Systems. Use o comando a seguir para iniciar o HPCC em todos os nós:

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

Esse script também pode ser usado para parar o HPCC Systems em todos os nós e para iniciar e parar componentes individuais em todos os nós. Veja o anexo (Anexo:Scripts de Exemplo) para maiores detalhes.

Informação adicional sobre chave SSH

No HPCC Systems com vários nós, os certificados e as chaves SSH devem corresponder em todos os nós para o sistema funcionar corretamente. Se você usou script *install-cluster.sh*, conforme descrito nas etapas acima, isso garantirá que tudo esteja corretamente sincronizado. No entanto, ainda é uma boa idéia verificar se está tudo sincronizado. Outra maneira de garantir isso é usar o script *hpcc-push.sh* entregue. Por exemplo, os seguintes comandos enviariam o certificado, chave e chave pública para todos os hosts definidos no ambiente.

```
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
```

Veja o anexo (Anexo:Scripts de Exemplo) para maiores informações ao utilizar esse script.

Atualizar SSH Keys

Você poderá atualizar o rotacionar suas SSH keys. Nós recomendamos utilizar o script fornecido para instalação ou atualização das SSH Keys. Veja o anexo (Apêndice:Scripts de Exemplo) para maiores informações sobre utilizar esse script.

Iniciando e Parando

Início, Parar, Reiniciar o Sistema

Após ter definido o ambiente do seu sistema, o comando **init** pode ser usado para iniciar, parar ou reiniciar componentes.

Os seguintes comandos podem ser usados:

Para iniciar o sistema:

Para iniciar a plataforma HPCC Systems use o seguinte comando;

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

Para CentOS 6 ou outro sistema baseado em System V veja Anexo: hpcc-init.

Para parar o sistema:

Para parar sua plataforma HPCC Systems use o seguinte comando;

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

Para CentOS 6 ou outro sistema baseado em System V veja Anexo: hpcc-init.



Você pode usar um script para iniciar o parar múltiplos nós no sistema. Veja *Scripts de Exemplo* na sessão Anexos.

Iniciar ou Parar um Único Componentes

Para iniciar ou parar um único componente, use a flag -c no init system como segue.

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

Para parar um único componente,

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

Para CentOS 6 ou outro sistema baseado em System V veja Anexo: hpcc-init.

Iniciar ou Parar o Gerenciador de Configurações

Configure o sistema como desejar usando o Gerenciador de Configurações.

1. Caso esteja em execução, pare o HPCC Systems usando este comando em **cada** nó:

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

2. Inicie o serviço do Gerenciador de Configurações em um nó (geralmente o primeiro nó é considerado como o nó principal e é usado para esta tarefa, mas isso fica a seu critério).

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

3. Usando um navegador de Internet, acesse a interface do Gerenciador de Configurações:

`http://<ip de instalação do sistema>:8015`

Configurando HPCC para Autenticação

Esta seção detalha as etapas para configurar a plataforma HPCC a usar autenticação. Atualmente existem algumas formas de usar a autenticação em seu HPCC Systems: autenticação simples htpasswd, LDAP, ou outro método de segurança de plugin.

O método de autenticação htpasswd constitui na autenticação simples da senha. Ele concede ou nega acesso a um usuário apenas com base na autenticação de senhas criptografadas por MD5.

Autenticação LDAP oferece mais recursos e opções. LDAP é capaz de autenticar usuários e de adicionar granularidade à autenticação. LDAP permite controlar acessos agrupados a recursos, funções e arquivos.

Você deve levar em conta as necessidades do seu sistema na hora de decidir qual desses métodos é o mais adequado para seu ambiente.



Ao implementar qualquer forma de autenticação, recomendamos ativar seu servidor ESP a usar HTTPS (SSL) e a configurar TODAS as conexões do serviço a usarem apenas HTTPS. Isso garante que as credenciais sejam transmitidas pela rede usando a criptografia SSL **Veja Como configurar o ESP Server para usar HTTPS (SSL)** para obter mais informações.

Não se deve tentar isso até que o ambiente a ser usado já tenha sido implementado, configurado e certificado.

Utilizando autenticação htpasswd

O modelo htpasswd oferece a autenticação simples de senhas para todo o sistema. Esta seção contém informações de instalação e de implementação do modelo de autenticação htpasswd.

Conectar ao Configuration Manager

Para alterar a configuração para os componentes do HPCC, conecte-se ao Configuration Manager.

1. Pare todos os componentes do HPCC se estiverem em execução.
2. Verifique se eles não estão mais sendo executados. É possível usar um único comando, como:

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

3. Inicie o Gerenciador de Configurações.

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

4. Conecte seu navegador de Internet à interface da Web do Gerenciador de Configurações.

(usando o URL `http://<configmgr_IP_Address>:8015`, onde `<configmgr_IP_Address>` é o endereço IP do nó que está executando o Configuration Manager)

5. Selecione o botão de opção **Advanced View**.
6. Use a lista suspensa para selecionar o arquivo de configuração XML adequado.

Observação: O Configuration Manager **nunca** atua no arquivo de configurações ativo. Após terminar a edição, será necessário copiar o arquivo `environment.xml` para o local ativo e forçá-lo a todos os nós.

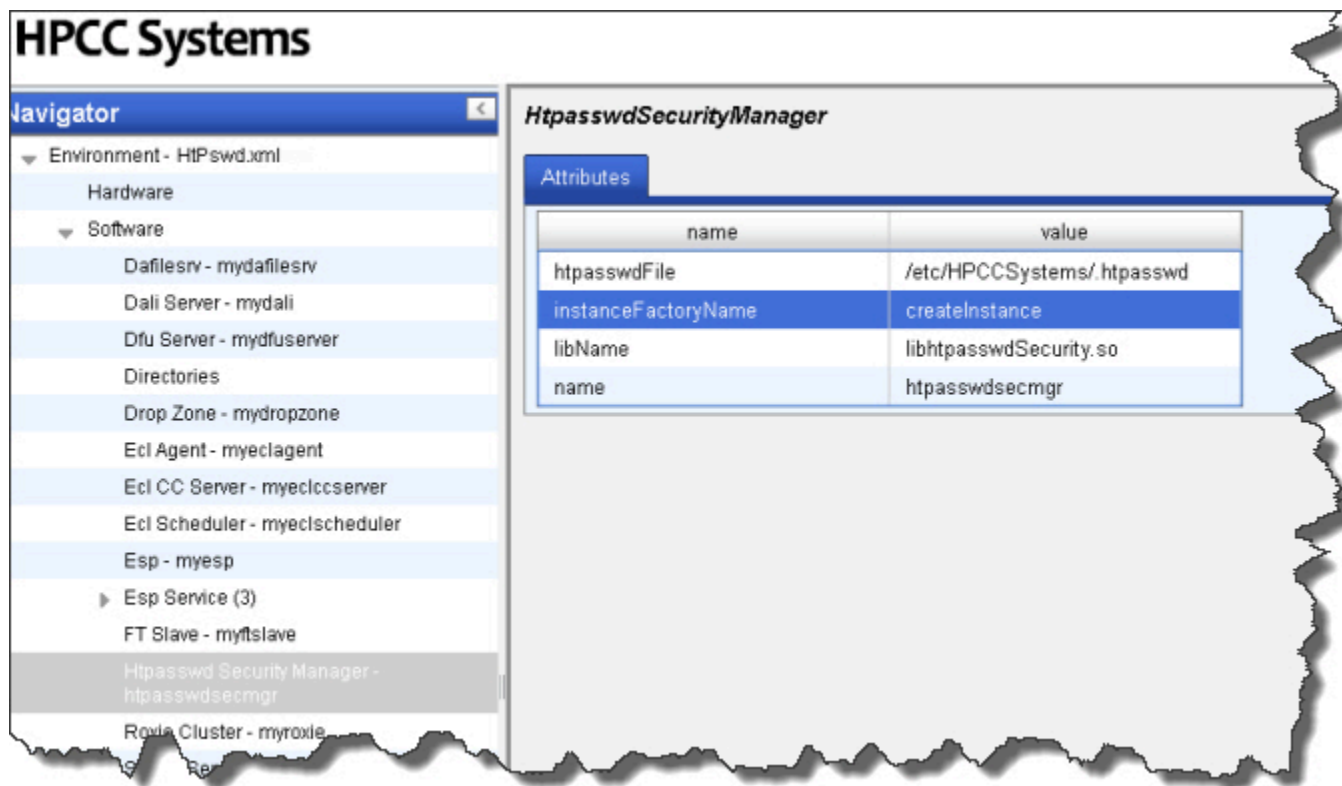
7. Marque a caixa de seleção **Write Access**.

O acesso padrão é somente leitura. Muitas opções estão disponíveis apenas quando o acesso à gravação estiver ativado.

Habilitando a autenticação htpasswd no HPCC

8. Crie uma instância do **Security Manager** Plugin:
 - a. Clique com o botão direito no Pannel de navegação ao lado esquerdo.
 - b. Selecione **New Components**.
 - c. Selecione o componente **htpasswdsecmgr**.
9. Configure o plugin do htpasswd

Figure 9. Página “Security Mgr Configuration” (Configuração do Security Manager)



- a. Digite a localização do arquivo Htpasswd que contém o nome do usuário e a senha no sistema de arquivos Linux para **htpasswdFile**
- b. **InstanceFactoryName** é o nome da função de fábrica do gerenciador de segurança implementado na biblioteca de segurança. O padrão é "createInstance". Use o padrão na implementação do método Htpasswd.
- c. Forneça um nome da biblioteca para **libName**. Para Htpasswd, use [libhtpasswdSecurity.so](#)
- d. Forneça um nome da instância para o valor **nome**. Por exemplo, [htpasswdsecmgr](#).

10. Selecione **Esp - myesp** no painel do navegador ao lado esquerdo.

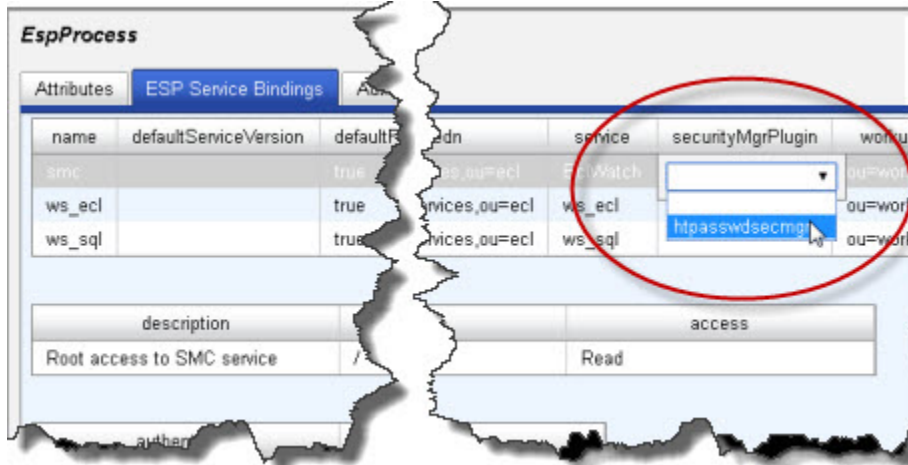
Observação: Se tiver mais de um ESP Server, use apenas um deles para autenticação.

11. Associe o Security Manager Plugin às conexões do ESP.

a. Clique no **Esp** de destino no painel do navegador ao lado esquerdo.

b. Selecione a **aba de conexões do ESP Service**

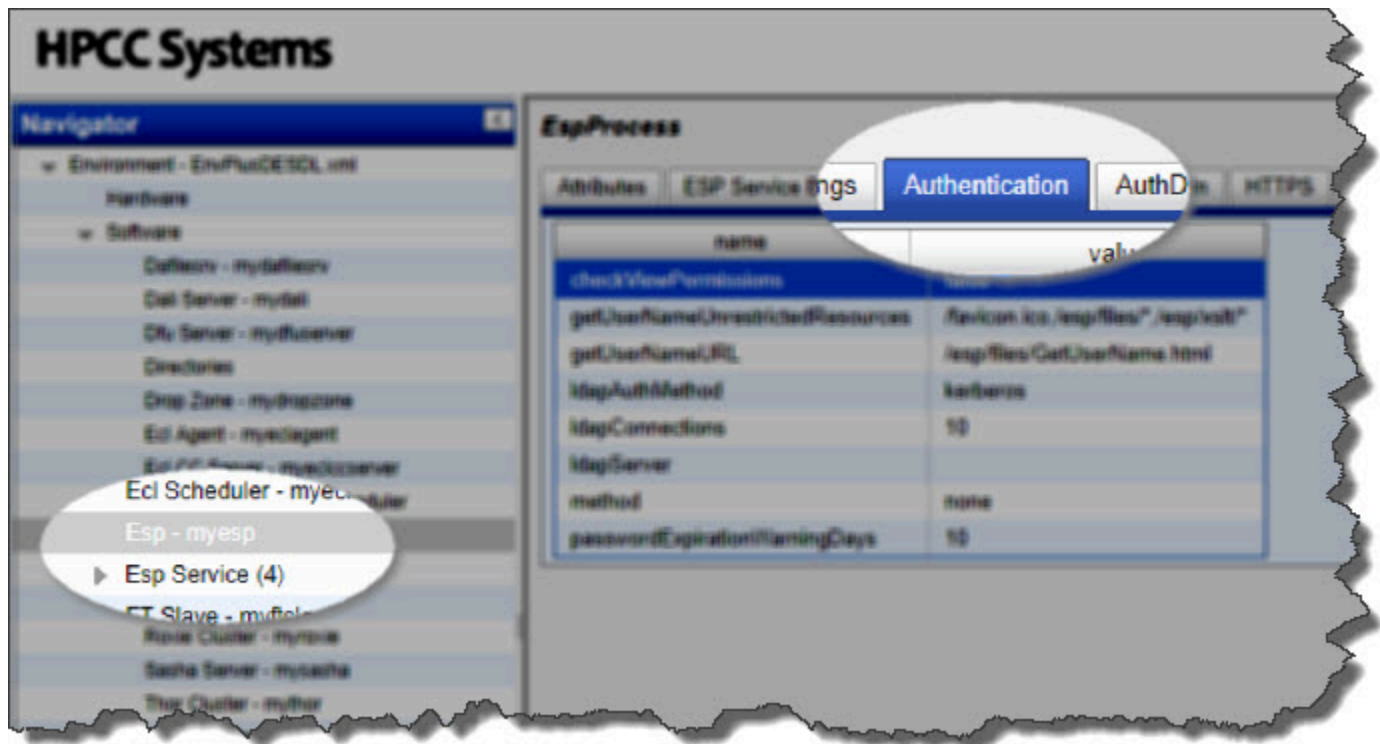
c. Nas ligações de destino, selecione a instância securityMgrPlugin adequada a partir da lista suspensa.



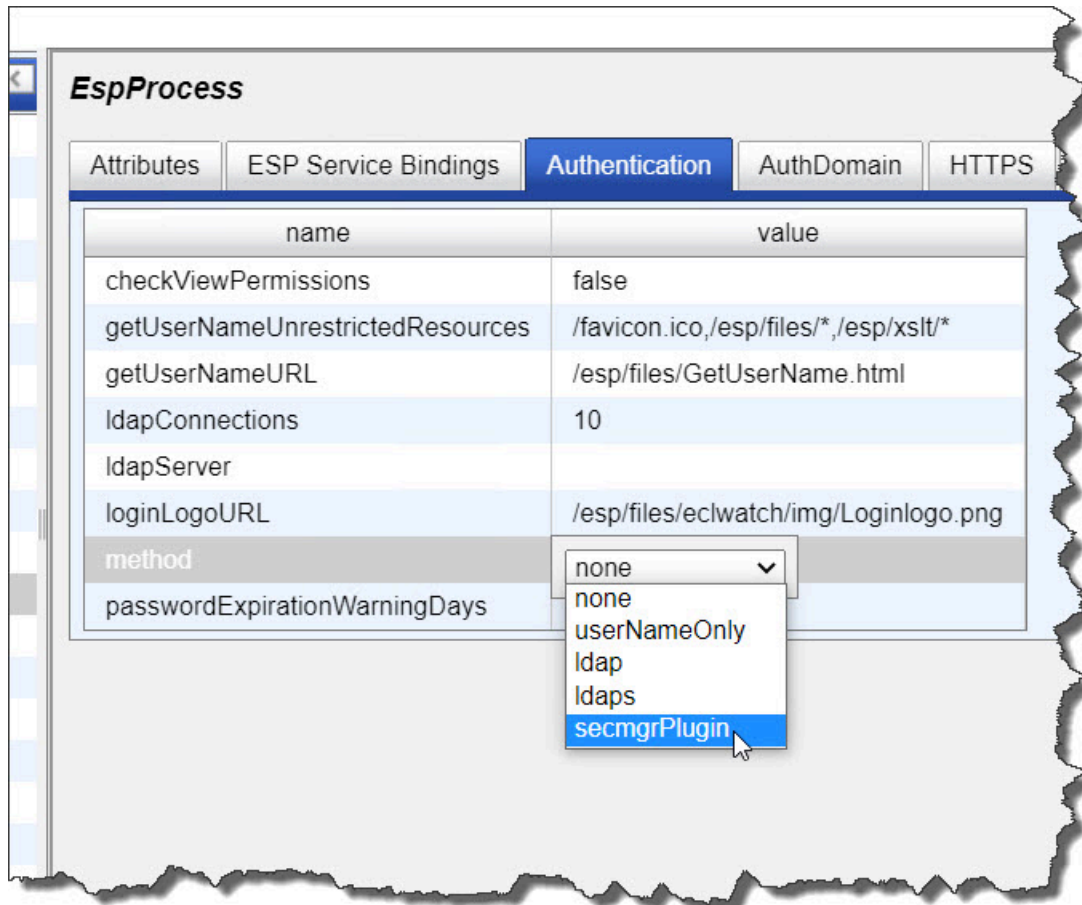
12. Selecione um plugin de segurança para cada serviço que exija um gerenciador de segurança.

Por exemplo, na imagem acima selecione [httpasswdsecmgr](#) para o serviço smc. Em seguida, selecione para ws_ecl e para qualquer outro serviço que deseja usar a segurança httpasswd.

13. Selecione a aba **Authentication**.



14. Clique na lista suspensa da coluna para exibir as opções do **method**.



15. Selecione **secmgrPlugin** na lista suspensa.

16. Clique no ícone de disco para salvar.

Usuário administrador com htpasswd

Usuários e senhas são mantidos no arquivo `htpasswd`. O arquivo `htpasswd` deve existir no nó do ESP onde a autenticação está habilitada. HPCC apenas reconhece senhas criptografadas em MD5.

O local padrão é: `/etc/HPCCSystems/.htpasswd` no nó do ESP configurado para autenticação, porém pode também ser configurado no Gerenciador de segurança do Htpasswd como destacado acima (etapa 9).

Você pode usar o utilitário do `htpasswd` para criar um arquivo de extensão `.htpasswd` para administrar usuários.

Pode ser que o utilitário do `htpasswd` já esteja instalado em seu sistema, uma vez que ele faz parte de alguns sistemas Linux. Verifique seu sistema Linux para ver se o utilitário já está instalado. Se não tiver, baixe o utilitário para seu sistema no The Apache Software Foundation.

Para obter mais informações sobre como usar o `htpasswd` acesse: <http://httpd.apache.org/docs/2.2/programs/htpasswd.html>.

Utilizando Autenticação LDAP

Esta seção contém informações de instalação e de implementação da autenticação baseada em LDAP. A autenticação LDAP oferece o maior número de opções para proteger o seu sistema ou partes de seu sistema. Além dessas definições de configuração, você precisa executar o utilitário **initldap** para criar o usuário padrão Admin do HPCC requerido em seu servidor LDAP.

Se optar por usar a autenticação LDAP, você precisa habilitar o LDAP security em sua configuração do HPCC System. Com a função LDAP security habilitada em seu sistema, você pode optar por ativar a segurança do escopo de arquivos. Há a opção de usar a autenticação LDAP sem habilitar a segurança do escopo de arquivos. As seções a seguir descrevem como habilitar a autenticação LDAP e a segurança do escopo de arquivos em seu HPCC System.

Conectar-se ao Configuration Manager

Para alterar a configuração para os componentes do HPCC, conecte-se ao Configuration Manager.

1. Pare todos os componentes do HPCC se estiverem em execução.
2. Verifique se eles não estão mais sendo executados. É possível usar um comando único, como:

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

3. Inicie o Gerenciador de Configurações.

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

4. Conecte à interface Web do Configuration Manager.

(usando o URL `http://<configmgr_IP_Address>:8015`, where `<configmgr_IP_Address>` é o endereço IP do nó que está executando o Configuration Manager)

5. Selecione o botão de opção **Advanced View**.
6. Use a lista suspensa para selecionar o arquivo de configuração XML adequado.

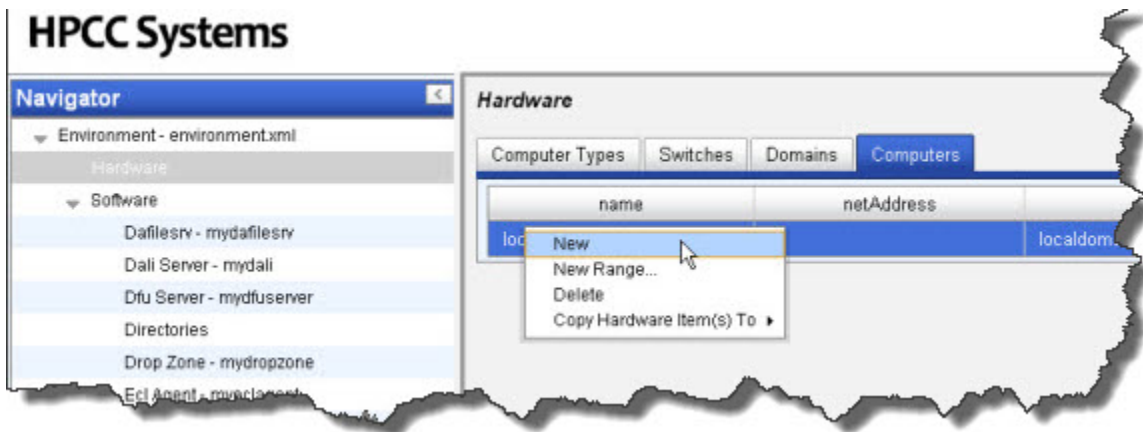
Observação: O Configuration Manager **nunca** atua no arquivo de configurações ativo. Após terminar a edição, será necessário copiar o arquivo `environment.xml` para o local ativo e distribuí-lo a todos os nós.

Modificando a Configuração

Siga as etapas abaixo para modificar sua configuração.

1. Marque a caixa de seleção **Write Access**.
2. No painel do **Navigator**, selecione **Hardware**.
3. Selecione a aba **Computers** no painel à direita.

4. Clique com o botão direito na tabela abaixo de computers e selecione a opção **New** no menu pop-up.



A caixa de diálogo **Add New Computers** será exibida.

5. Preencha a área de **Computer Attributes**

- a. Forneça um **Name Prefix**, como por exemplo: **ldap**.

Isso ajudará a identificá-lo na lista de computadores.

- b. Preencha as informações de **Domain** e **Type** com o nome do seu domínio e os tipos de máquinas que você está usando.

No exemplo acima, o **Domain** é **localdomain**, e o **Type** é **linuxmachine**. Estes devem corresponder ao seu domínio e tipo.

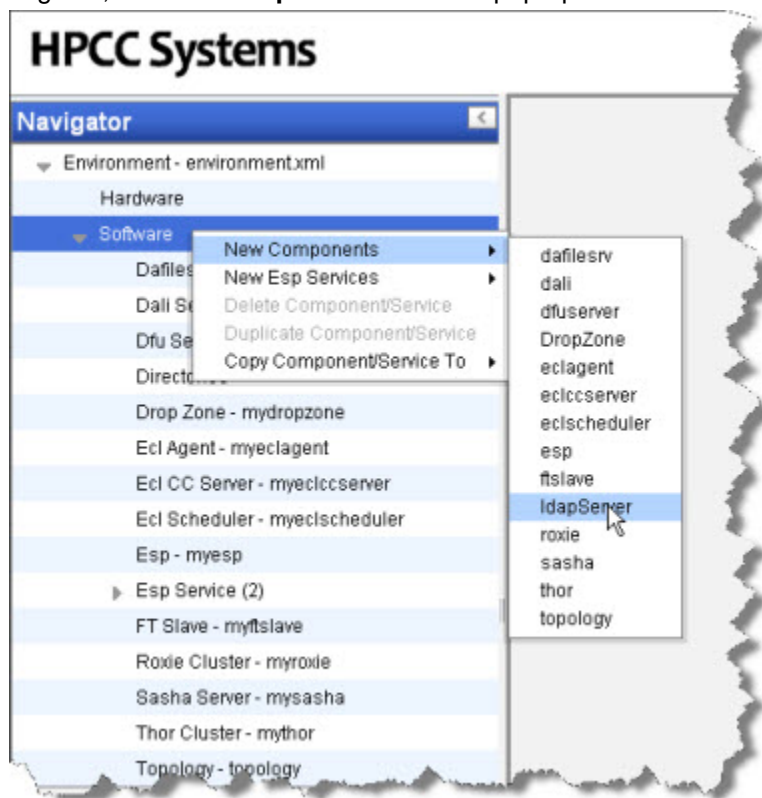
Se for preciso adicionar um novo domínio ou tipo de máquina ao seu sistema para poder definir um servidor LDAP existente, primeiramente é necessário configurar isso nas outras duas abas na seção Hardware.

- c. Adicione o endereço IP como apropriado para o servidor LDAP.
- d. Pressione o botão **Ok**.
- e. Clique no ícone de disco para salvar.

Adicionando o componente IdapServer

Após o nó do LDAP Server ter sido adicionado às configurações de Hardware, configure a definição de Software do servidor LDAP.

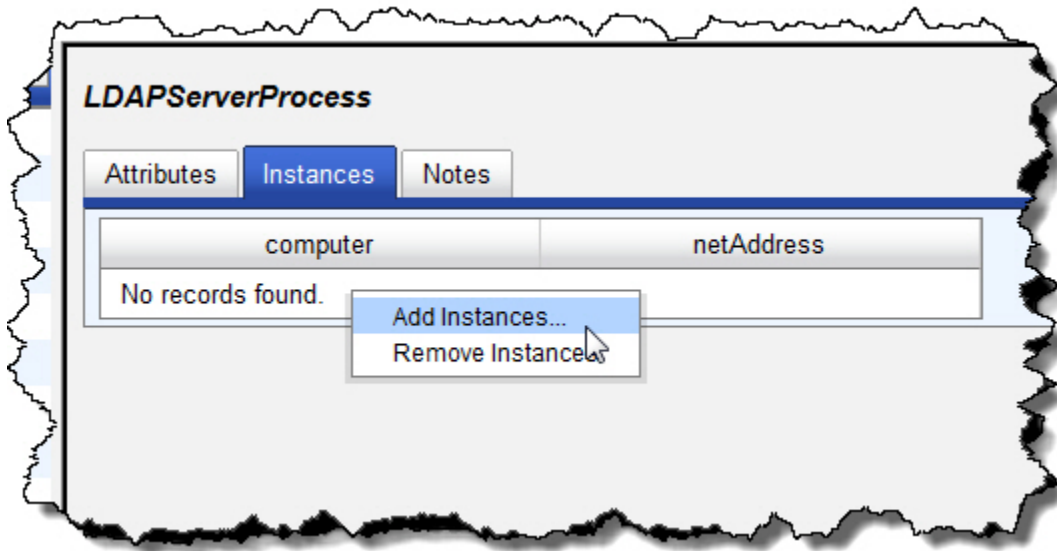
1. Clique com o botão direito no painel **Navigator** e selecione **New Components** no menu pop-up; em seguida, selecione **IdapServer** no menu pop-up.



Observação: O componente IdapServer é meramente uma definição que especifica um servidor LDAP existente. Ele não instala um servidor.

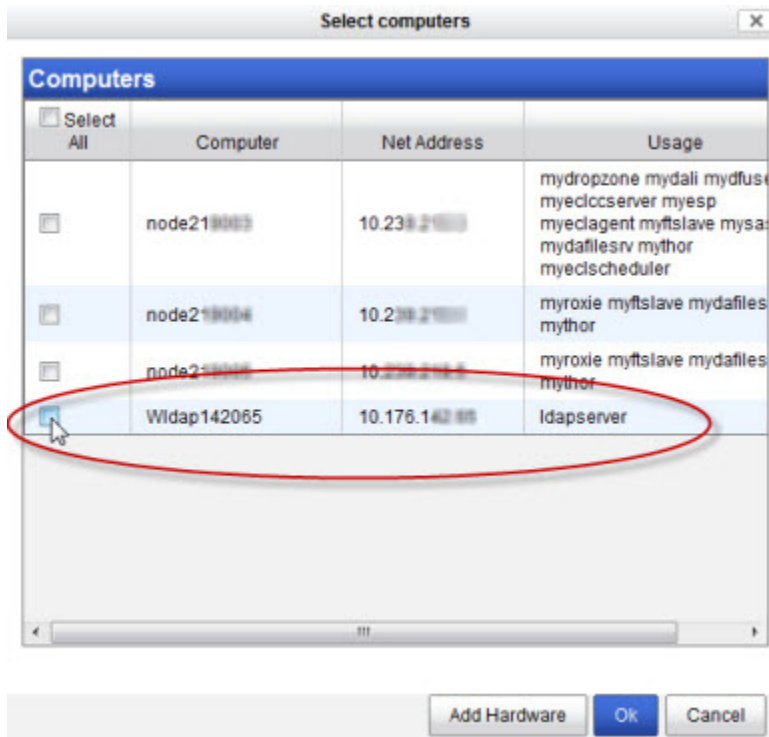
2. Preencha as **propriedades do LDAP Server Process**:

- a. Na aba **Instances** , clique com o botão direito na tabela à direita e selecione **Add Instances...**



A caixa de diálogo **Select Computers** aparecerá.

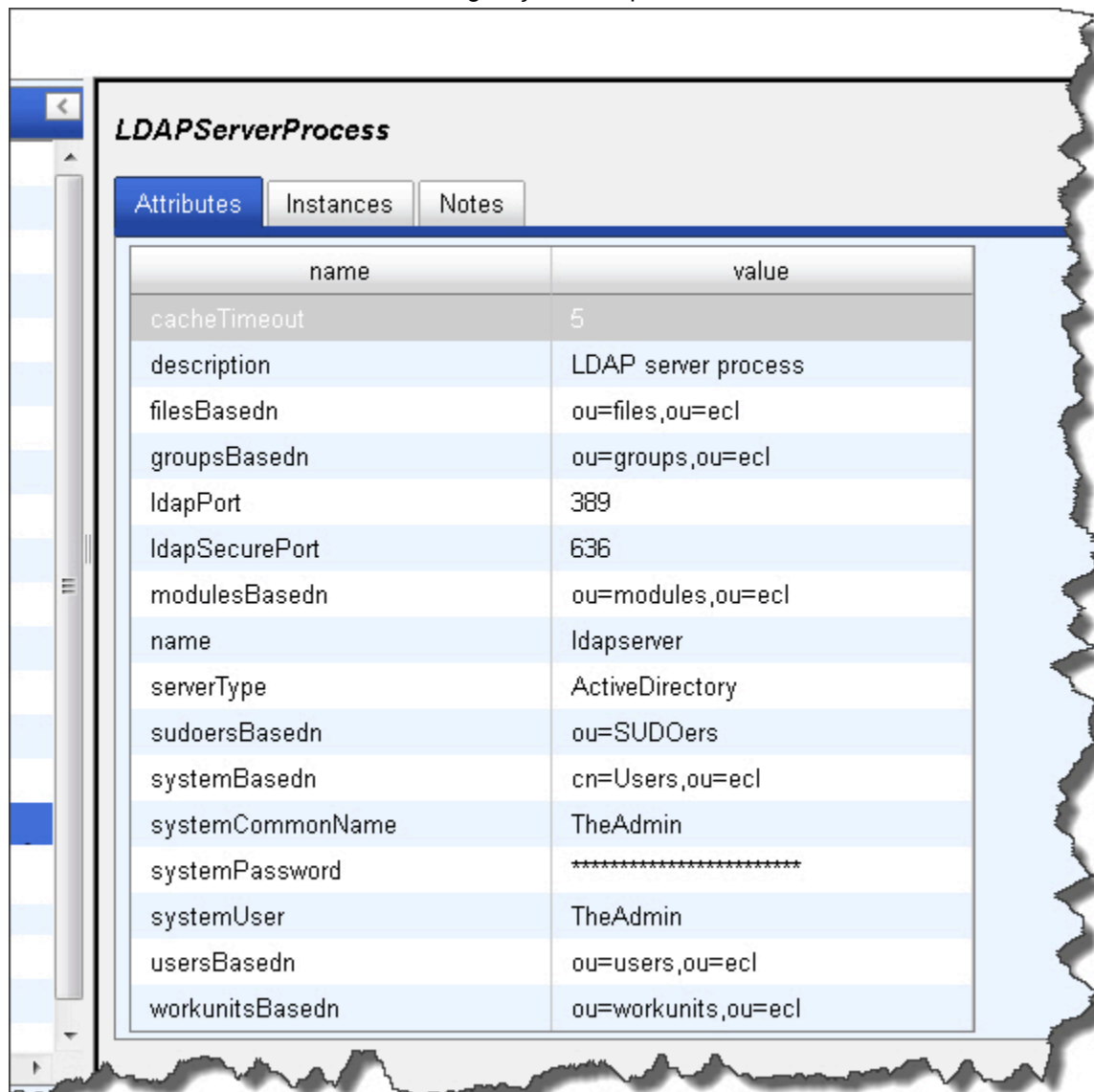
- b. Selecione o computador a ser usado clicando na caixa ao lado dele.



Este é o computador que foi adicionado anteriormente na parte **Hardware / Add New Computer** .

- c. Pressione o botão **OK** .

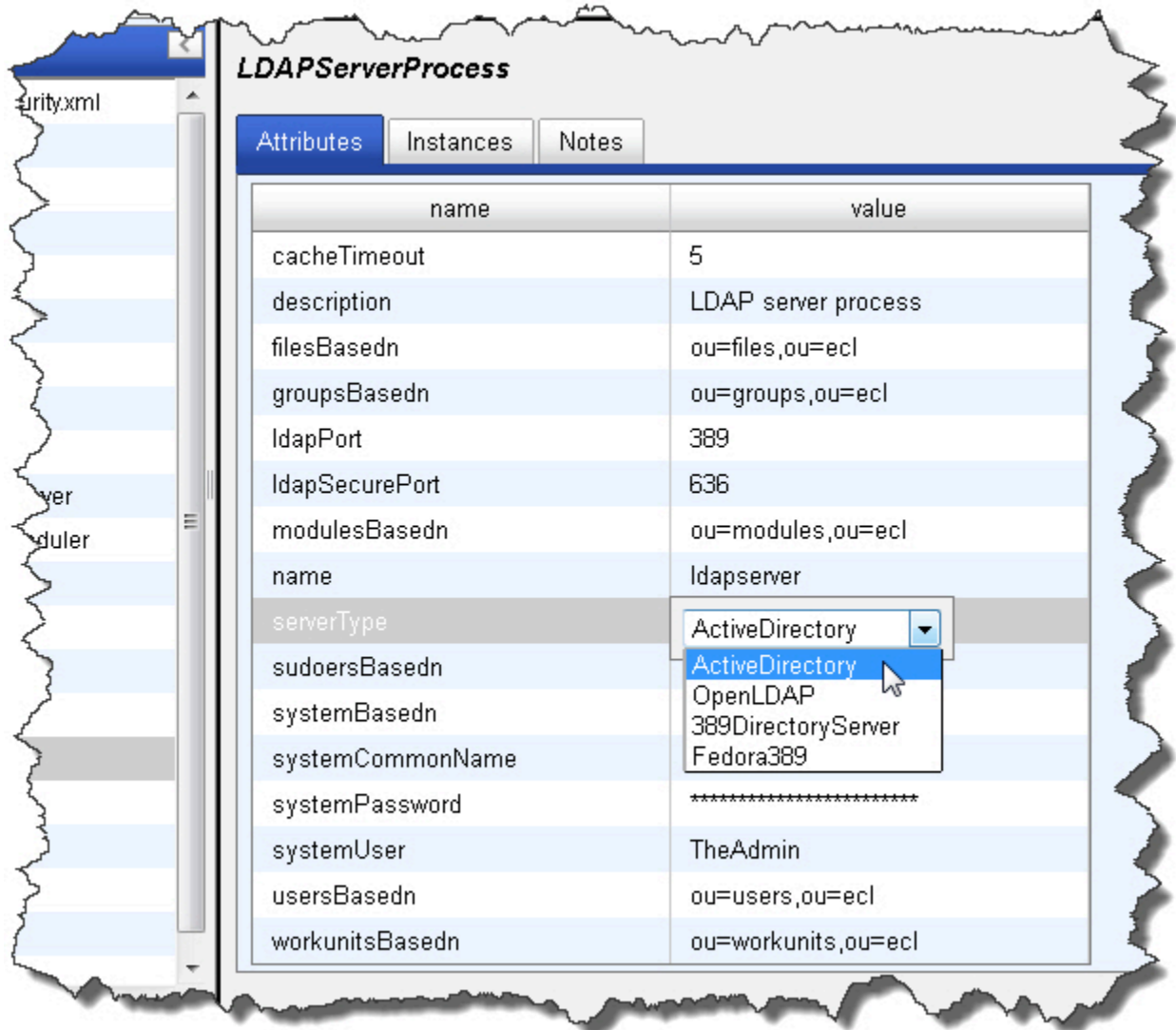
d. Preencha a aba **Attributes** com as configurações adequadas de seu LDAP Server existente.



The screenshot shows a configuration window titled "LDAPServerProcess". It has three tabs: "Attributes" (selected), "Instances", and "Notes". Below the tabs is a table with two columns: "name" and "value". The table contains the following entries:

name	value
cacheTimeout	5
description	LDAP server process
filesBasedn	ou=files,ou=ecl
groupsBasedn	ou=groups,ou=ecl
ldapPort	389
ldapSecurePort	636
modulesBasedn	ou=modules,ou=ecl
name	ldapserver
serverType	ActiveDirectory
sudoersBasedn	ou=SUDOers
systemBasedn	cn=Users,ou=ecl
systemCommonName	TheAdmin
systemPassword	*****
systemUser	TheAdmin
usersBasedn	ou=users,ou=ecl
workunitsBasedn	ou=workunits,ou=ecl

e. Selecione tipo de servidor LDAP no atributo serverType da caixa suspensa.



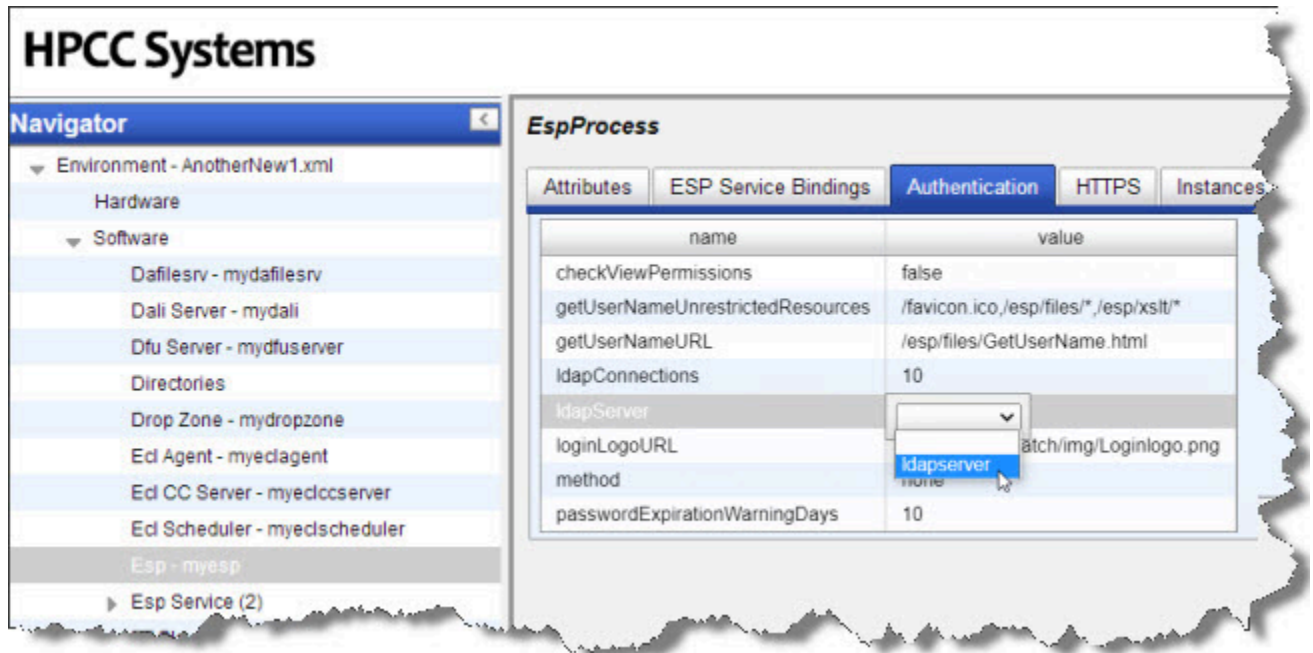
OBSERVAÇÃO: O suporte para OpenLDAP foi descontinuado. Esta opção foi incluída apenas para necessidades legadas.

f. Clique no ícone de disco para salvar.

Observação: O valor do **cacheTimeout** corresponde ao número de minutos em que as permissões estão em cache no ESP. Ao alterar qualquer permissão no LDAP, as novas configurações não estarão em vigor até que o ESP e o Dali atualizem. Isso pode demorar a mesma quantidade de tempo do cacheTimeout. A definição disso para 0 significa sem cache, porém sobrecarrega o desempenho, assim não deve ser usado em produção.

3. No painel do navegador, clique em **ESP -- myesp**

4. Na página **EspProcess** ao lado direito, selecione a aba **Authentication** .

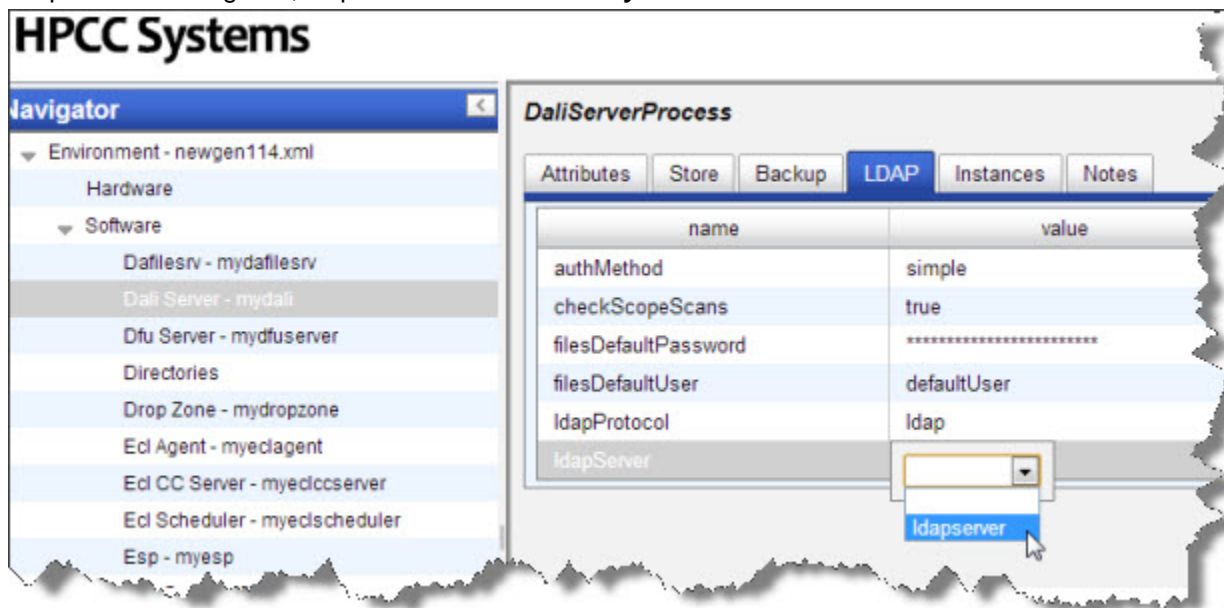


Preencha as informações adequadas:

- Altere o **ldapConnections** para o número adequado ao seu sistema (o número 10 é apenas um exemplo).
- Selecione o componente **ldapServer** adicionado anteriormente da lista suspensa, por exemplo: [ldapserver](#).
- Altere a informação do **método** para [ldap](#).
- Selecione a aba **ESP Service Bindings**. Certifique-se de que as configurações do LDAP apareçam em **resourcesBasedn** e **workunitsBasedn**
- Clique no ícone de disco para salvar.

5. Para habilitar as permissões do escopo de arquivos, realize a configuração no servidor Dali.

No painel do navegador, clique em **Dali Server -- mydali**



Preencha com as informações apropriadas:

- Selecione a aba **LDAP**.
- Altere o **authMethod** para **simple (simples)**
- Defina o **checkScopeScans** para **true (verdadeiro)**.

Defina esse campo para “true” apenas quando quiser habilitar a segurança do escopo de arquivos. As configurações de segurança podem ter três estados.

- Nenhum, sem autenticação e sem segurança do escopo de arquivos.
- LDAP segurança apenas para autenticação, sem habilitar a segurança do escopo de arquivos.
- LDAP autenticação e segurança do escopo de arquivos habilitados.

- Altere as informações do LDAP como apropriado para que correspondam às configurações do componente de seu servidor LDAP no Configuration Manager.

Exemplo: altere o **ldapServer** para o mesmo valor do seu LDAP Server. Ness caso, o valor é: *ldapserver*.

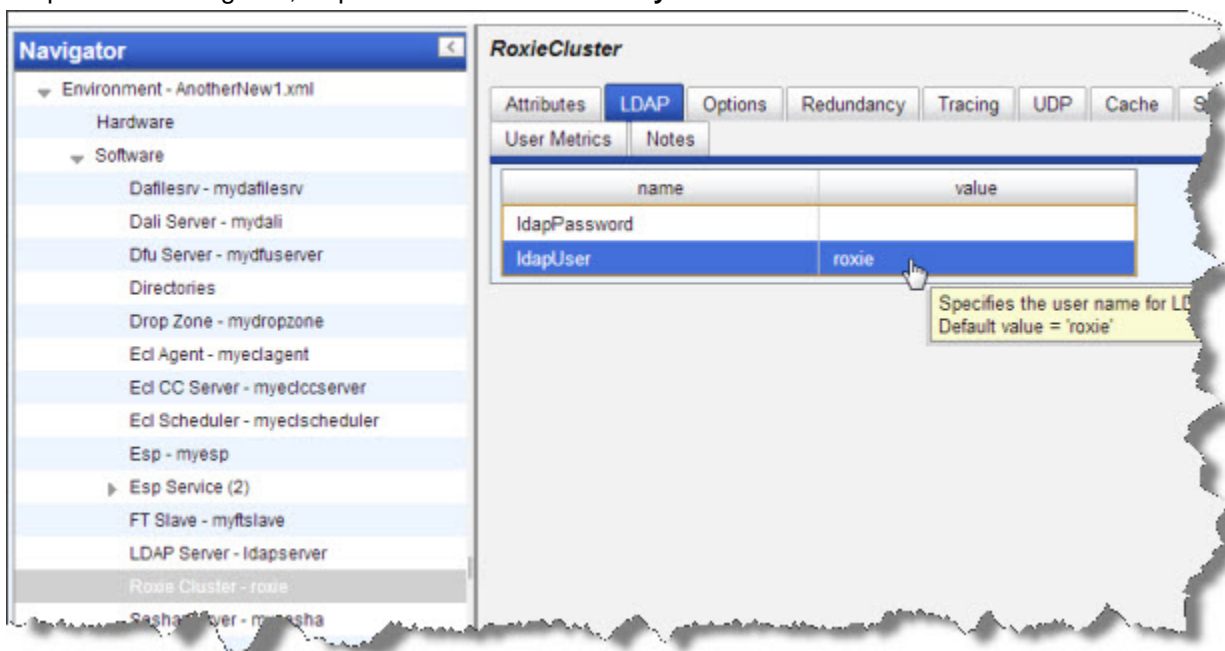
Confirme a alteração quando solicitado.

O **filesDefaultUser** é uma conta do LDAP usada para acessar arquivos quando nenhuma não há nenhuma credencial. É semelhante a conta “convidado”, por isso deve ter acesso **bastante** limitado em seu uso. Deixe o **filesDefaultUser** em branco para desabilitar esse tipo de acesso.


O **filesDefaultPassword** corresponde a senha dessa conta.

- Clique no ícone de disco para salvar

6. No painel do navegador, clique em **Roxie Cluster -- myroxie**



- Na página **RoxieCluster** ao lado direito, selecione a aba **LDAP**.
- Localize o campo **ldapUser** e verifique se há um usuário válido do HPCC que seja membro do grupo de Usuários autenticados em seu servidor LDAP. Por exemplo, o usuário "roxie" assume que usuário "roxie" é um usuário autenticado válido do HPCC.
- Adicione a segurança de senha para Roxie, adicionando-a ao campo **ldapPassword** na mesma guia.



Para executar consultas no Roxie através da segurança do escopo de arquivos, verifique se um usuário do Roxie foi criado na lista de usuários autenticados.

Na seção seguinte, *Adicionar e editar usuários*, adicione o usuário *roxie* e verifique se a senha é a mesma que foi inserida no Configuration Manager.

Instalando o usuário de Admin padrão

Após habilitar suas configurações do LDAP Security, é preciso copiar seu arquivo de ambiente para o diretório `/etc/HPCCSystems`. Ver a seção *Como configurar um sistema de múltiplos nós* para obter mais informações sobre como configurar seu sistema. Com o arquivo `environment.xml` correto em vigor, é preciso executar o utilitário **initldap** para inicializar os componentes de segurança e os usuários padrão.

O utilitário initldap

O utilitário **initldap** cria a conta de usuário de Administrador do HPCC e as OUs do HPCC para um servidor LDAP recém-definido. O utilitário **initldap** extrai essas configurações dos componentes do LDAP Server no `environment.xml` ligado aos ESPs configurados.

Você pode executar o utilitário **initldap** após ter concluído a configuração com componentes do LDAP ativados e depois de ter distribuído o arquivo `environment.xml` para todos os nós.

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

O utilitário **initldap** solicitará as credenciais de administrador do LDAP. Insira os valores apropriados quando solicitado.

Segue abaixo um exemplo de initldap na implementação do 389DirectoryServer.

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

Utilizando a ferramenta addScopes

Quando uma nova conta de usuário do ESP é criada, um escopo de arquivo privado "hpccinternal::<user>" também é criado concedendo aos novos usuários o acesso total àquele escopo e acesso restrito aos outros usuários. Este escopo de arquivo é usado para armazenar temporariamente arquivos do HPCC como os arquivos de despejo e temporário.

Se você estiver habilitando a segurança do escopo de arquivos do LDAP e já tiver contas de usuários, execute o programa de utilitário addScopes para criar um escopo hpccinternal::<user> para esses usuários existentes.

Usuários que já pertençam a esse escopo são ignorados o que permite o uso seguro dessa solução tanto em contas de usuários ESP novas como pré-existentes.

A ferramenta está localizada na pasta **/opt/HPCCSystems/bin/** e, para executá-la, é preciso especificar a localização do **daliconf.xml**, por exemplo:

```
/opt/HPCCSystems/bin/addScopes /var/lib/HPCCSystems/mydali/daliconf.xml
```

Execute o addScopes no nó do Dali.

Manutenção de Segurança do Usuário

Configurar o HPCC System para usar o Active Directory ou segurança baseada em LDAP permite definir permissões para o controle de acesso aos Recursos, Escopo de arquivos e Escopos da Workunit.

Introdução

HPCC systems® preserva sua segurança de diversas formas. HPCC Systems® pode ser configurado para gerenciar os direitos de segurança dos usuários direcionando para o Active Directory da Microsoft no sistema Windows ou para o 389Directory Server no sistema Linux.

Ao usar a interface Permissões no ECL Watch, os administradores podem controlar o acesso aos recursos no ECL IDE, ECL Watch, ECL Plus, DFU Plus, e nos módulos ECL no atributo Repositório. Você também pode optar por implementar o controle de acesso a arquivos e workunit habilitando essa configuração no servidor Dali.

Estabeleça as permissões por grupo ou por usuário e determine-as por associação com um recurso específico do HPCC System. As permissões podem ser determinadas para cada combinação única de um grupo e de um recurso. As permissões são divididas entre as seguintes categorias:

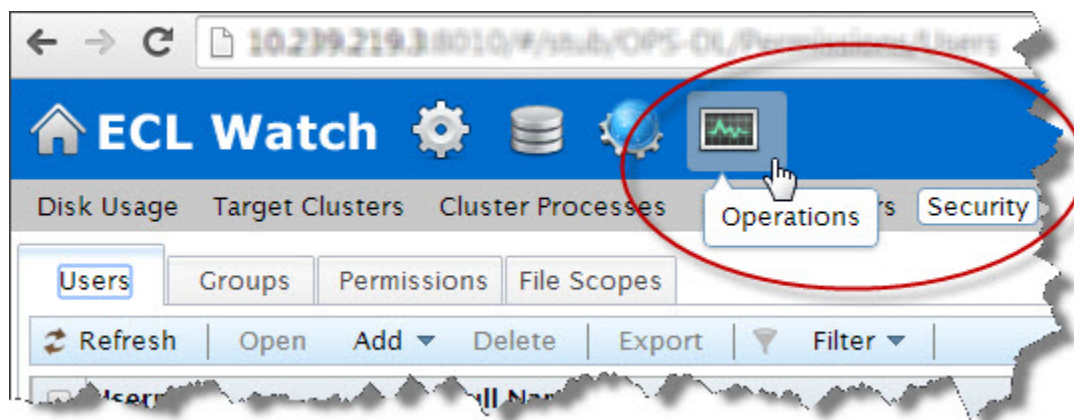
Esp Features for SMC	Controla o acesso a recursos no ECLWatch e a recursos similares acessados a partir do ECL IDE.
Esp Features for WsEclAccess	Controla o acesso ao serviço Web WS-ECL
Esp Features for EcIDirectAccess	Controla o acesso ao serviço Web do ECLDirect
File Scopes	Controla o acesso aos arquivos de dados aplicando permissões aos escopo de arquivos
Workunit Scopes	Controla o acesso às workunits aplicando permissões aos Escopos de tarefa
Repository Modules	Controla o acesso ao atributo Repositório e aos módulos no repositório (antigo)

Administração de Segurança utilizando o ECL Watch

É preciso ter direitos de administrador para administrar as permissões. Após obter direitos de administrador, abra o ECL Watch em seu navegador usando o seguinte URL:

- **http://nnn.nnn.nnn.nnn:pppp** (onde nnn.nnn.nnn.nnn é o endereço IP do seu ESP Server e pppp é a porta. A porta padrão é 8010).

A administração da segurança é controlada através da área **Security** do ECL Watch. Para acessar a área de Security, clique no ícone **Operations**, e em seguida clique no link **Security** a partir do submenu de navegação.



As três áreas nas quais as permissões devem ser definidas são:

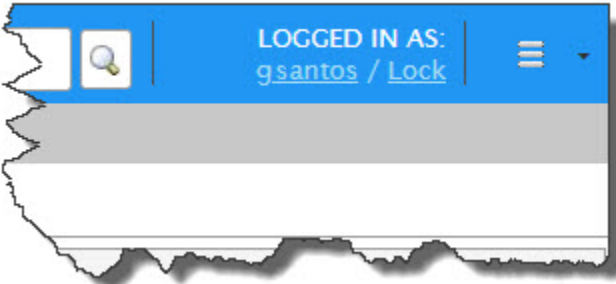
- **Users.** Mostra a configuração atual de todos os usuários. Use esta área para adicionar ou remover um usuário, editar as informações do usuário, definir/redefinir a senha do usuário e visualizar as permissões que estão atualmente atribuídas para o usuário.
- **Groups.** Mostra a configuração atual de todos os grupos. Use esta área para adicionar ou remover um grupo, visualizar e editar os membros do grupo, visualizar e editar as permissões que foram determinadas para o grupo.
- **Permissions.** Mostra os recursos do HPCC System onde as permissões devem ser determinadas. Use esta área para visualizar as permissões atualmente determinadas para qualquer área do HPCC System, para adicionar grupos e usuários e para definir ou modificar permissões em relação a um recurso específico.



OBSERVAÇÃO: É preciso ter cautela ao determinar qualquer configuração de permissão para **negar um direito**. A permissão mais restritiva sempre se aplica.

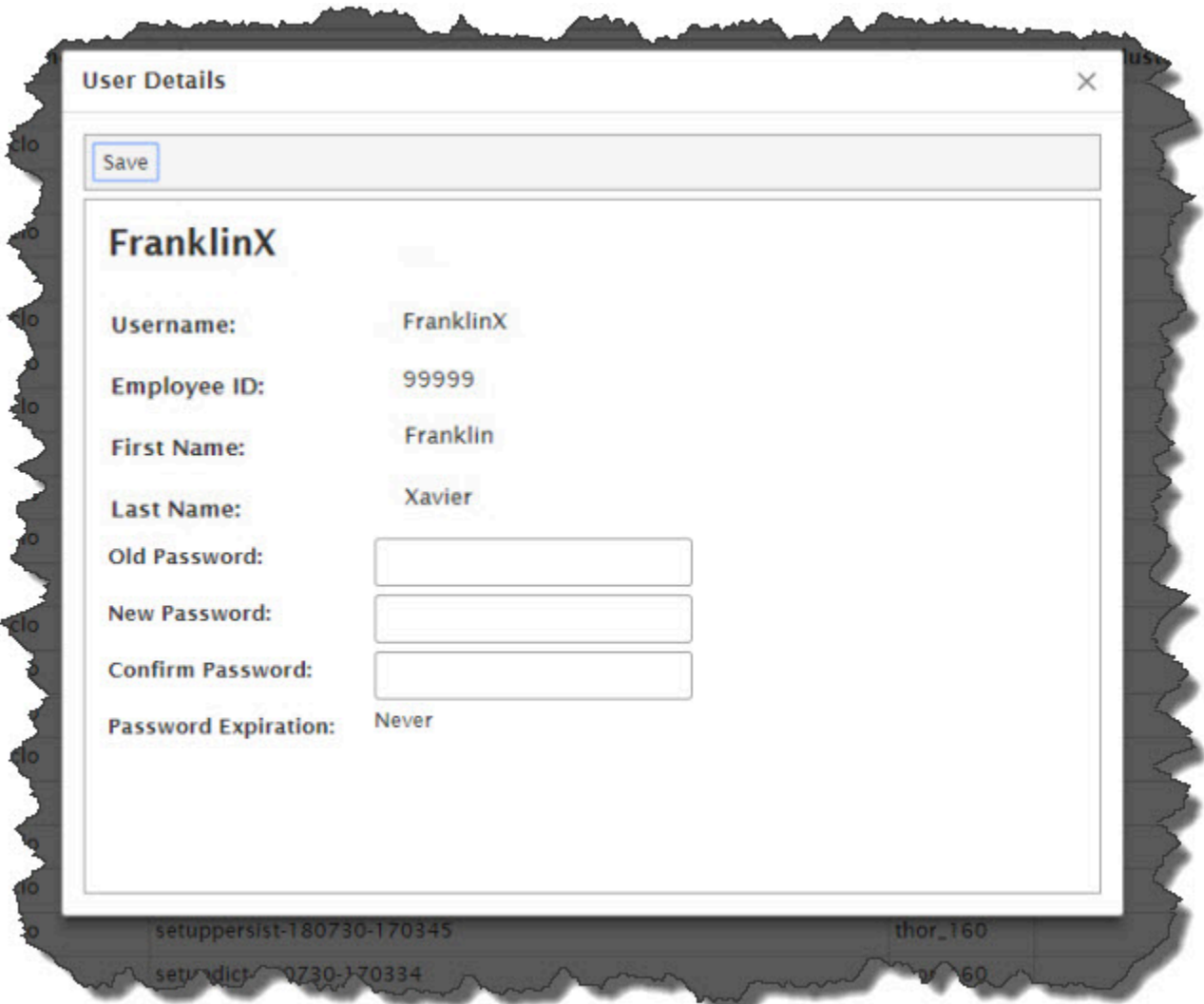
Informações sobre sua conta

Para obter mais informações sobre sua conta no ECL Watch, clique no link **LOGGED IN AS:** localizado no topo da página do ECL Watch .



1. Clique no link **LOGGED IN AS:**

A aba User Details será exibida com as informações de sua conta.



2. Confirme o User Name que você usou para entrar no sistema.

Observe que são necessários direitos de administrador para gerenciar usuários e permissões.

Verifique se você está usando uma conta com direitos de administrador se precisar gerenciar usuários ou permissões.

3. Verifique a data de validade da senha ou se a senha está prestes a expirar.

Se desejar, você também pode mudar sua senha aqui.

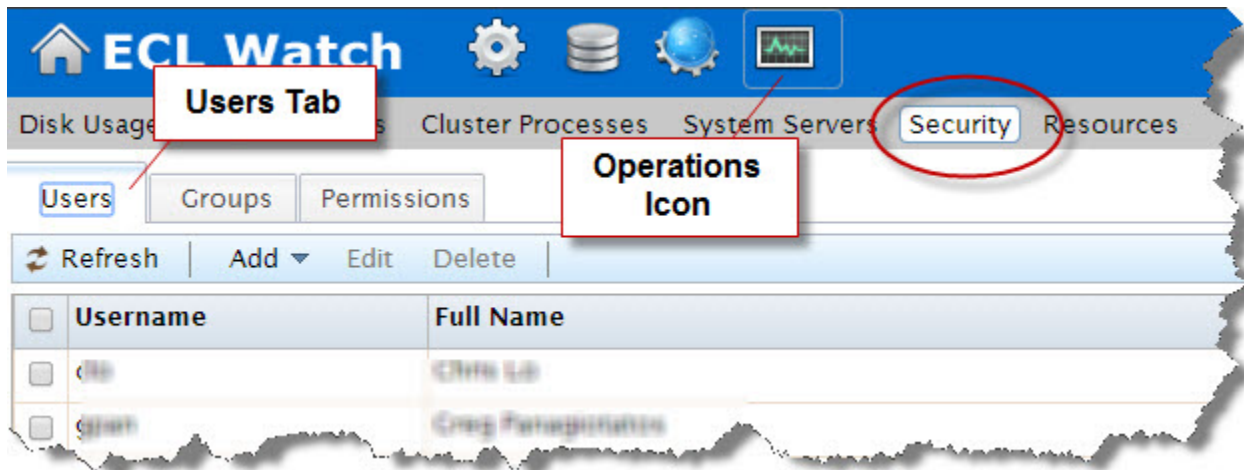
Configurando e modificando permissões de usuários

Em um ambiente habilitado para segurança, o acesso ao ECL Watch e seus recursos é controlado com o uso de um login e senha. A área **Users** permite controlar quem acessa o ECL Watch e os recursos do seu HPCC System para os quais esses usuários têm acesso. As permissões dos usuários podem ser definidas com base nas necessidades individuais de cada usuário, e também é possível adicionar usuários aos grupos que já tenham sido configurados. Use o item **Users** do menu para:

- Adicionar um novo usuário (**observação:** o Username não pode ser alterado)
- Remover um usuário
- Adicionar o usuário a um grupo
- Alterar a senha do usuário
- Modificar os detalhes ou as permissões de um usuário

Adicionando e editando usuários

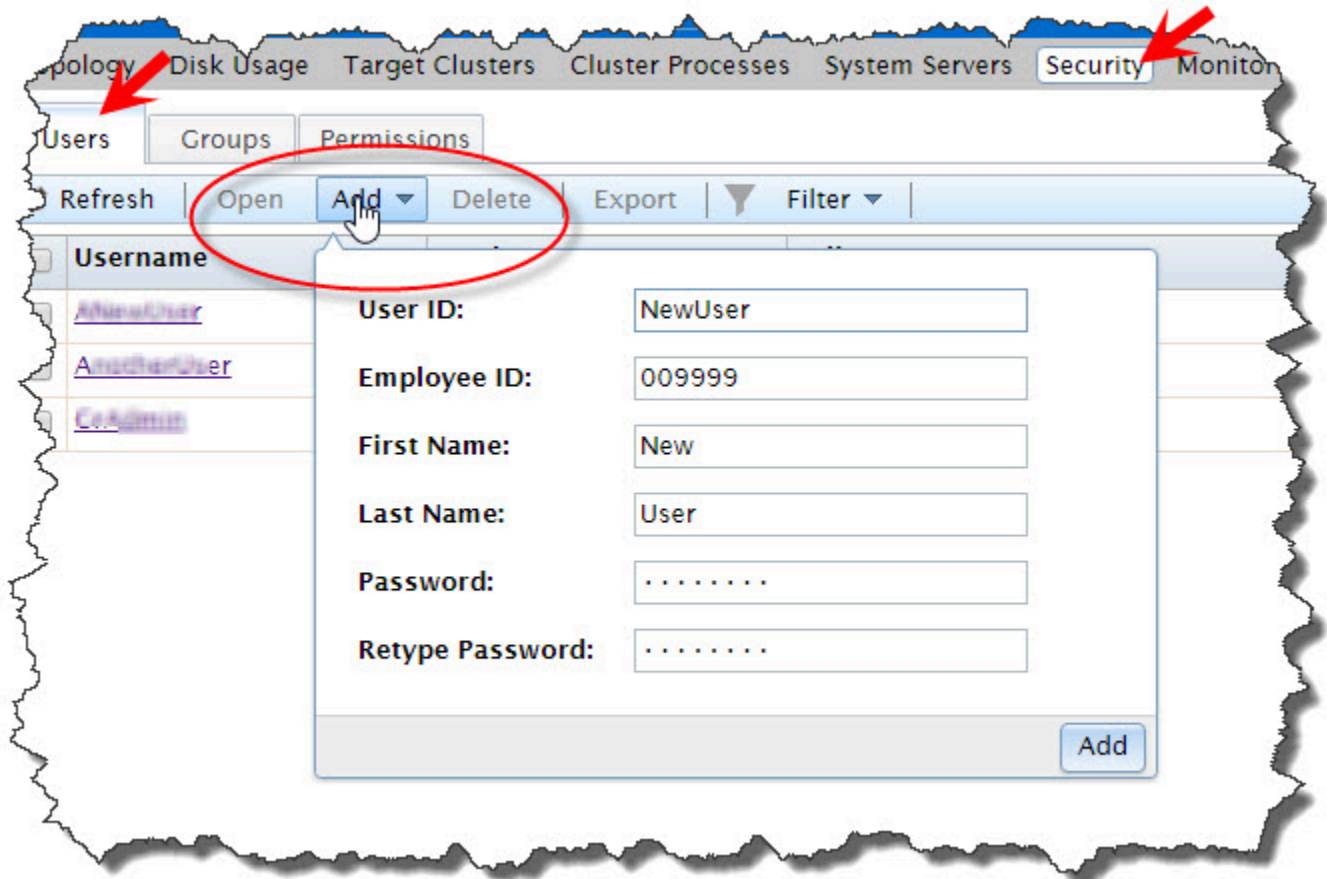
Para acessar as seções de administração do usuário, clique no ícone **Operations** e em seguida clique no link **Security** no submenu de navegação. Clique na guia **Users** para adicionar ou editar usuários.



Todos os usuários atuais são identificados na lista pelo seu Username e Full Name.

Para adicionar um novo usuário a lista de usuários autenticados:

Você precisa ter privilégio de administrador para adicionar um novo usuário.



1. Pressione o botão **Add** .

A caixa de diálogo Adicionar usuário será exibida.

2. Insira um **User ID**.

Este é o login que será usado no ECL Watch, ECL IDE, WsECL, etc.

3. Insira o **First Name** e o **Last Name** do usuário.

Estas informações ajudam a identificar o usuário e são exibidas no campo **Full Name** na janela principal **User** .

4. Insira uma **senha** para o usuário e confirme-a no campo **Retype Password** .

OBSERVAÇÃO: A senha deve estar em conformidade com a política do servidor do gerenciador de segurança.

5. Pressione o botão **Add** .

Após ter adicionado essas informações com sucesso, uma nova guia será aberta para que você possa verificar as informações do novo usuário.

6. Pressione o botão **Save** .

Após ter sido adicionado, o novo usuário será exibido na lista e você poderá modificar os detalhes e determinar as permissões conforme exigido.

Modificar detalhes do usuário:

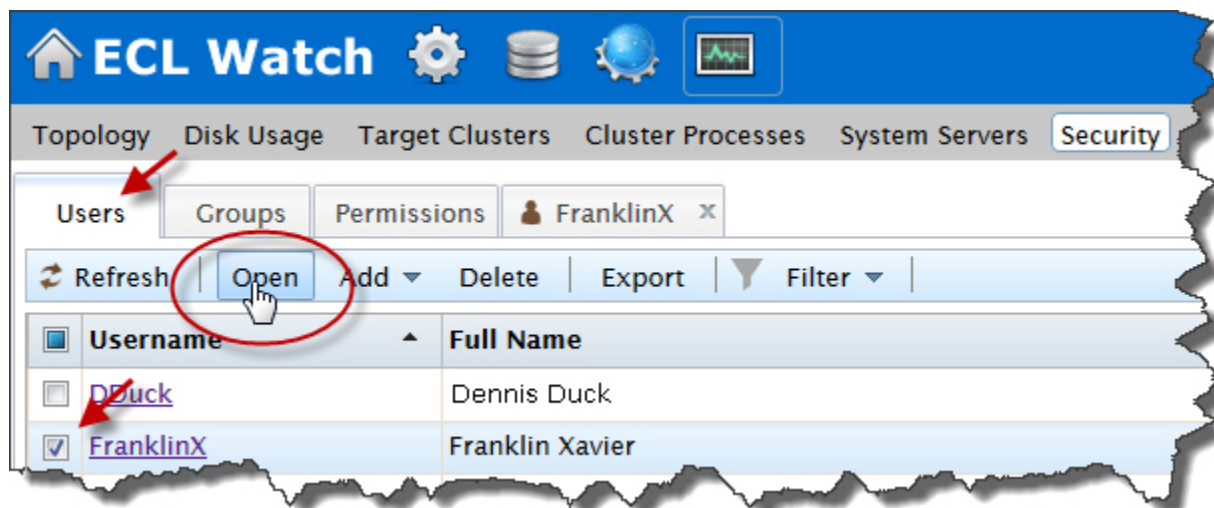
No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security** .

1. Clique na **aba Users**.

Os usuários serão exibidos em uma lista.

2. Selecione o(s) usuário(s) que deseja modificar. Clique no link **Username** para abrir a aba de detalhes do usuário.

Para selecionar vários usuários, marque a caixa de seleção ao lado do User Name. Isso ativará os botões de ação para Users. Pressione o botão de ação **Open** .



Uma aba será aberta para cada usuário selecionado. Cada aba de usuário contém várias sub-abas.

Os detalhes do usuário estão localizados na aba **Summary**.

3. Modifique os detalhes do usuário como solicitado (caso tenha selecionado mais de um usuário, repita a operação para cada um deles).

Observação: O **Username** não pode ser alterado.

4. Pressione o botão **Save**.

Uma mensagem de confirmação será exibida.

Para adicionar um usuário para um grupo:

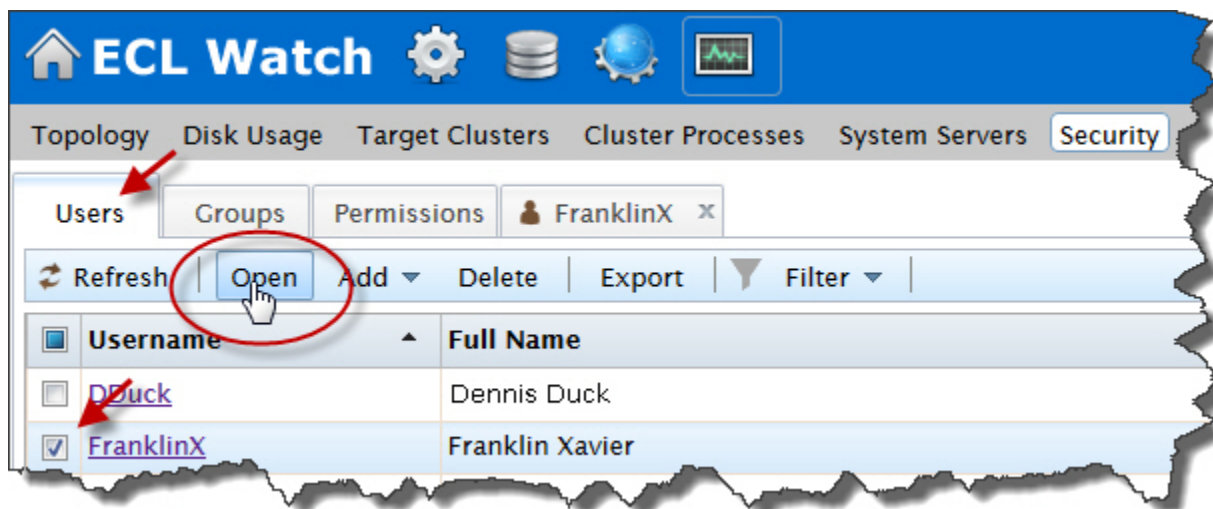
No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security**.

1. Clique na aba **Users**.

Os usuários serão exibidos em uma lista.

2. Selecione o(s) usuário(s) que deseja modificar. Clique no link **User Name** para abrir a aba de detalhes do usuário.>

Para selecionar vários usuários, marque a caixa de seleção ao lado do User Name. Isso ativará os botões de ação para Users. Pressione o botão de ação **Open**.

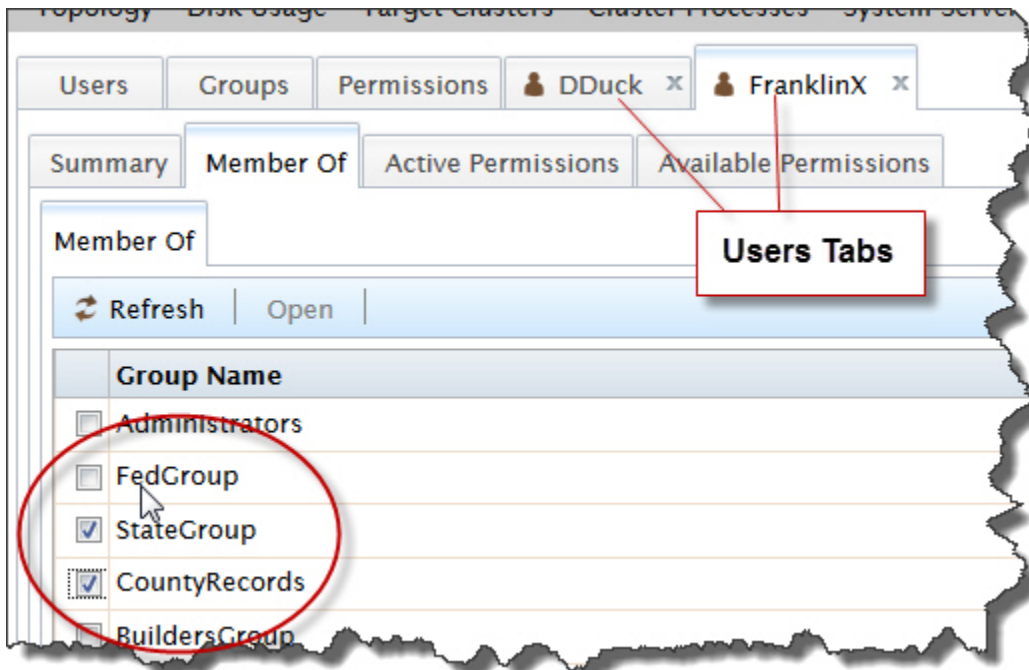


Uma aba será aberta para cada usuário selecionado. Cada aba de usuário contém várias sub-abas.

Os detalhes do usuário estão localizados na aba **Summary**.

3. Clique na aba do usuário para fazer a modificação desejada (caso tenha selecionado mais de um usuário, repita a operação para cada um deles).

A aba do usuário contém várias sub-abas.



Clique na subaba **Member of** para modificar os grupos do usuário.

4. Uma lista dos grupos disponíveis será exibida na aba **Member of** desse usuário.

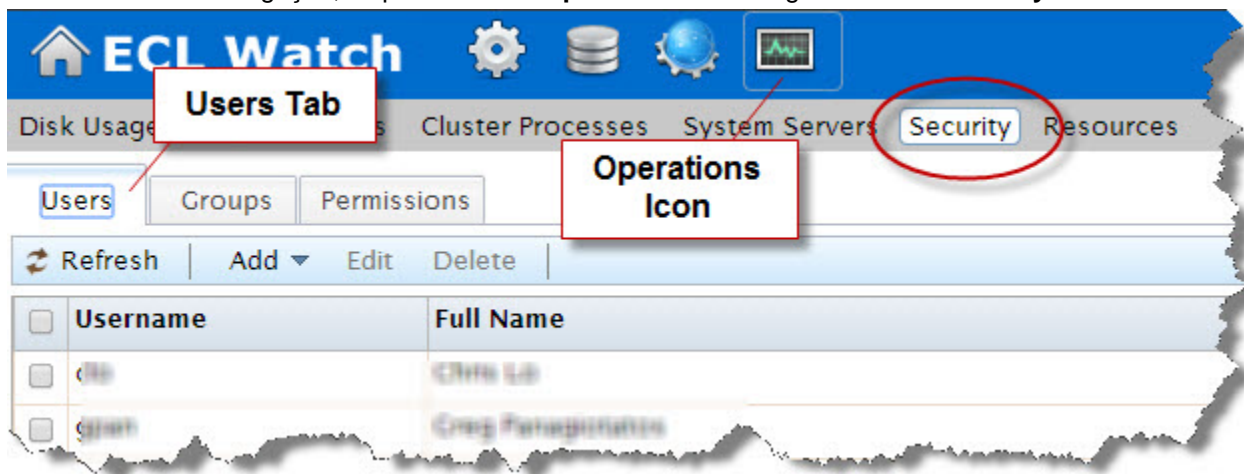
Para adicionar o usuário ao grupo, marque a caixa de seleção ao lado do grupo desejado.

5. As alterações serão salvas automaticamente. Feche a aba.

Promover um usuário para Administrador

Para modificar as credenciais de usuário você precisa ter acesso de administrador. Você pode designar a conta do Administrador do HPCC para permissões limitadas apenas relacionadas aos elementos do HPCC e não a direitos de administrador no LDAP.. Para promover um usuário a um administrador do HPCC, adicione o usuário ao grupo **Administrators**.

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security**.

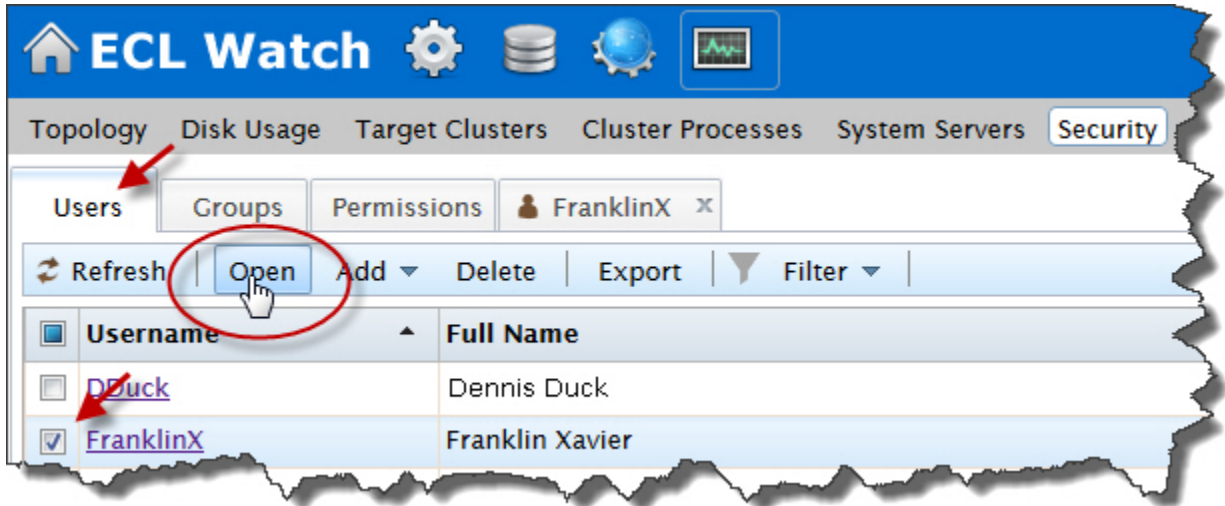


1. Clique na **aba Users**.

Os usuários serão exibidos em uma lista.

2. Selecione o(s) usuário(s) que deseja mudar de função. Clique no link **Username** para abrir a aba de detalhes do usuário.

Para selecionar vários usuários, marque a caixa de seleção ao lado do User Name. Isso ativará os botões de ação para Users. Pressione o botão de ação **Open**.



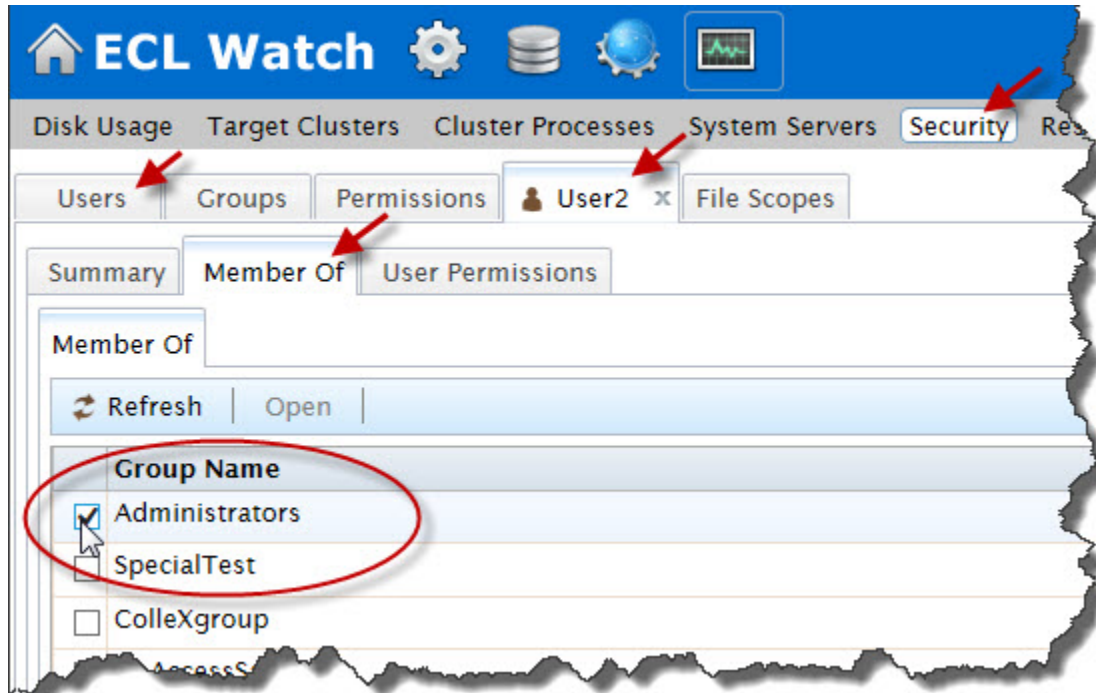
Uma aba será aberta para cada usuário selecionado. Cada aba de usuário contém várias sub-abas.

Os detalhes do usuário estão localizados na aba **Summary**.

3. Clique na aba do usuário para fazer a modificação desejada (caso tenha selecionado mais de um usuário, repita a operação para cada um deles).

A aba do usuário contém várias sub-abas.

Clique na subaba **Member of**.



4. Selecione **Administrators** marcando a caixa de seleção.

OBSERVAÇÃO: O nome do grupo padrão Administrador pode variar. É um valor configurável definido em **adminGroupName**. Por exemplo, se você configurar no ambiente o adminGroup-Name para "HPCCAdministrators", então a opção HPCCAdministrators será exibida na lista

5. As alterações serão salvas automaticamente. Feche a(s) aba(s).

Excluir um usuário de um grupo:

Você precisa ter acesso em nível de administrador para remover o usuário de um grupo.

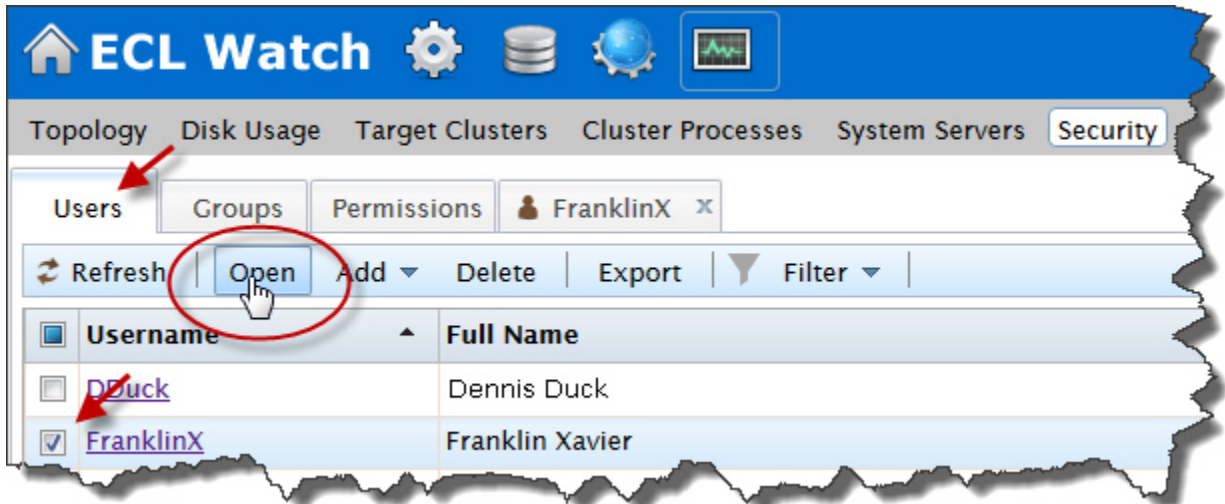
No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security**.

1. Clique no **hiperlink Users**.

Os usuários serão exibidos em uma lista.

2. Selecione o(s) usuário(s) que deseja remover. Clique no link **Username** para abrir a aba de detalhes do usuário.

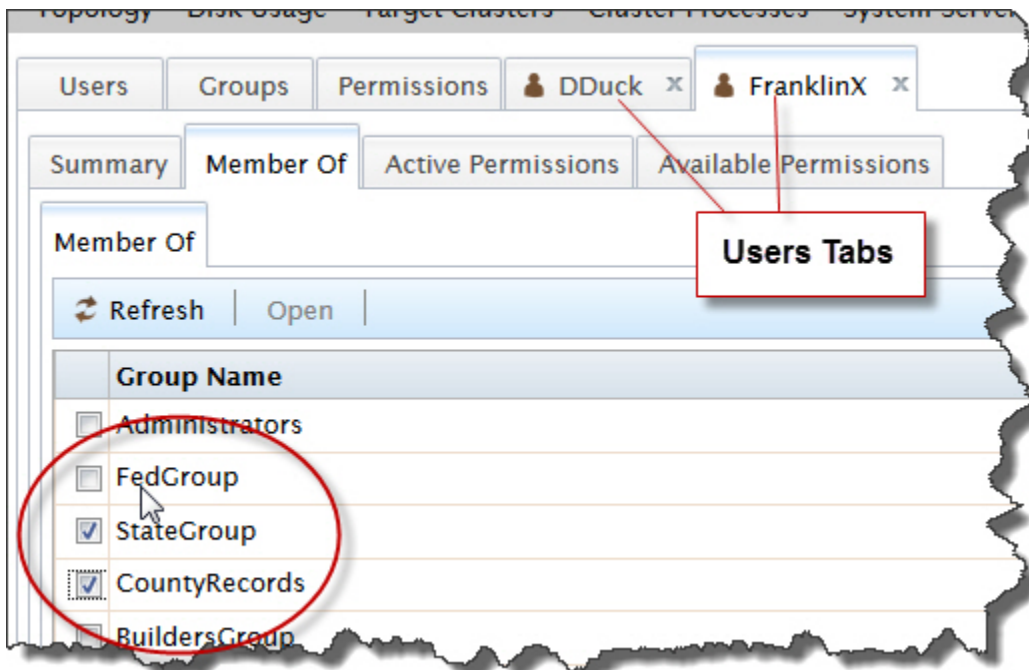
Para selecionar vários usuários, marque a caixa de seleção ao lado do User Name. Isso ativará os botões de ação para Users. Pressione o botão de ação **Open**.



Uma aba será aberta para cada usuário selecionado. Cada aba de usuário contém várias sub-abas.

3. Clique na guia do usuário que deseja modificar (caso tenha selecionado múltiplos usuários, repita a operação para cada um deles).

A aba do usuário contém várias sub-abas.



Clique na subaba **Member of** para modificar os grupos do usuário.

4. Há uma lista dos grupos disponíveis na aba **Member of** desse usuário.

Há uma caixa de seleção marcada ao lado de cada grupo ao qual o usuário pertence.

Para remover o usuário de um grupo, desmarque a caixa de seleção ao lado do grupo desejado.

5. As alterações serão salvas automaticamente. Feche a aba.

Alterar a senha do usuário:

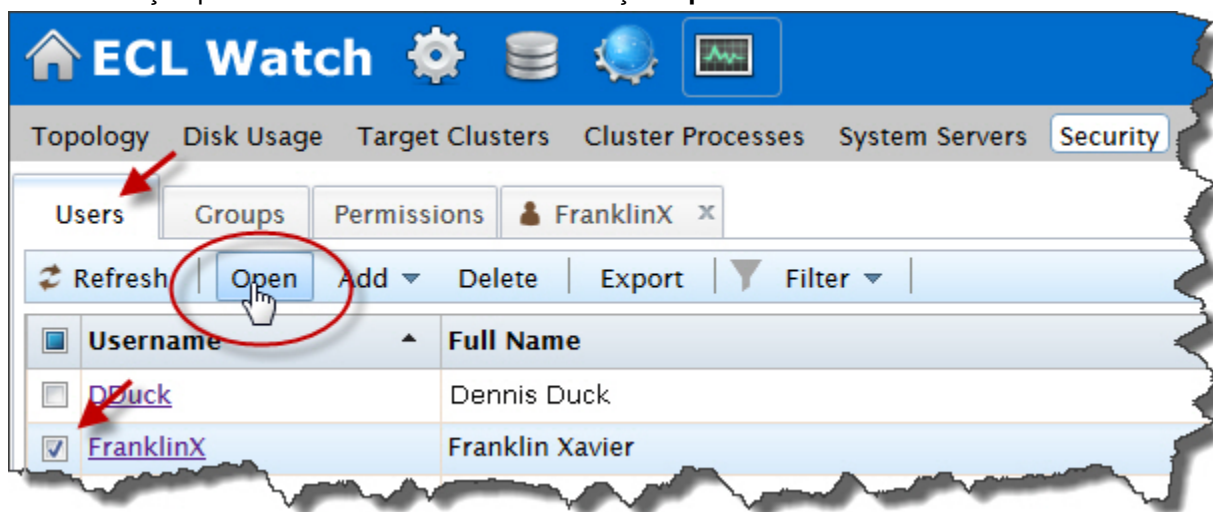
No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security** .

1. Clique na aba **Users**.

Os usuários serão exibidos em uma lista.

2. Selecione o(s) usuário(s) que deseja modificar. Clique no link **Username** para abrir a aba de detalhes do usuário.

Para selecionar vários usuários, marque a caixa de seleção ao lado do User Name. Isso ativará os botões de ação para Users. Pressione o botão de ação **Open** .



Uma aba será aberta para cada usuário selecionado. Essa aba contém várias sub-abas.

Os detalhes do usuário estão localizados na aba **Summary** .

3. Selecione a aba Summary.
4. Altere a senha nos campos **Password** e **Retype new Password** na aba de detalhes do usuário conforme solicitado (caso tenha selecionado mais de um usuário, repita o procedimento para cada um dos demais).

Observação: O **Username** não pode ser alterado.

5. Pressione o botão **Save** .

Uma mensagem de confirmação será exibida.

Excluir um usuário da lista de usuários autenticados:

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security** .

1. Clique na aba **Users** .

Os usuários serão exibidos em uma lista.

2. Marque a caixa à esquerda do nome do(s) usuário(s) que deseja remover.

Observação: Estes usuários não terão mais acesso ao ECL Watch.

3. Pressione o botão de ação **Delete**.

A confirmação será exibida.

Configurar permissões para um usuário individual

Haverá casos em que você precisará modificar as permissões para usuários individuais. Por exemplo, os usuários podem ter necessidades individuais de segurança que não sejam totalmente cobertas em nenhum grupo; ou poderá haver situações em que um usuário solicitará acesso temporário a um recurso do HPCC Systems. As permissões configuradas nesta área do ECL Watch afetam apenas o usuário selecionado. A maioria das permissões individuais configuradas aqui substitui as que foram configuradas em qualquer grupo ao qual o usuário pertença, exceto em casos de negação explícita.

Configurando permissões para um usuário individual:

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security**.

1. Clique na aba **Users**.

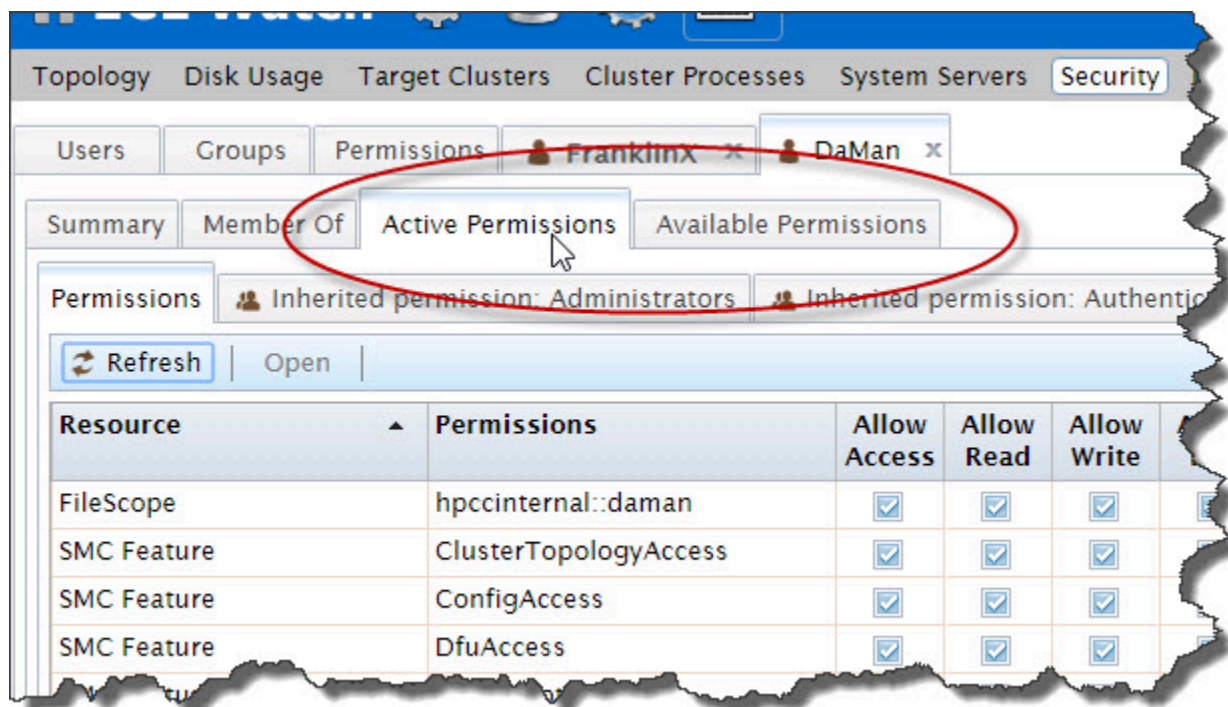
Os usuários serão exibidos em uma lista.

2. Selecione o(s) usuário(s) que deseja modificar. Clique no link **Username** para abrir a guia de detalhes do usuário.

Para selecionar vários usuários, marque a caixa de seleção ao lado do Username. Isso ativará os botões de ação para Users. Pressione o botão de ação **Open**.

3. Clique na aba do nome do usuário para modificar (caso tenha selecionado múltiplos usuários, repita a operação para cada um deles).

A aba do usuário contém várias sub-abas.

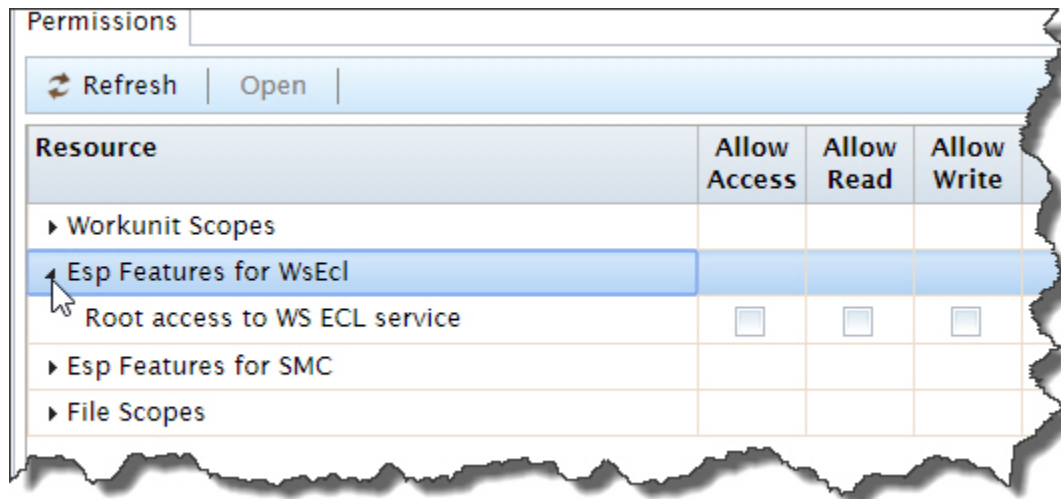


Clique na subaba **Active Permissions** para visualizar as permissões atuais do usuário.

4. Clique na aba **Available Permissions** para ver todos os conjuntos de permissões disponíveis para esse usuário.

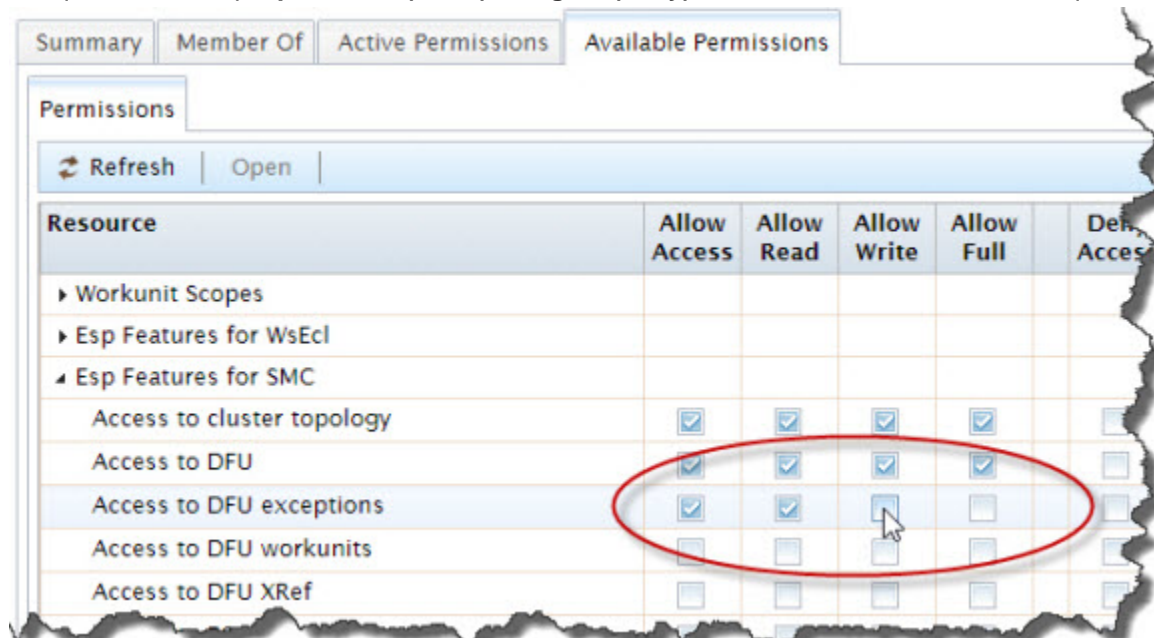
Ao selecionar as permissões na aba Available Permissions disponíveis, elas serão exibidas e podem ser configuradas na aba Active Permissions.

5. Clique na seta ao lado do recurso para exibir as permissões que podem ser configuradas para esse recurso.



A lista dos grupos de permissão atualmente configurados para este usuário e dos grupos que foram herdados pelo usuário também está listada. Clique na seta para permitir a definição das configurações individuais do recurso.

6. Pode haver mais de uma configuração de recurso disponível em cada grupo. Por isso, não se esqueça de definir as permissões para cada configuração conforme requerido.
7. Marque as caixas que **permitem (allow)** e **negam (deny)** acesso ao usuário conforme requerido.





OBSERVAÇÃO: É preciso ter cautela ao determinar qualquer configuração de permissão para **negar** um direito. A permissão mais restritiva sempre se aplica.

8. As alterações serão salvas automaticamente. Feche a aba.

Configurando e modificando grupos de permissões

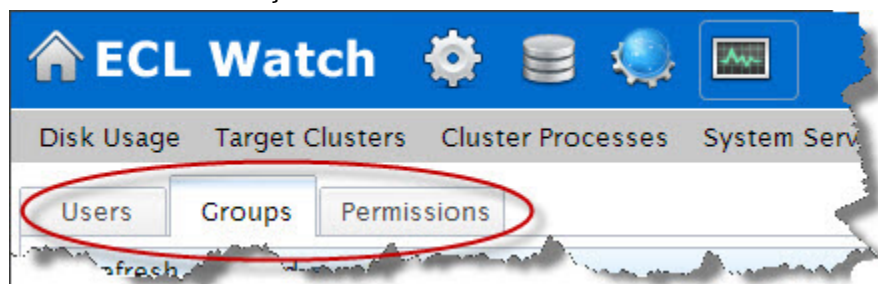
A organização dos grupos garante que todos os usuários com as mesmas necessidades de permissão tenham as mesmas configurações de permissão. Você pode fornecer aos usuários o acesso necessário às áreas de recursos do HPCC. Não há limite quanto ao número de grupos que podem ser criados. Você pode criar quantos grupos forem precisos para controlar o acesso de todos os seus usuários, independentemente das workunit desempenhadas por eles.

Use o item **Groups** do menu para:

- Adicionar um novo grupo.
- Remover um grupo.
- Adicionar membros a um grupo
- Modificar as permissões de um grupo

Adicionando e editando grupos

Ao adicionar ou alterar as permissões de um grupo, todos os membros desse grupo receberão essas configurações de permissão. Por isso, é importante ter certeza de estar concedendo ou negando acesso aos recursos apropriados para os membros desse grupo. Se precisar fazer alterações para um único usuário (ou para um pequeno número de usuários), será melhor fazer tais alterações para cada usuário individual como ilustrado nas seções anteriores.

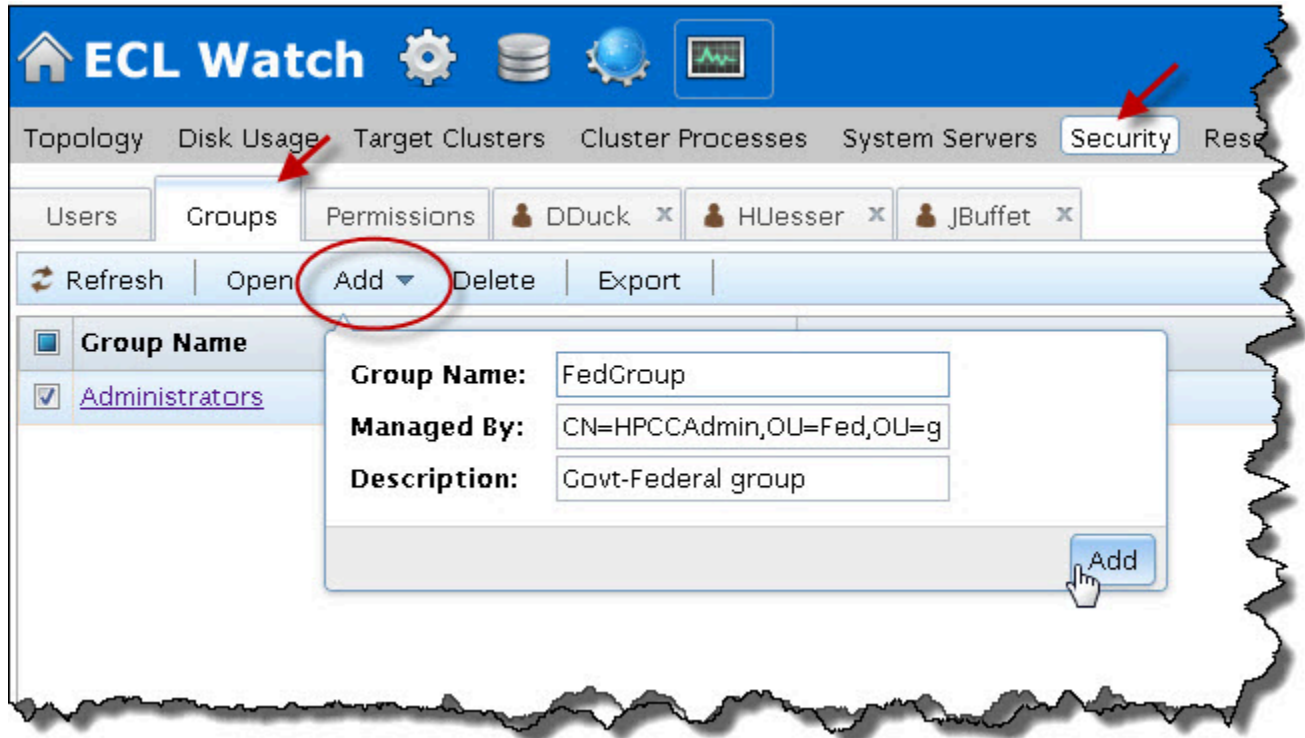


Para modificar grupos, clique no ícone **Operations**, e em seguida no link **Security** do submenu de navegação. Clique na aba **Groups**.

Adicionando um novo grupo:

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security**

1. Clique na aba **Groups**.
2. Pressione o botão de ação **Add**.



Isso abrirá a caixa de diálogo onde é possível inserir um nome para o grupo.

3. Insira o **Group Name**.
4. Insira um nome completamente distinto para o dono do grupo no campo **Manager by**.
5. Insira uma descrição para o grupo. (opcional)
6. Pressione o botão **Add**.

Isso abrirá uma nova aba e várias subabas para o grupo

A subaba **Summary** exibe o nome do grupo.

A aba **Members** exibe a lista dos usuários; marque a caixa de seleção ao lado de cada usuário para adicioná-lo ao grupo.

A aba **Active Group Permissions** exibe as permissões aplicadas ao grupo.

A aba **Available Groups Permissions** exibe todas as permissões disponíveis; a seleção a partir da aba Permissions disponíveis aplica as permissões à aba Permissão de grupo ativo.

Você pode definir as permissões e adicionar membros a esse grupo nas respectivas sub-abas do grupo.

Excluir um grupo:

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security**.

1. Clique na aba **Groups**.
2. Localize o grupo na lista e marque a caixa de seleção ao lado dele.

3. Pressione o botão de ação **Delete** .

4. Pressione o botão de confirmação **OK**

O grupo não será mais exibido na lista.

Adicionar novos membros para um grupo:

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security** .

1. Clique na aba **Groups** .

2. Localize o grupo na lista e marque a caixa de seleção ao lado dele.

3. Pressione o botão de ação **Open** .

Isso abrirá uma nova aba para o grupo.

As sub-abas exibem: Summary , Members, **Active Group Permissions**, e **Available Group Permissions**.

4. Selecione a aba **Members**

A aba Members exibirá uma lista de todos os usuários no sistema. Aqueles que pertencem ao grupo selecionado terão a caixa de seleção marcada ao lado.

5. Marque a(s) caixa(s) à esquerda do nome dos usuários que deseja adicionar ao grupo.

6. As alterações serão salvas automaticamente. Feche a aba.

Excluir membros de um grupo:

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security** .

1. Clique na aba **Groups** .

2. Localize o grupo na lista e marque a caixa de seleção ao lado dele.

3. Pressione o botão de ação **Open** .

Isso abrirá uma nova aba para o grupo.

A aba Grupos possui diversas sub-abas: **Summary**, **Members**, **Active Group Permissions**, e **Available Group Permissions**.

4. Selecione a aba **Members** .

A aba Members exibirá uma lista de todos os usuários no sistema. Aqueles que pertencem ao grupo selecionado terão a caixa de seleção marcada ao lado.

5. Desmarque a(s) caixa(s) à esquerda para todos os usuários que deseja remover do grupo.

6. As alterações serão salvas automaticamente. Feche a aba.

Configurar Permissões para Grupo

Por padrão, todos os usuários são membros do grupo **Authenticated Users** . O grupo **Authenticated Users** possui direitos de acesso a quase todos os recursos. Para definir controles mais restritos, é preciso criar grupos específicos com permissões mais limitadas.

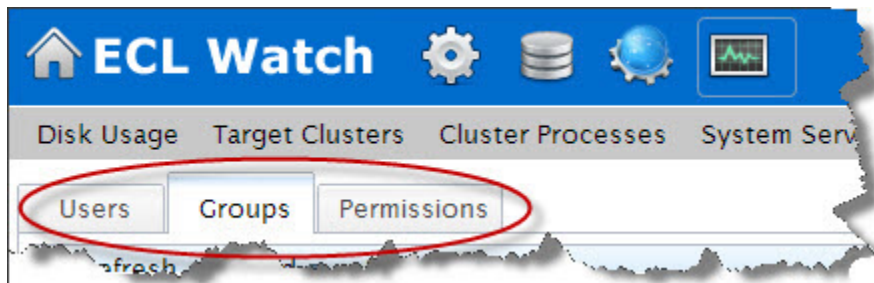
Você pode criar grupos apenas com os direitos de acesso que deseja conceder. Essa abordagem oferece maior flexibilidade, já que um único ID de usuário pode estar associada a vários grupos.

Como prática recomendada, use **Allow** em vez de **Deny** para controlar o acesso. Quando possível, use a função Deny “negar” apenas como exceção. Caso queira negar o acesso de um usuário a algum controle específico, recomenda-se criar um grupo para isso e adicionar o(s) usuário(s) neste grupo para, então, negar o acesso somente para esse grupo.

Lembre-se de que o controle mais restritivo tem precedência. Por exemplo, se um usuário faz parte de um grupo que não dá permissão de acesso a um determinado arquivo, porém este mesmo usuário também faz parte de outro grupo cujo acesso a tal arquivo é permitido, o usuário continuará sem permissão para acessar o arquivo.

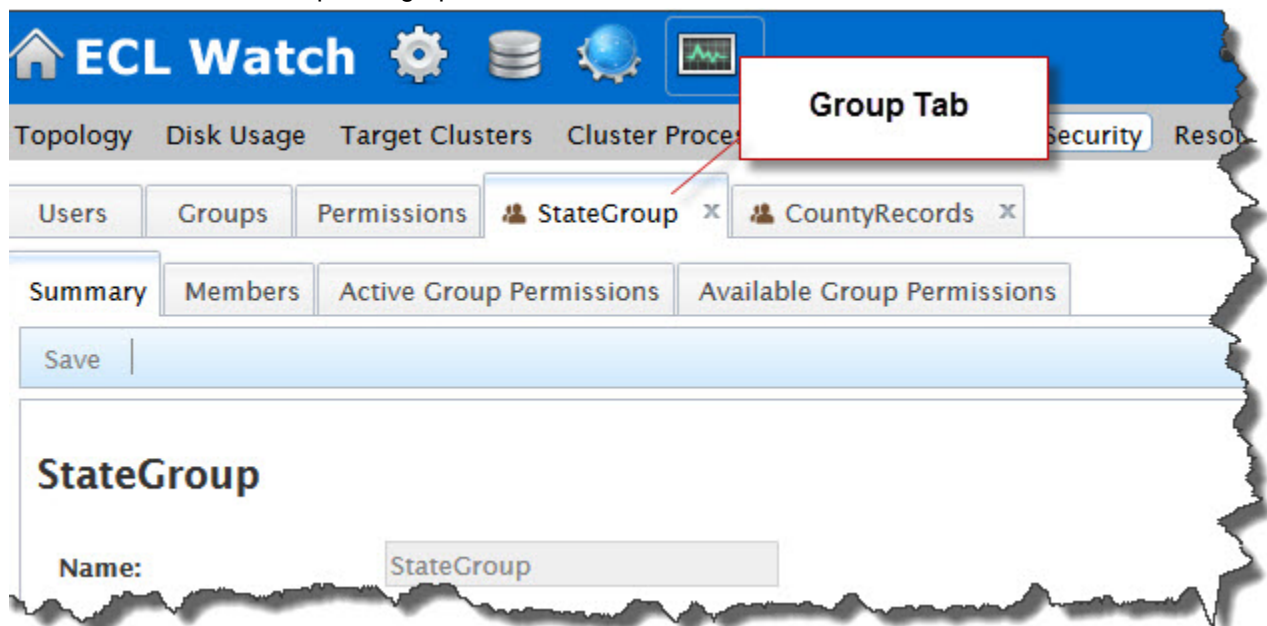
Configurando Permissões para Grupo:

No submenu de navegação, clique no ícone **Operations** e em seguida no link **Security**.



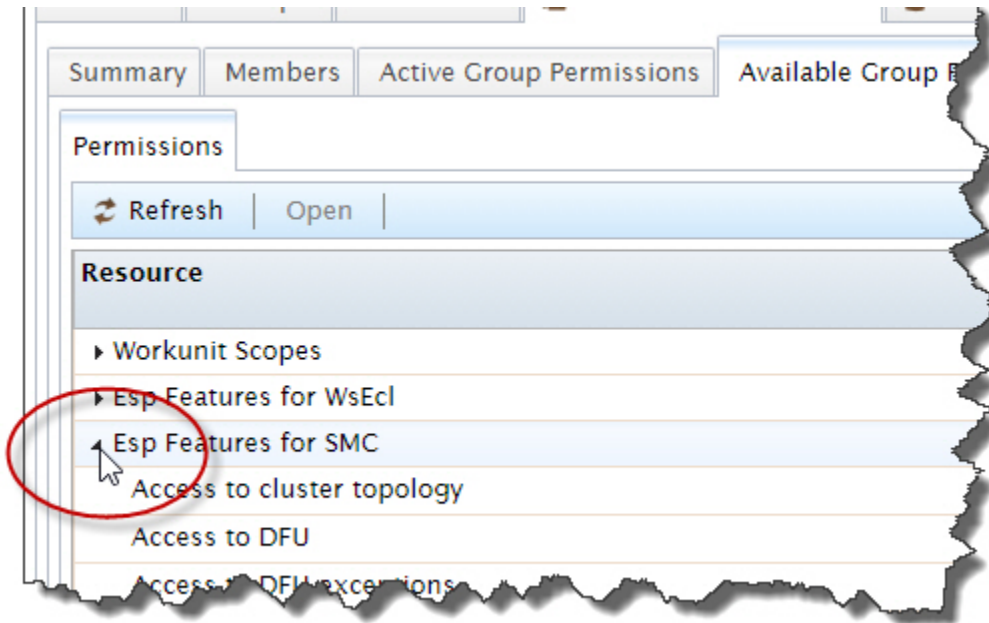
1. Clique na aba **Groups**.
2. Localize o grupo na lista e marque a caixa de seleção ao lado dele.
3. Pressione o botão de ação **Open**.

Isso abrirá uma nova aba para o grupo.



A guia do grupo exibirá as sub-abas: **Summary**, **Members**, **Active Group Permissions**, e **Available Group Permissions**.

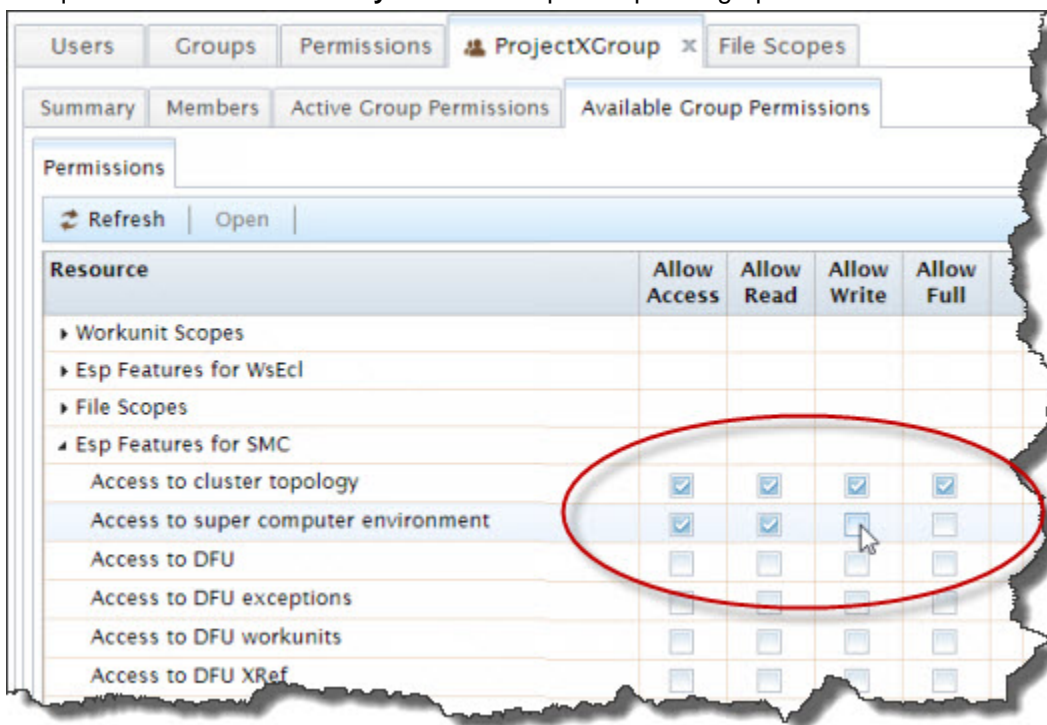
4. Selecione a sub-aba **Available Group Permissions** . Isso exibirá todos os recursos de permissão disponíveis.
5. Clique na seta à esquerda de **Resource** para expandir e mostrar as configurações de permissão para os recursos.



Os recursos de permissão dos grupos serão exibidos.

6. Pode haver mais de uma configuração de recurso disponível em cada grupo. Por isso, não se esqueça de definir as permissões para cada configuração conforme requerido.

7. Marque as caixas **Allow** e **Deny** conforme requerido para o grupo.



OBSERVAÇÃO: É preciso ter cautela ao determinar qualquer configuração de permissão para **negar** um acesso. A permissão mais restritiva sempre se aplica.

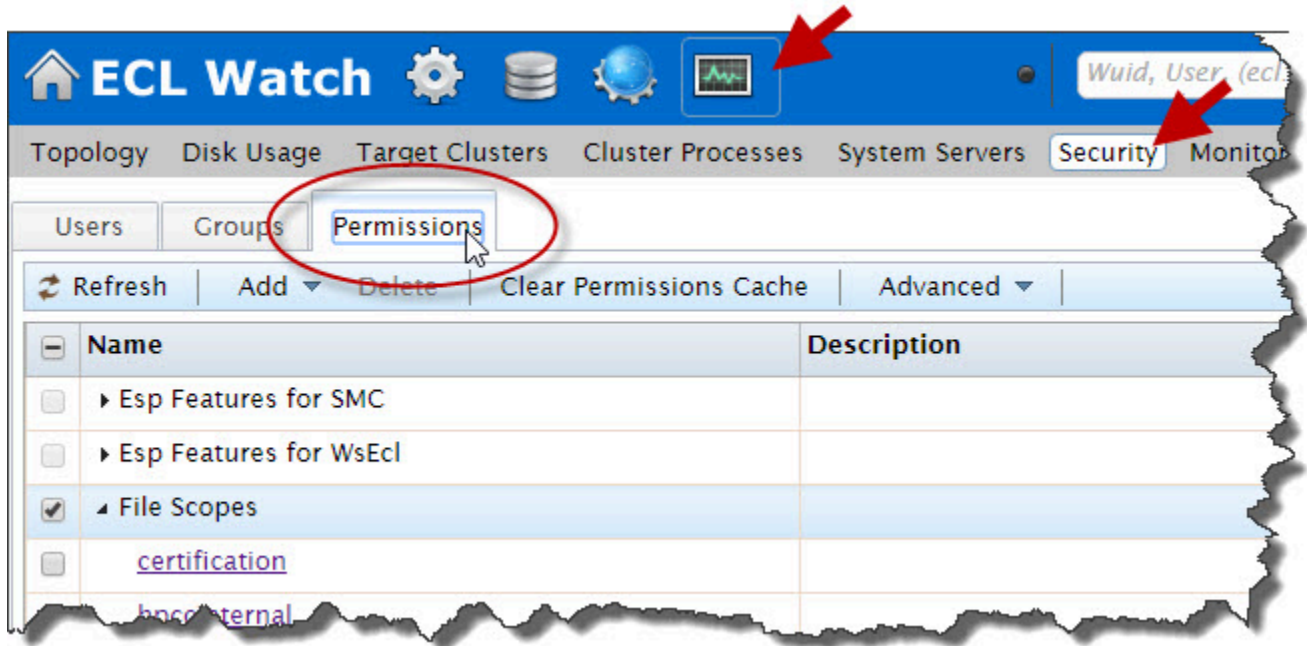
8. Pode haver mais de uma configuração de recurso disponível, selecione o(s) recurso(s) necessário(s) na lista suspensa.

Repita o procedimento para cada recurso aplicável.

9. As alterações serão salvas automaticamente. Feche a aba.

Controle de acesso em nível de recurso

O acesso às permissões específicas está disponível através do ECL Watch. Para modificar as permissões específicas, é preciso ter acesso em nível de administrador. Para acessar as permissões específicas, clique no ícone **Operations** , e em seguida clique no link **Security** a partir do submenu de navegação.

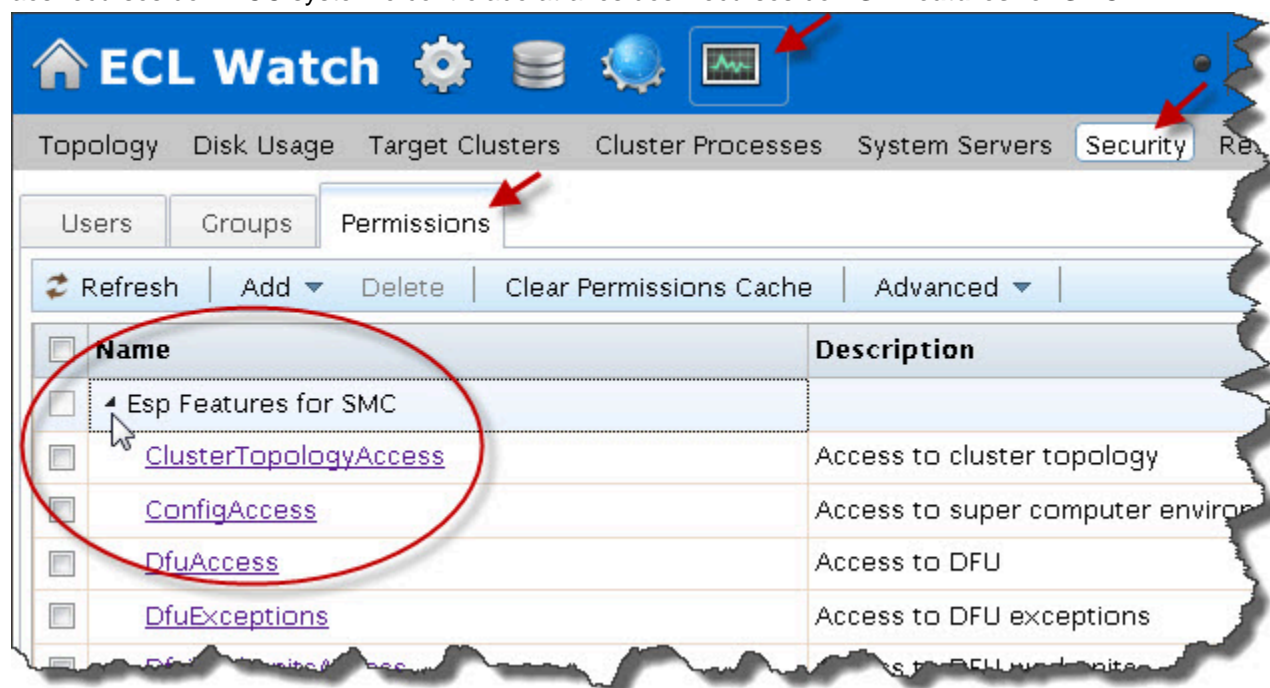


Para usar os controles de nível específico, aplique o recurso específico da aba **Available Permissions** para a aba **Active Permissions** para usuários e grupos. O uso de controles de nível específico permitirá que você:

- Veja as funcionalidades e as permissões para qualquer recurso
- Edite as permissões para qualquer recurso
- Atualize as permissões de usuários e grupos para um recurso específico

Recursos

Há muitos outros recursos para os quais você pode configurar o controle de acesso no HPCC. O acesso aos recursos do HPCC system é controlado através dos Recursos do **ESP Features for SMC**.



Os recursos disponíveis estão listados abaixo da aba **Permissions**. Você pode visualizar e obter acesso aos controles específicos aqui. No entanto, os controles específicos devem ser aplicados aos usuários e não aos grupos. Ao clicar no link do nome específico, será aberta a guia que mostra os usuários e grupos onde essas permissões específicas são aplicadas.

As configurações de permissão dos recursos do ECL Watch que não estão listadas são irrelevantes e não devem ser usadas.

Aplicar permissões para um recurso:

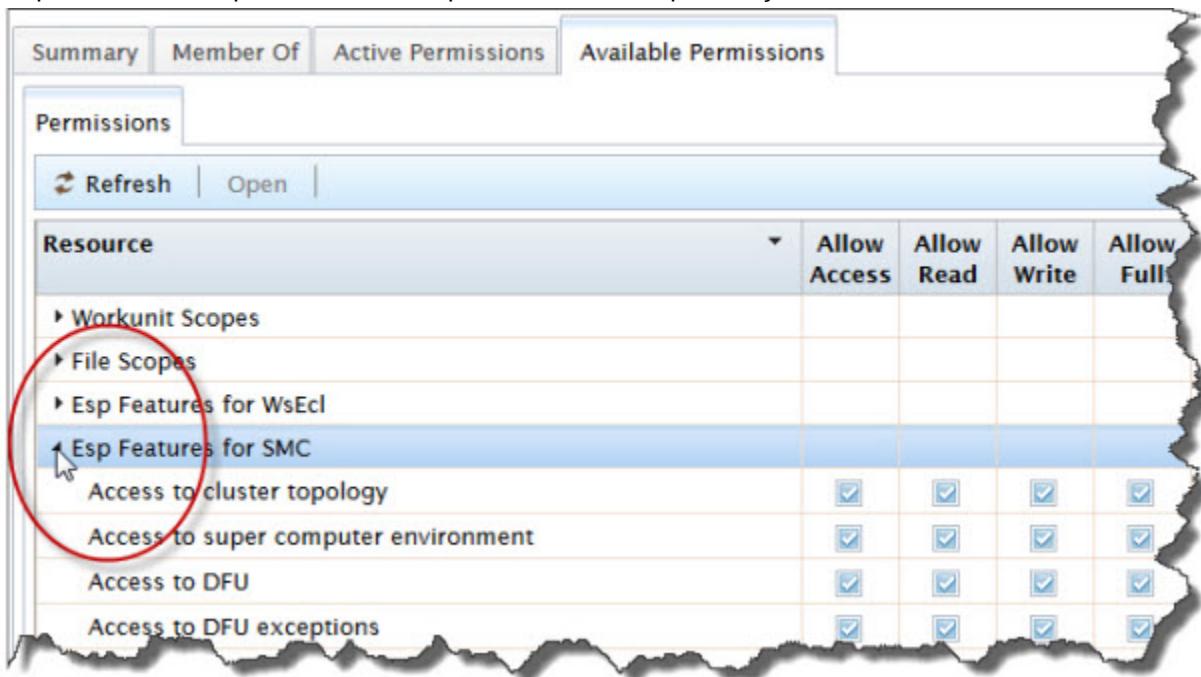
Para usar permissões específicas, é preciso aplicá-las a um usuário ou grupo(s). Para acessar as permissões específicas, clique no ícone **Operations**, e em seguida clique no link **Security** a partir do submenu de navegação.

1. Identifique o(s) usuário(s) ou grupo(s) que deseja modificar as permissões específicas.

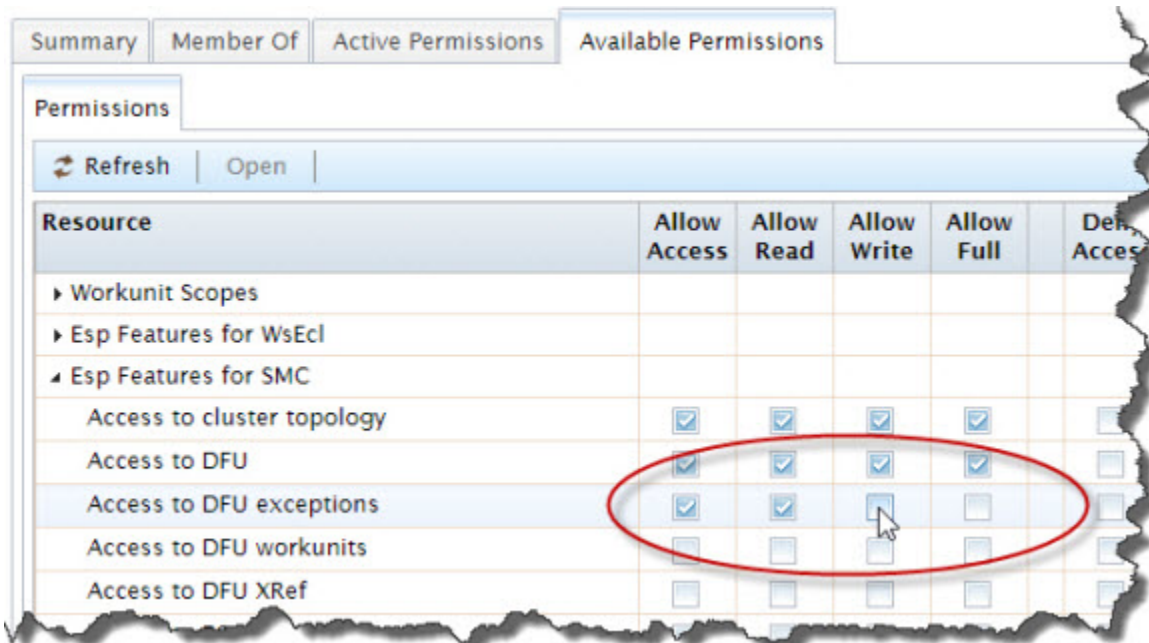
Selecione a aba apropriada. (Users or Groups)

2. Marque a(s) caixa(s) de seleção ao lado do(s) usuário(s) ou grupo(s) que deseja modificar.
3. Pressione o botão de ação **Open**. Uma aba será aberta para cada usuário ou grupo.
4. Clique na sub-aba **Available Permissions**.

5. Clique na seta à esquerda do recurso para mostrar as especificações desse recurso.



6. Localize o(s) recurso(s) específico(s) que deseja atualizar.



7. Clique nas colunas “allow” e “deny” na(s) caixa(s) de seleção.
8. As alterações serão salvas automaticamente. Feche a(s) aba(s).

Observação: Esse processo deve ser realizado individualmente para cada usuário ou grupo.

Recursos de Permissões SMC

A tabela a seguir descreve o nível de acesso exigido para que esses recursos do ECL Watch do HPCC possam ser usados.

Nome	Descrição	Acesso
ClusterTopologyAccess	Acesso à Topologia do cluster	Leitura
	Ver arquivos de log.	Completo
DfuAccess	Acesso aos arquivos lógicos DFU	Leitura
	Remover arquivos, Adicionar aos superarquivos e remover dos superarquivos	Escrita
	Apagar metadados do histórico do arquivo	Completo
DfuExceptions	Acesso à leitura de Exceções DFU	Leitura
DfuWorkunitsAccess	Acesso à leitura de Workunit DFU	Leitura
	Acesso para Criar, Excluir, Atualizar, Enviar e Abortar DFU Workunits	Gravação
DfuXrefAccess	Acesso à leitura de DFU XREF	Leitura
	Limpar diretório	Gravação
	Fazer alterações e gerar relatórios XREF	Completo
EclDirectAccess	Acesso ao serviço ECL Direct.	Completo
ESDLConfigAccess	ESDL Acesso à configuração	Leitura
	Publicar definição e conexão ESDL, configurar método de conexão ESDL.	Gravação
	Apagar definições ESDL, apagar conexões ESDL	Completo
FileDesprayAccess	Permite que o usuário faça o despray (consolidar dados dos nós) dos arquivos lógicos.	Gravação
FileIOAccess	Acesso à leitura de arquivos na Zona de entrada de arquivos	Leitura
	Acesso à gravação de arquivos na Zona de entrada de arquivos	Gravação
PackageMapAccess	Acesso à(ao) ListPackage, ListPackages, GetPackage, GetPackageMapById, ValidatePackage, GetQueryFileMapping, GetPackageMapSelectOptions, GetPartFromPackageMap	Leitura
	Access a(ao) AddPackage, CopyPackageMap, ActivatePackage, DeActivatePackage, AddPartToPackageMap, RemovePartFromPackageMap	Gravação
	Apagar Pacote	Completo
FileScopeAccess	Permite acesso à consulta, configuração e remoção de permissões do escopo de arquivos	Completo
FileDesprayAccess	Acesso ao spraying (processo de distribuição dos dados aos nós) e cópia	Leitura
	Renomear, spray, copiar e replicar arquivos	Gravação


Nome	Descrição	Acesso
	Fazer o download Apagar da Zona de entrada de arquivos	Completo
MachineInfoAccess	Acesso às informações da máquina/preflight	Leitura
MetricsAccess	Acesso às informações sobre métricas SNMP (Métricas Roxie)	Leitura
OthersWorkunitsAccess	Acesso à visualização de workunit de outro usuário	Leitura
	Acesso à Modificar ou reenviar workunit do usuário	Gravação
	Acesso à Remover workunit de outros usuários	Completo
OwnWorkunitsAccess	Acesso à visualização da própria workunit	Leitura
	Acesso à Criar ou modificar a própria workunit	Gravação
	Acesso a remoção da própria workunit	Completo
RoxieControlAccess	Acesso aos comandos de controle do Roxie	Leitura
SmcAccess	Acesso ao ECL Watch (Serviço SMC)	Leitura
ThorQueueAccess	Acesso ao controle da fila de workunit do Thor	Completo
WsEclAccess	Acesso ao serviço WS ECL	Completo
WsLogAccess	Habilita a função de leitura de logs dos componentes	Leitura

Algumas Notas de Permissões de Recursos

- Para o SMCAccess é obrigatório ter feito o login no ECL Watch.
- ThorQueueAccess permite manipular a fila promovendo ou rebaixando as workunit de acordo com a prioridade.
- ThorQueueAccess também permite pausar ou limpar a fila do Thor. Você também pode ver as estatísticas de uso do Thor.
- Dependendo do nível de acesso do usuário, é possível visualizar, modificar e remover suas próprias workunit ou as workunit de outros usuários. Trata-se do OwnWorkunitsAccess e OthersWorkunitsAccess, respectivamente.
- As permissões do DfuWorkunitsAccess permitem que os usuários visualizem ou manipulem as workunit DFU .
- Os usuários precisam ter autorização para ver os arquivos na zona de entrada de arquivos, assim como também para inserir arquivos lá. Também é preciso obter permissões adicionais para fazer o spray (distribuir aos nós) e copiar arquivos da zona de entrada de arquivos para o cluster, assim como para fazer o despray (consolidar dados dos nós) dos arquivos do cluster para a zona de entrada de arquivos.

DFU Xref

XREF é usado para monitorar os arquivos nos clusters. Os relatórios gerados mostram onde a organização é necessária nos clusters, e os usuários precisam obter permissão adicional para usar este recurso.

	Em um sistema maior, sugerimos limitar o número de usuários que têm permissão para gerar relatórios XREF configurando o acesso ao DfuXrefAccess para FULL (Completo) apenas para esses usuários.
---	--

Usuários/Permissões

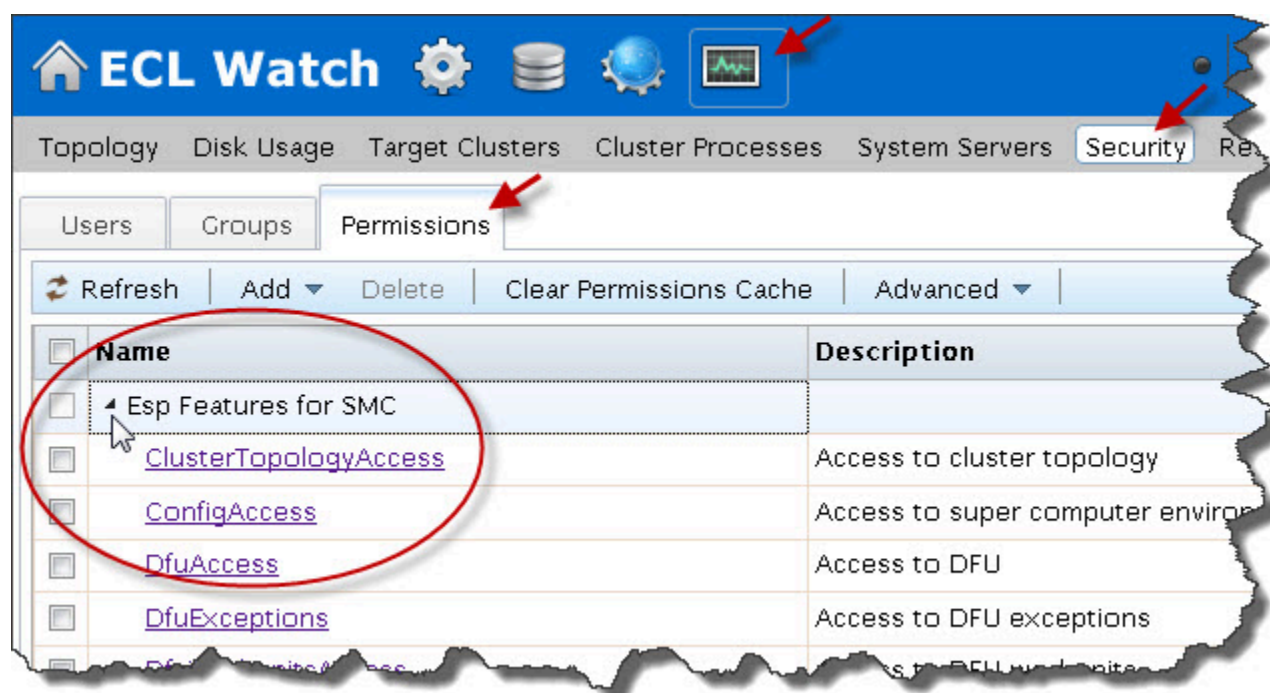
Para poder visualizar a área **Users/Permissions** no ECL Watch, o usuário precisa ser um membro do grupo Administradores (ou de nome similar) com permissões adequadas no servidor LDAP ou Active Directory.

Controle de Acesso a Arquivos

A tecnologia do **servidor LDAP Dali** do HPCC permite configurar permissões de acesso seguro às pastas de arquivo de dados (ou escopos de arquivo). Isso é controlado pelo uso dos recursos de escopo de arquivos.

Uma OU denominada **Files** é criado automaticamente quando o servidor Dali é inicializado. Para proteger as pastas de dados, crie escopos de arquivo para essa pasta e aplique os direitos para cada escopo.

Figure 10. Permissões de escopo de arquivos



Por exemplo, abaixo de **Files** há uma unidade (OU) representando o cluster, como **thor** (ou o nome configurado para seu cluster). Além disso, logo abaixo poderia ter uma unidade denominada **collectionx** que contém duas unidades: **publicdata** e **securedata**. A pasta **publicdata** possui direitos concedidos a um grande grupo de usuários; já para a pasta **securedata** foi concedido o acesso limitado. Isso permite impedir que usuários não autorizados acessem os arquivos da pasta **securedata** folder.

A estrutura descrita acima corresponde a essa estrutura lógica:

collectionx::securedata

A qual corresponde a essa estrutura física:

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

Todos os componentes e ferramentas HPCC respeitam a segurança de acesso a arquivos definidos no LDAP. As seguintes exceções são consideradas a nível de sistema ou para usuários administradores:

- Acesso aos arquivos de rede usando UNC's, Serviços de Terminal, ou SSH.
- Utilitários administrativos

A tentativa de acesso a um arquivo em uma pasta sem que a permissão tenha sido concedida, resultará em um dos seguintes erros:

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

ou

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

(onde <filepath> corresponde ao caminho completo do escopo de arquivo lógico)

Criando um escopo de arquivo

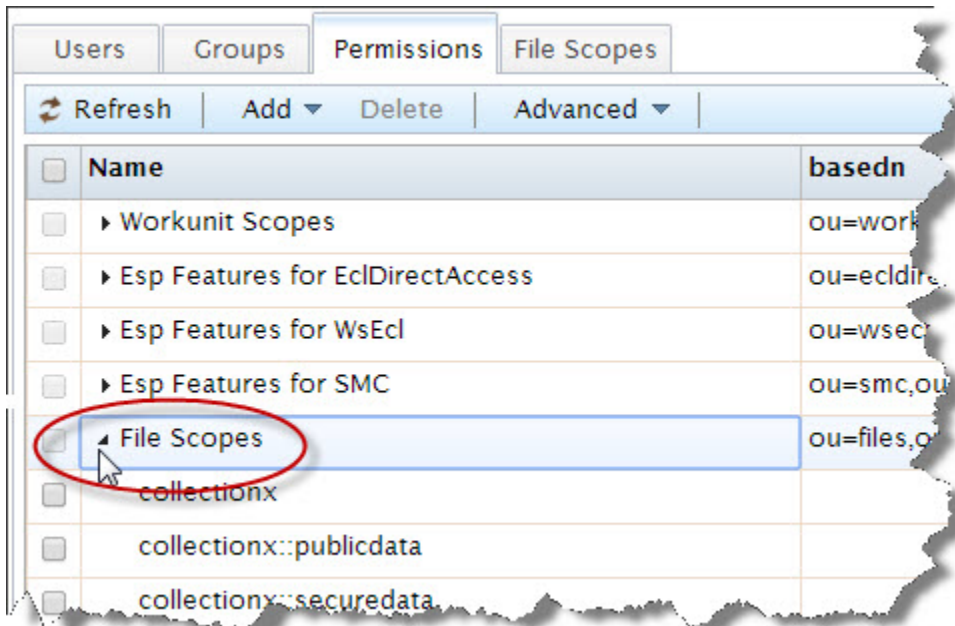
Para aplicar as permissões a um escopo de arquivos, primeiramente é preciso criar o(s) escopo(s) de arquivos.

Para criar o(s) escopo(s) de arquivos, clique no ícone **Operations** , e em seguida no link **Security** localizados no submenu de navegação.

1. Clique na aba **Permissions** .

Os recursos específicos serão exibidos.

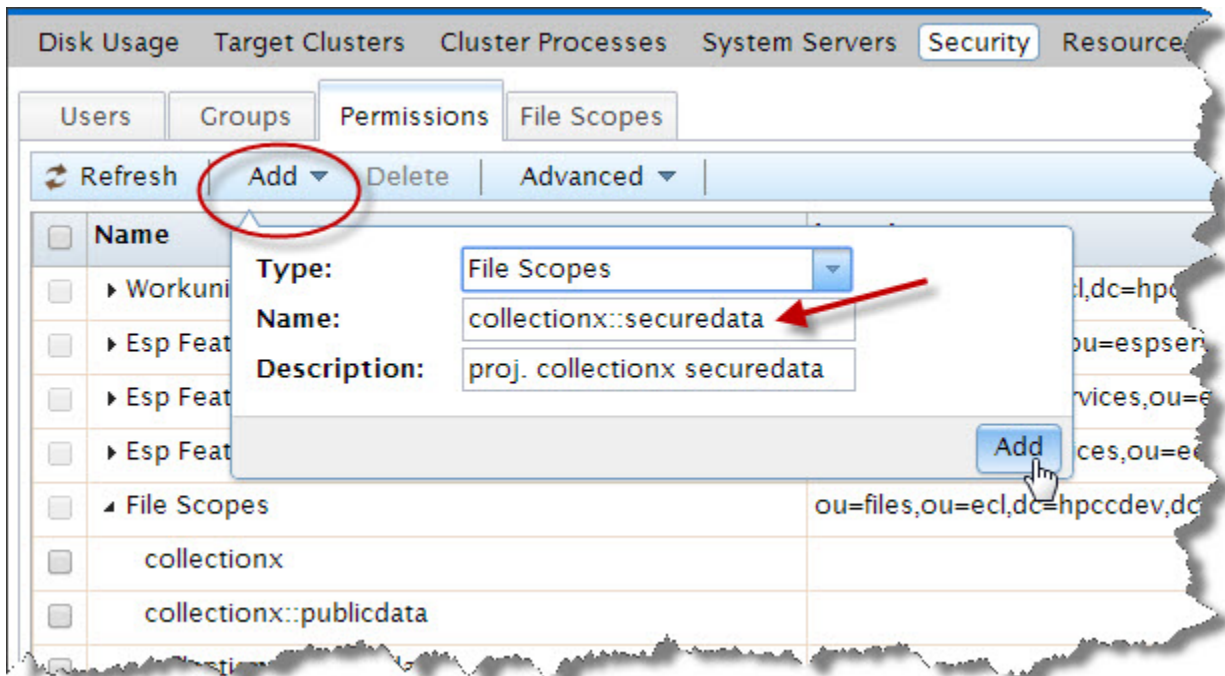
2. Clique na seta à esquerda do recurso **File Scopes** para exibir os escopos do arquivo.



3. Pressione o botão **Add** .
4. Selecione **File Scopes** na lista suspensa.



5. Digite no o nome exato do escopo que deseja adicionar. **Digite no campo** Name



o nome exato do escopo que deseja adicionar. **Digite uma breve descrição no campo** Description.

6. Pressione o botão **Add**.

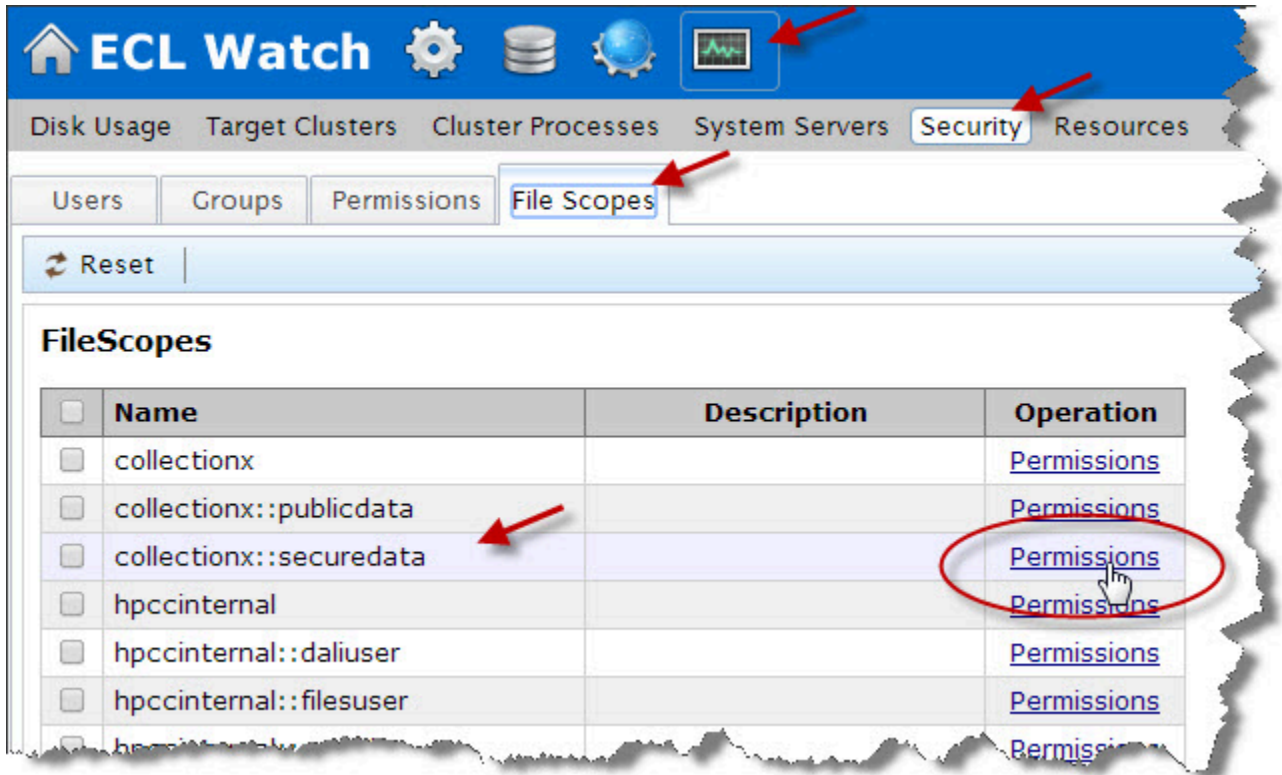
O novo escopo será exibido na lista.

Configurando permissões para escopos de arquivos

Você precisa estabelecer permissões para os escopos de arquivo dos usuários ou grupos. Se desejar aplicar o escopo em um novo grupo, crie o(s) grupo(s) como requerido.

Para configurar as permissões de escopo de arquivos, clique no ícone **Operations** e no link **Security** a partir do submenu de navegação.

1. Selecione a aba **File Scopes**.
2. Selecione o escopo a ser modificado. Clique no link **Permissions** desse escopo.



3. As permissões definidas para os usuários e grupos desse escopo serão exibidas.

Disk Usage Target Clusters Cluster Processes System Servers **Security** Resources

Users Groups **Permissions** File Scopes

Reset

Permissions of collectionx::securedata

Account	allow				deny				Operation
	access	read	write	full	access	read	write	full	
Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete update
Authenticated Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete update
EmilyKate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete update
Jimmy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	delete update

Add

- Marque (ou desmarque) as caixas de seleção nas colunas **allow** e **deny** dos usuários ou grupos exibidos.
- Para adicionar usuários ou grupos ao escopo, pressione o botão **Add**.
- A caixa de diálogo Adicionar permissão será exibida.
- Selecione o usuário ou o grupo que deseja adicionar a permissão a partir da lista suspensa.

Disk Usage Target Clusters Cluster Processes System Servers **Security**

Users Groups Permissions **File Scopes**

Reset

Add Permission for collectionx::securedata

Select user: none

Or group: none

allow:

access	read	write	full
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

deny:

access	read	write	full
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add

Add user or group permission drop list

Após ter selecionado o usuário ou grupo, o botão Adicionar e as caixas de seleção “permitir” e “negar” serão ativadas.

7. Marque as caixas “permitir” e “negar” para configurar as permissões para este escopo.

Users Groups Permissions File Scopes

Reset

Add Permission for collectionx::securedata

Select user: guser

Or group: none

allow: access read write full

deny: access read write full

Add

8. Pressione o botão **Adicionar** .

9. As alterações serão salvas automaticamente. Feche a(s) aba(s).

Permissões de escopo de arquivos

Abaixo da lista de escopo de arquivos há botões que permitem:

- Redefinir o(s) arquivo(s) selecionado(s) para **Default Permissions** .

Isso permite remover rapidamente quaisquer configurações de permissão adicionadas a um arquivo e redefinir para o acesso padrão.

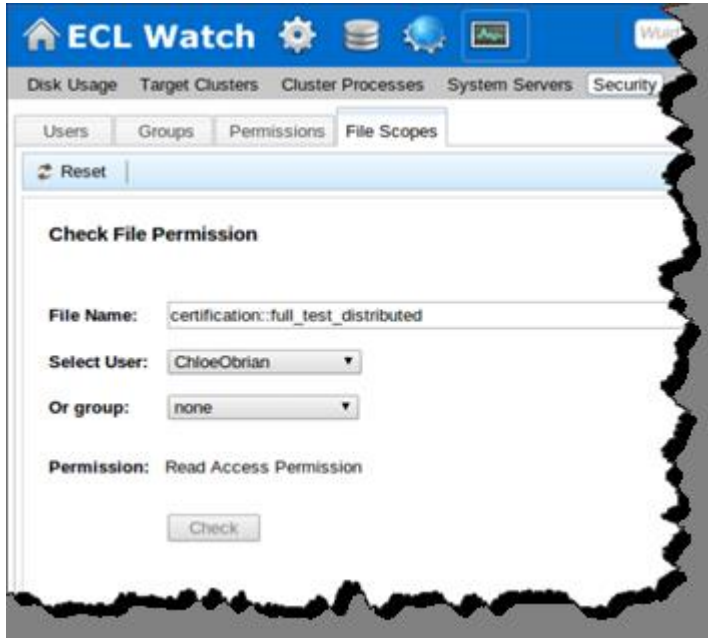
- Permitir ou negar acesso aos arquivos físicos na zona de entrada de arquivos

Isso oferece uma maneira de permitir ou negar acesso ao escopo de arquivo principal.

Por padrão, apenas os administradores têm acesso a esse escopo.

- Verificar permissões do arquivo para um usuário ou grupo

Isso oferece uma maneira de verificar o acesso de um usuário ou grupo a um arquivo lógico.



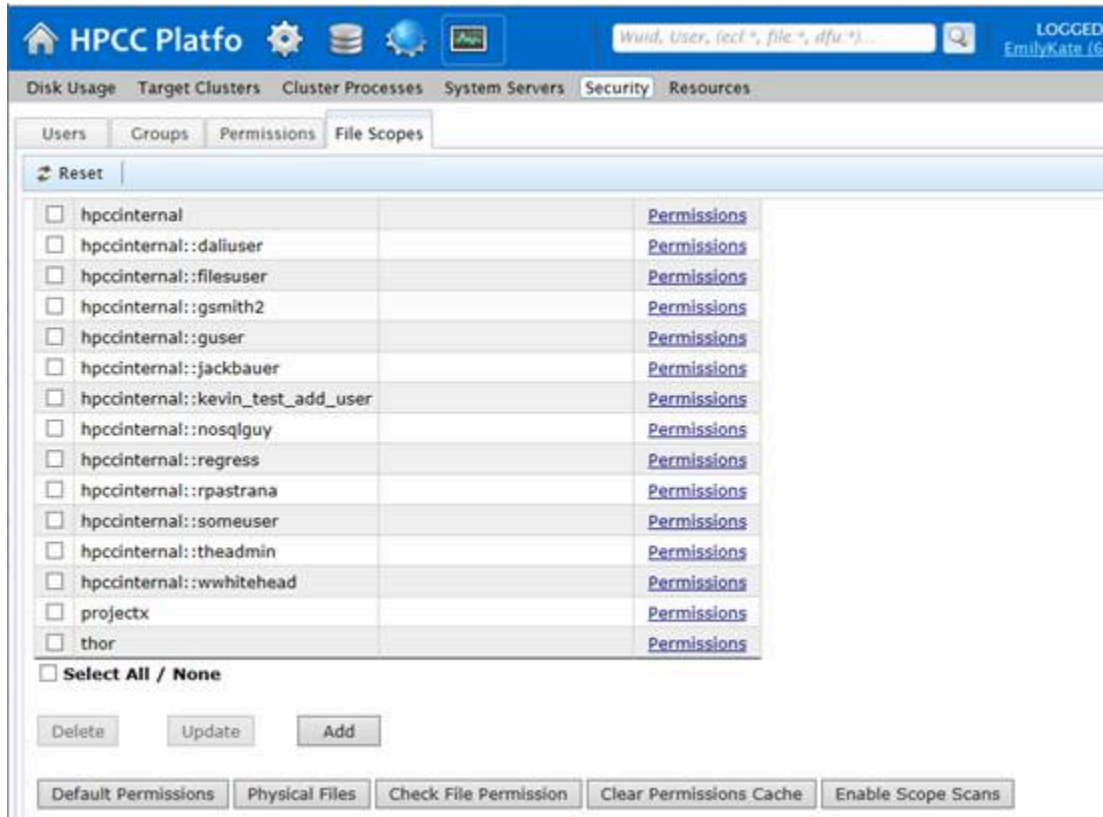
- Limpar cache de permissões

Isso limpa o cache de permissões e permite que quaisquer outras configurações de permissão passem a vigorar de imediato.

- Habilitar/Desabilitar busca de escopo

Isso fornece meios de habilitar ou desabilitar busca de escopo. Habilite a busca de escopos para verificar permissões de acesso aos escopos para os usuários. Este procedimento afetará o desempenho. A função Disable busca de escopo ignora quaisquer permissões de escopo e remove todos os controles de acesso, mas melhora o desempenho. Desabilitar o controle de acesso não é recomendado.

Mudar essa configuração através do ECL Watch, como descrito aqui, é apenas uma substituição temporária. Quando o Dali é reiniciado, essa configuração será revertida para seu estado definido na configuração environment.xml.



Controle de Acesso a Workunit

Existem 2 aspectos sobre a segurança da tarefa (WU) security:

- A Autenticação de recursos para workunit permite configurar permissões para controlar se os usuários podem visualizar suas próprias WUs e/ou as WUs de outros usuários.
- A segurança do escopo do workunit permite configurar permissões para escopos individuais da WU. Todas as workunit possuem um valor de escopo. Todas as tarefas possuem um valor de escopo.

Ambos os métodos podem ser usados (separadamente ou em conjunto), e a restrição mais estrita sempre se aplica.

Em outras palavras, se alguém tiver permissão para ver as WUs no escopo *johndoe*, mas não tem permissão para ver as WUs de outros usuários nas permissões de Autenticação de recursos, esse usuário terá o acesso à visualização de WUs no escopo *johndoe* negado.

Por outro lado, se o usuário tiver permissão de acesso à visualização de WUs de outros usuários, mas não tiver permissão de acesso ao escopo *johndoe* da WU, esse usuário poderá ver outras WUs nesse escopo.

Observação: Caso não tenha acesso à WU, você nunca poderá visualizá-la ou sequer saber da sua existência.

Por padrão, uma WU enviada possui o escopo da ID do usuário. Por exemplo, a WU que JohnDoe enviou possui o valor *scope=johndoe* na WU. Este valor em uma WU permite que ESP e seus serviços LDAP verifiquem as permissões e as coloquem em vigor.

Você pode substituir o escopo padrão usando o código ECL:

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

Protegendo os escopos dos workunits

ESP (na inicialização) cria automaticamente uma OU no LDAP denominada **Workunits** (a menos que ele já exista). Se uma OU de escopo específico não existir no LDAP (p.ex., o escopo johndoe usado no exemplo anterior), as permissões da OU primária serão usadas. Todos os escopos da WU estão localizados abaixo da OU das *workunit*, tanto de forma implícita quanto explícita.

Se uma OU de escopo específico não existir no LDAP (p.ex., o escopo johndoe usado no exemplo anterior), as permissões da OU primária serão usadas. Em outras palavras, o escopo de *johndoe* está implicitamente abaixo da OU *workunit* mesmo não estando listado de maneira explícita na estrutura do LDAP; consequentemente, ele usaria as permissões concedidas às *workunit primárias*

Permissões de Recursos de Workunits

Ao usar o recurso de **escopos da Workunit** na área **Permissions** do ECL Watch, as permissões de qualquer escopo podem ser redefinidas para as configurações padrão de permissão para seu sistema. As configurações de permissão para os Escopos de tarefa podem ser definidas da seguinte forma:

Descrição	Acesso
View WUs in that scope (Visualização de WUs nesse escopo)	Leitura
Create/modify a WU in that scope (Criar ou modificar uma WU nesse escopo)	Gravação
Delete a WU in that scope (Remover uma WU nesse escopo)	Completo

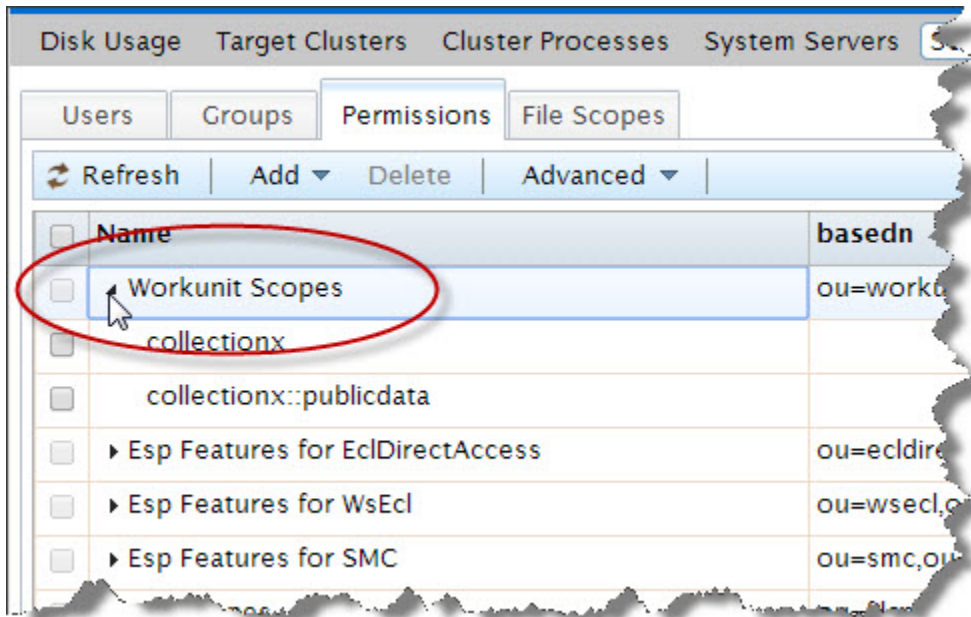
Permissões de Recursos das Workunits

Para adicionar permissões ao escopo de tarefa, clique no ícone **Operations** e no link **Security** a partir do submenu de navegação.

1. Clique na **aba** Permissions.

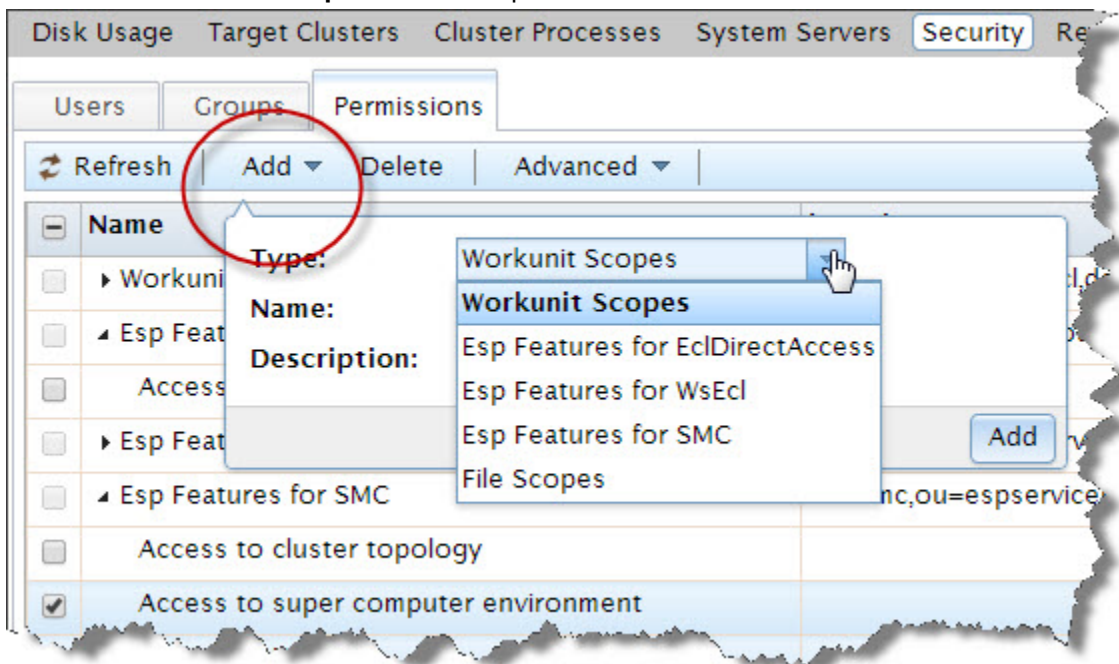
Os recursos específicos serão exibidos.

2. Clique na seta à esquerda do recurso **Workunit Scopes** para exibir os escopos do arquivo.

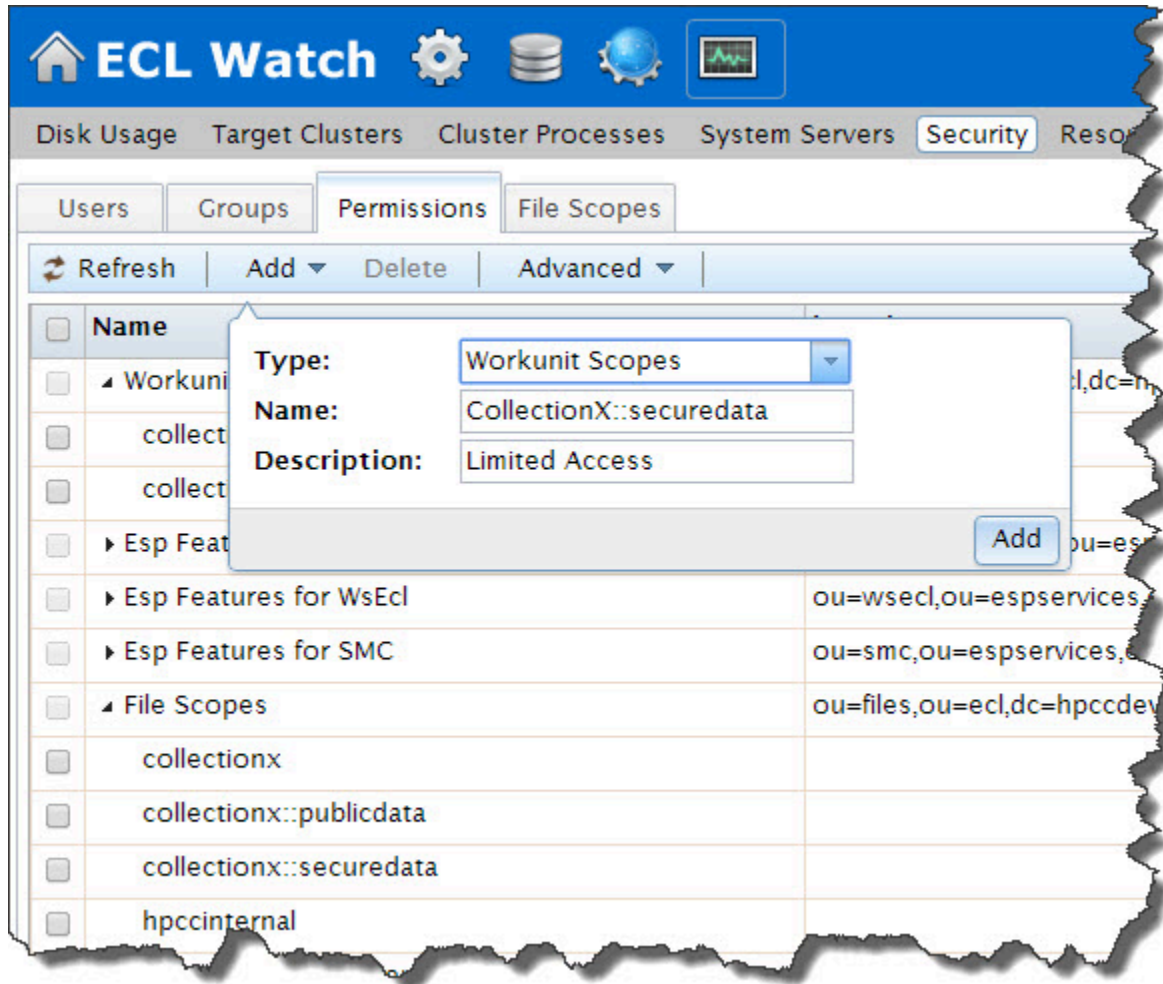


3. Pressione o botão **Add**.

4. Selecione **Workunits Scopes** na lista suspensa.



5. Digite no o nome exato do escopo que deseja adicionar. **Digite no campo Name** o nome exato do escopo que deseja adicionar.



Digite uma breve descrição no campo **Description** .

6. Pressione o botão **Add** .

O novo escopo será exibido na lista.

Ajustar permissões do Escopo.

Aplique os escopos de workunit a um grupo. Se desejar aplicar o escopo em um novo grupo, crie o(s) grupo(s) como requerido.

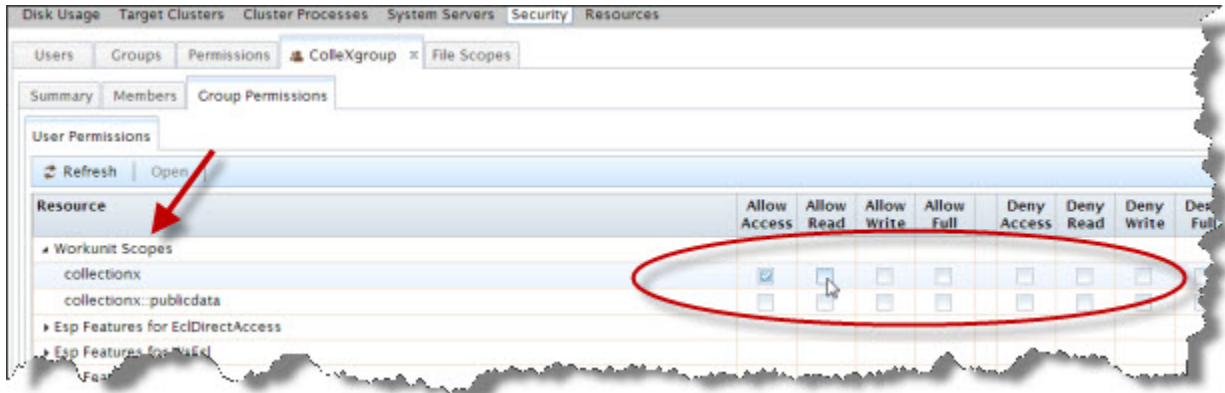
1. Vá para a aba **Groups** .

2. Selecione um grupo no qual deseja aplicar o escopo marcando a caixa ao lado do nome do grupo.

Pressione o botão de ação **Open** . Você pode selecionar múltiplos grupos; uma guia será aberta para cada um deles.

3. Selecione a aba **Group Permissions** para esse grupo. (caso tenha selecionado mais de um grupo, realize esse mesmo procedimento para cada grupo)

4. Clique na seta à esquerda de Workunit Scopes para exibir os escopos disponíveis.



Os escopos de tarefa serão exibidos. Marque as caixas de forma adequada para configurar as permissões para este escopo.

5. Para configurar as permissões neste escopo para outro grupo, abra e acesse a guia do grupo desejado.
6. Para configurar permissões neste escopo para um usuário, selecione a guia.
7. Selecione o usuário e pressione o botão de ação Edit.

Uma nova guia será aberta para esse usuário.

8. Nessa aba, clique na sub-aba **User Permissions**.
9. Localize o novo escopo listado no recurso apropriado.

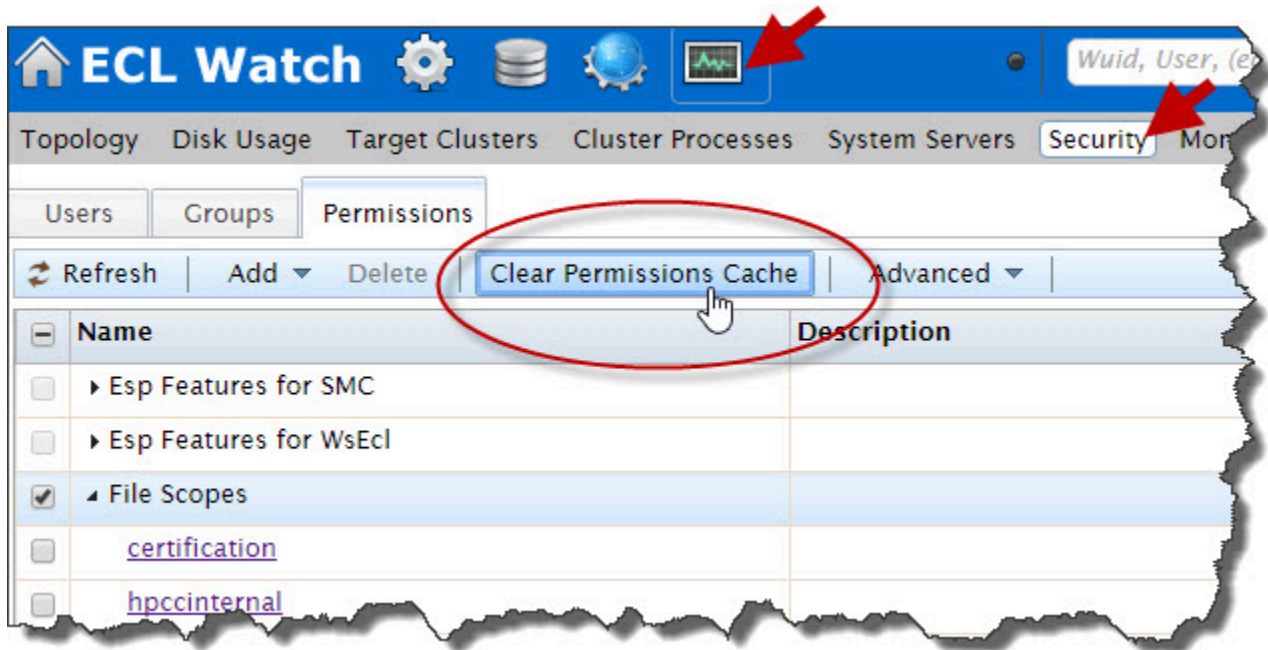
Configure as permissões de acesso da forma adequada para esse usuário.

10. As alterações serão salvas automaticamente. Feche a(s) aba(s).

Cache de Permissão

O botão *Clear Permissions Cache* é um recurso bastante útil e pode ser encontrado na aba Permissions. O botão *Clear Permissions Cache* apaga as permissões armazenadas em cache do Dali e da ESP.

Ao alterar uma permissão no ECL Watch, as configurações são armazenadas em cache no servidor da ESP e armazenadas no servidor Dali. As informações armazenadas em cache são atualizadas em um intervalo configurável. Esse intervalo pode ser definido no Configuration Manager, na aba *LDAP Server settings Attributes*. O tempo limite padrão do cache é 5 minutos.

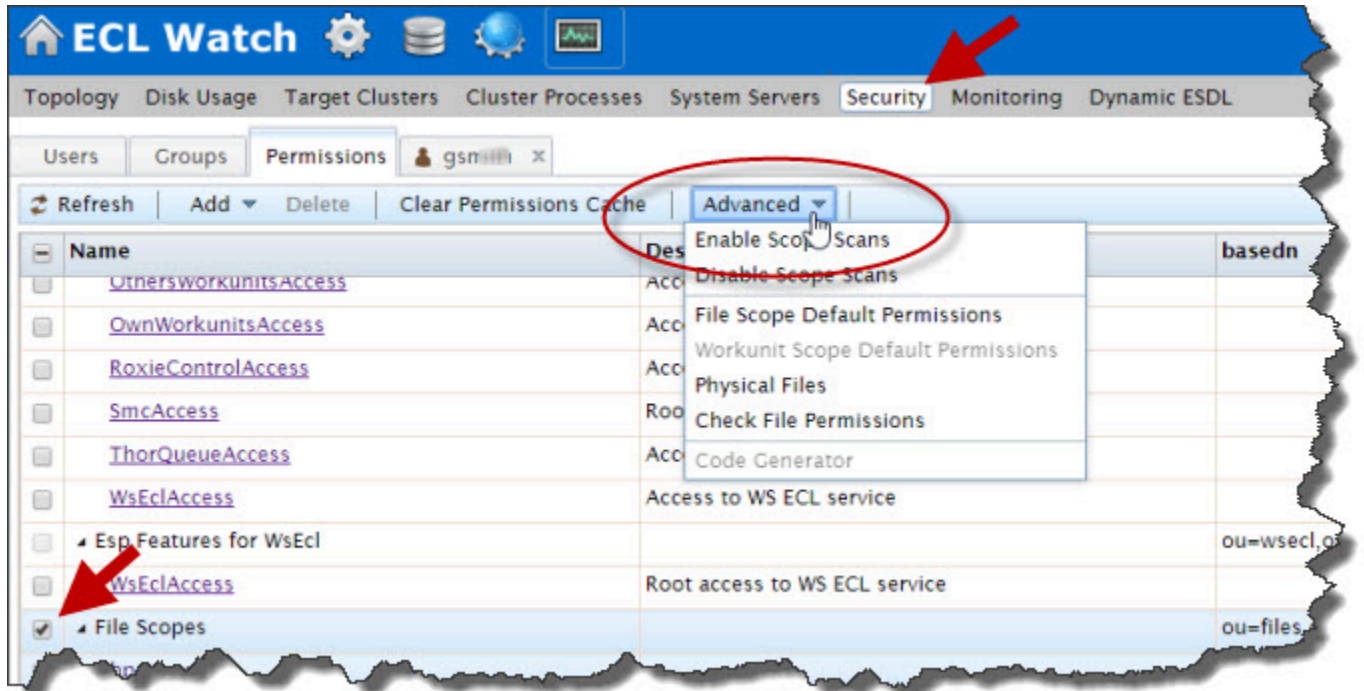


O Cache de permissões pode ser apagado de qualquer lugar na aba ECL Watch Permissions.

Se quiser que uma alteração de permissão comece a vigorar de imediato, apague o cache e force o Dali a atualizar as configurações de permissão pressionando o botão **Clear Permission Cache**. Esta ação transfere as configurações ao pressionar o botão. Use esse recurso criteriosamente, pois o desempenho geral do sistema será temporariamente afetado enquanto as configurações do LDAP são preenchidas novamente na Armazenagem de dados do Dali System.

Permissões Avançadas

Trata-se do botão **Advanced** (Permissions) localizado na aba Permissions. O botão/menu Advanced oferece acesso ao gerenciamento da segurança do escopo de arquivos e workunit. O botão Advanced é habilitado apenas quando você selecionar Files Scope ou Workunit Scopes na aba Permissions.

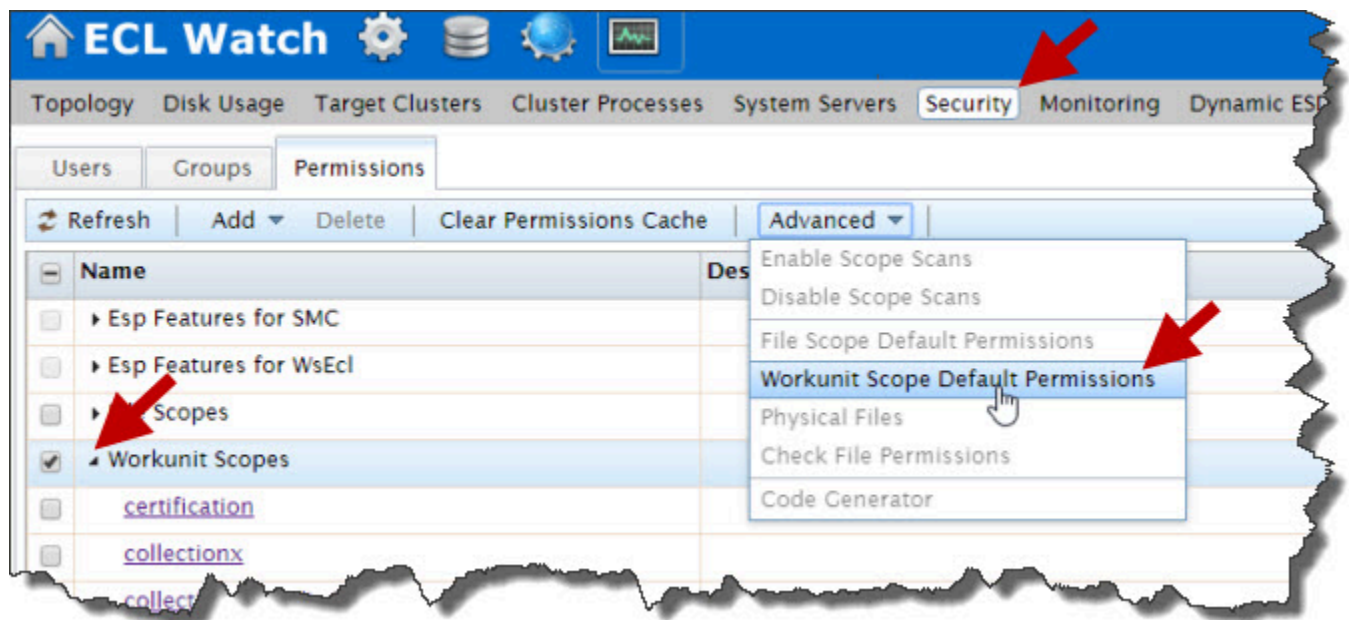


Pressione o botão Advanced para exibir o menu de permissões avançadas. O menu Advanced é sensível ao contexto, portanto, se você selecionar Escopo de arquivos na aba Permissions, poderá optar apenas por aplicar as permissões dos escopos de arquivo que são relevantes; isso também se aplica ao selecionar escopos de tarefa.

Verificações de arquivos

Usando o menu Avançado com a opção Escopo de arquivos selecionada:

- Habilite ou desabilite a segurança do escopo de arquivos
- Acesse a página de permissão padrão do escopo de arquivos
- Acesse a página de permissão para Arquivos físicos.
- Verificar as permissões do arquivo – Essa opção abre uma caixa de diálogo onde é possível inserir um nome de arquivo e selecionar usuários ou grupos para o escopo de segurança do arquivo.



Verificação de tarefa

O uso do menu Avançado com a opção Escopos de tarefa selecionada abre apenas a guia Permissões padrão das Permissões dos Escopos de tarefa (Padrão).

OBSERVAÇÃO: A segurança dos escopos de tarefa ou de arquivo precisa estar habilitada nas configurações do seu sistema para que você possa usar o recurso de segurança dos escopos de tarefa ou de arquivo no sistema.

Configurando o Servidor ESP para utilizar HTTPS (SSL)

O servidor Enterprise Service Platform (ESP) do HPCC suporta o protocolo SSL usado para enviar e receber dados ou documentos privados.

O SSL funciona com uso de uma chave privada para criptografar e descriptografar dados transferidos pela conexão por SSL. Por convenção, URLs que usam uma conexão por SSL começam com HTTPS em vez de HTTP.

A opção do SSL no ESP Server permite uma comunicação segura e criptografada entre um navegador ou a aplicação SOAP client e a plataforma do HPCC.

Os recursos do SSL são configurados no Configuration Manager, porém exigem que um certificado seja instalado no servidor ESP. As bibliotecas OpenSSL oferecem formas de criar os arquivos do certificado necessário em uma das duas formas.

- Você pode usar as bibliotecas OpenSSL para criar uma chave privada e uma Certificate Signing Request (CSR) para adquirir um certificado de um Certificate Issuing Authority (como a VeriSign).
- Você pode usar essa CSR para gerar seu próprio certificado autoassinado e, em seguida, para instalar o certificado e a chave privada em seu ESP Server.

De qualquer forma, uma vez instalado e configurado, o tráfego de rede é criptografado e protegido. As chaves pública e privada usam a criptografia RSA de 2048 bit.

Essas chaves do servidor são lidas durante a execução pelo processo ESP. É importante que as chaves instaladas tenham o owner e permissões corretas. Normalmente, é o usuário HPCC e sua chave pública (certificate.cer) com permissões de leitura como 0444 (ou 0644), juntamente com a chave privada (privatekey.cer) com permissões mais restritivas de 0400 (ou 0600).

Gerar uma Chave RSA Private

Use o toolkit OpenSSL para criar uma chave privada RSA e uma Solicitação de assinatura do certificado (CSR). Isso também pode ser a base para um certificado auto-assinado. Os certificados auto-assinados são usados internamente ou para testes.

Em nosso exemplo, criamos uma chave privada RSA de 2048 bit que é criptografada através do algoritmo 3 DES e armazenada no formato Privacy Enhanced Mail (PEM).

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

Quando solicitado, informe uma frase secreta. Ela será usada como base da criptografia.

Lembre-se desta frase secreta, pois você terá que inseri-la no Configuration Manager mais tarde.

Gerar um CSR - (Certificate Signing Request)

Após ter uma chave privada, você pode usá-la para criar uma Solicitação de Assinatura do Certificado (CSR). Sua CSR pode ser usada para solicitar um certificado assinado de um Órgão de Emissão de Certificados (como VeriSign ou Network Solutions). Você também pode usar a CSR para criar um certificado autoassinado.

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

Responda as perguntas quando solicitado:

Nome do país (código de 2 letras):	
Nome do estado ou província (nome completo):	
Nome da localidade (p.ex., cidade):	
Nome da organização (p.ex., empresa):	
Nome da Unidade organizacional (p.ex., seção):	
Nome comum (p.ex., nome do host do servidor):	
Endereço de e-mail:	
Uma senha de desafio (opcional):	
Outro nome de empresa (opcional):	

Gerar um Certificado Auto-assinado

Para gerar um certificado temporário, válido por até 365 dias, preencha o comando a seguir:

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

Quando solicitado, digite a frase secreta usada anteriormente ao criar seu CSR.

Instalando um Certificado e Chave Privada para o seu servidor ESP

Você deve instalar o certificado e a chave privada em **todos** os nós do servidor ESP que hospedarão um serviço de conexão usando SSL. Copie as chaves e certificados para os locais corretos e defina o owner a propriedade e as permissões apropriadas

Sua chave privada e seu certificado devem ser copiados para /var/lib/HPCCSystems/myesp/conforme ilustrado no exemplo a seguir:

1. Copiar o arquivo do certificado (crt) para o diretório no servidor(s) ESP:

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

2. Alterar o owner do arquivo do HPCC:

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

3. Configurar permissões do arquivo:

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

4. Copiar a chave privada para o servidor(es) ESP:


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

5. Alterar o owner do arquivo do HPCC:

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

6. Configurar permissões do arquivo:

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

Configurar o HTTPS no seu Servidor ESP

Inicie o Configuration Manager em Modo Avançado

1. Inicie o serviço do Configuration Manager em um nó (geralmente o primeiro nó é considerado como o nó principal e é usado para esta tarefa, mas isso fica a seu critério).

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

2. Usando um navegador de Internet, acesse a interface do Configuration Manager.

Use o URL de `http://nnn.nnn.nnn.nnn:pppp`, onde `nnn.nnn.nnn.nnn` é o endereço IP do nó que está executando o Configuration Manager e `pppp` é a porta (o padrão é 8015).

O assistente de inicialização do Gerenciador de Configurações é exibido.

3. Selecione **Visão avançada**.

4. Selecione um arquivo XML da lista suspensa.

Essa lista é preenchida a partir das versões de um arquivo XML no diretório `/etc/HPCCSystems/source/` do seu servidor.

Dica: O arquivo XML correspondente ao `environment.xml` ativo será destacado.

5. Pressione o botão **Avançar**.

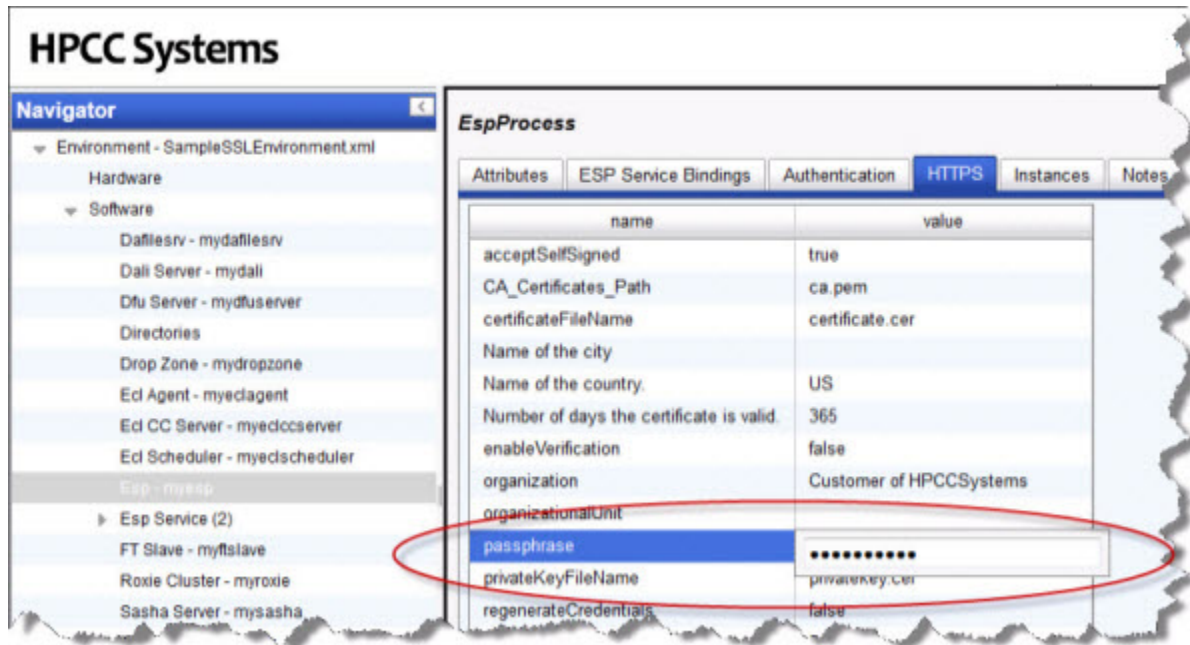
A interface Advanced View do Configuration Manager será exibida.

6. Marque a caixa **Write Access** no topo da página.

Configurar o ESP

1. Selecione ESP - MyEsp no painel do navegador ao lado esquerdo.
2. Selecionar a guia **HTTPS**.

Figure 11. Selecionar guia HTTPS

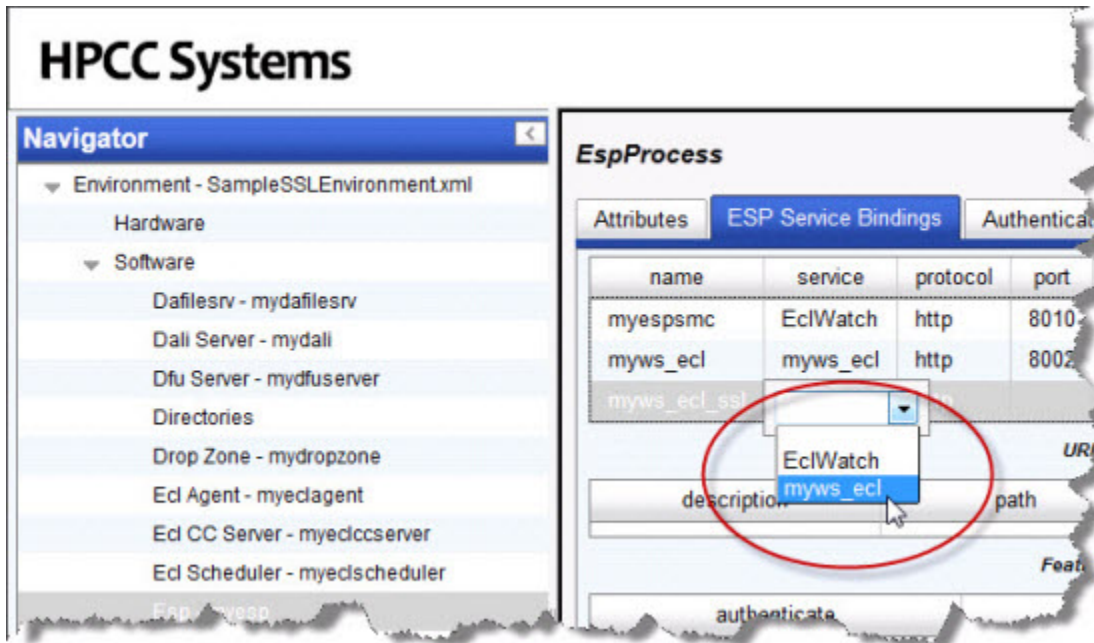


3. No controle de entrada da **passphrase (frase secreta)**, digite a frase secreta usada anteriormente ao criar sua chave privada.
4. Quando solicitado, informe a frase secreta novamente.
5. Clique no ícone de disco para salvar.

Configurar uma ou mais conexões de serviços com SSL ativado.

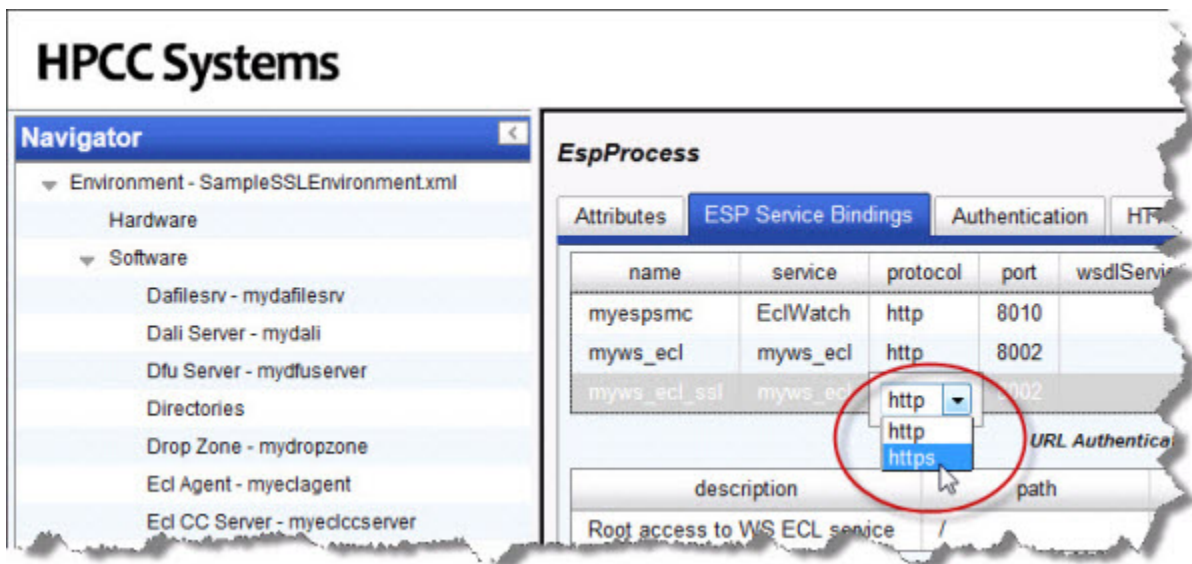
1. Selecione a aba ESP Service Bindings.
2. Clique com o botão direito na lista de serviços e selecione **Add**.
3. Forneça um nome para a ligação (p.ex., myws_ecl_ssl)
4. Selecione myws_ecl na lista suspensa de serviços.

Figure 12. myws_ecl



5. Selecione https na lista suspensa de protocolos.

Figure 13. Selecionar HTTPS



Observação: Caso não tenha editado previamente a porta, a alteração de http para https faz com que o Configuration Manager altere automaticamente a porta para a porta padrão usada para https (18002). Essa alteração ocorrerá automaticamente apenas se a porta não tiver sido editada.

6. Clique no ícone de disco para salvar.

Para garantir a segurança, depois de confirmar o acesso ao seu serviço de maneira segura via https, você deve excluir a conexão que faz uso de http. Em seguida, repita o processo para **todas** as outras conexões.

Distribuir o arquivo de configuração do ambiente para todos os nós, Reiniciar e Certificar

Após ter configurado seu ambiente da forma desejada, é preciso copiar o arquivo de configuração para os demais nós.

1. Se o sistema estiver em execução, pare o sistema.

Certifique-se de que o sistema não esteja em execução antes de tentar mover o arquivo `environment.xml`.

2. Salve o arquivo `environment.xml` em um backup.

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

Observação: o arquivo `environment.xml` do ambiente em execução está localizado em seu diretório **/etc/HPCCSystems/**. O Gerenciador de Configurações funciona em arquivos no diretório **/etc/HPCCSystems/source**. É necessário copiar o arquivo XML deste local para criar um arquivo `environment.xml` ativo.

3. Copie o novo arquivo `NewEnvironment.xml` do diretório de origem para `/etc/HPCCSystems` e renomeie o arquivo para `environment.xml`

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

4. Copie o **/etc/HPCCSystems/environment.xml** para o **/etc/HPCCSystems/** em cada nó.

Se preferir, use um script para automatizar essa etapa, especialmente se você tiver muitos nós. Consulte a seção `Scripts` de exemplo na seção `Anexos` do manual `Como instalar e executar a plataforma do HPCC`.

5. Reinicie o HPCC System e certifique os componentes como de costume.

Configurando SSL para o Roxie

O Roxie também pode ser configurado para usar o protocolo SSL. Caso já tenha configurado o ESP Server para usar o protocolo SSL, como descrito na seção anterior, você pode já ter concluído algumas dessas etapas. Consulte a seção SSL para ESP para obter mais informações sobre como criar chaves e certificados.

Configurar o HTTPS no seu Servidor de cluster Roxie

Inicie o Configuration Manager em Modo Avançado

1. Inicie o serviço do Configuration Manager em um nó (geralmente o primeiro nó é considerado como o nó principal e é usado para esta tarefa, mas isso fica a seu critério).

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

2. Usando um navegador de Internet, acesse a interface do Configuration Manager.

Use o URL de `http://nnn.nnn.nnn.nnn:pppp`, onde `nnn.nnn.nnn.nnn` é o endereço IP do nó que está executando o Configuration Manager e `pppp` é a porta (o padrão é 8015).

O assistente de inicialização do Gerenciador de Configurações é exibido.

3. Selecione **Advanced View**.

4. Selecione um arquivo XML da lista suspensa.

Essa lista é preenchida a partir das versões de um arquivo XML no diretório `/etc/HPCCSystems/source/`.

Dica: O arquivo XML correspondente ao `environment.xml` ativo será destacado.

5. Pressione o botão **Avançar**.

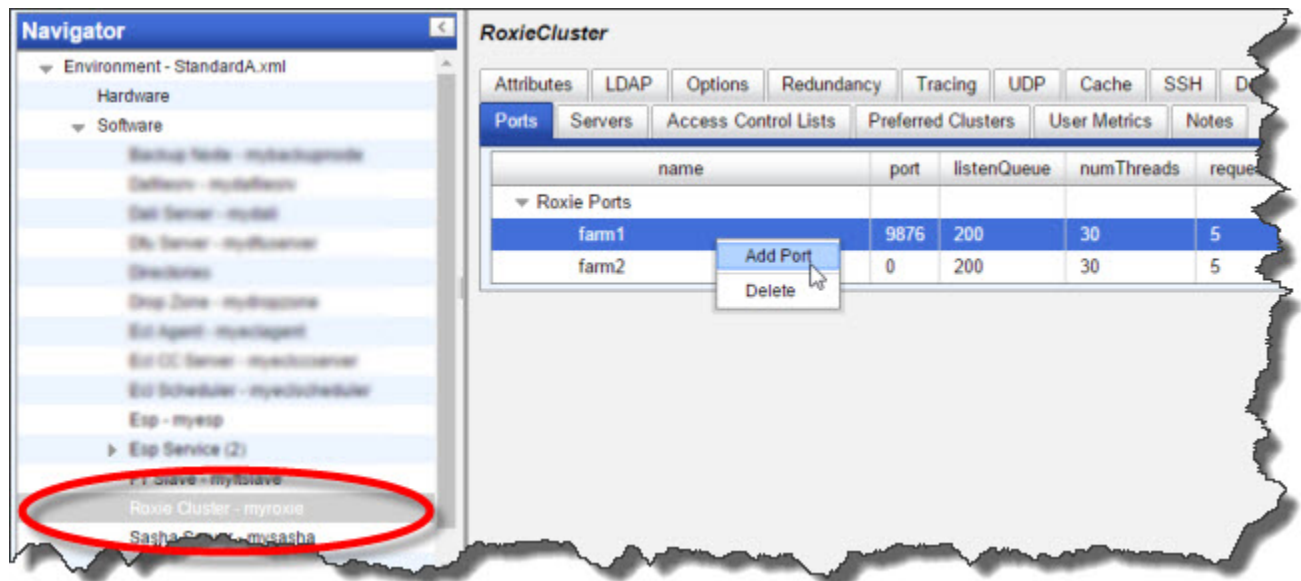
A interface Advanced View do Configuration Manager será exibida.

6. Marque a caixa **Write Access** no topo da página.

Configurar Roxie SSL

1. Selecione seu cluster Roxie no painel do navegador ao lado esquerdo.
2. Selecione a aba **Ports**.
3. Clique com o botão direito na lista de portas e selecione **Add**.

Figure 14. Selecionar a aba Port



4. O número da porta padrão é 9876. Altere o número da porta padrão para, por exemplo, 19876.
5. Mude o protocolo de *Native* para *SSL* no menu suspenso (imagem).
6. No controle de entrada da **passphrase (frase secreta)**, digite a frase secreta usada anteriormente ao criar sua chave privada. Deixe este campo em branco caso não tenha usado uma frase secreta.
7. Quando solicitado, informe a frase secreta novamente.
8. Insira o nome do arquivo do certificado.
9. Insira o nome do arquivo da chave.
10. Clique no ícone de disco para salvar.

O local de pesquisa padrão para os arquivos de certificado e chave está em `/var/lib/HPCCSystems/myroxie`. Você pode especificar o caminho completo se quiser que esses arquivos estejam em um local diferente. Os arquivos de certificado e chave devem estar disponíveis para cada nó do Roxie.

Distribuir o arquivo de configuração do ambiente para todos os nós, Reiniciar e Certificar

Após ter configurado seu ambiente da forma desejada, é preciso copiar o arquivo de configuração para os demais nós. Para obter mais informações sobre como distribuir seu ambiente, consulte a seção acima Distribuir o arquivo de configuração do ambiente.

Mais Exemplos

Esta seção contém outros exemplos do ECL que podem ser usados no cluster do seu HPCC . Eles podem ser executados em um sistema de nó único ou em um cluster maior com vários nós.

Exemplos de Anagrama

Os exemplos a seguir mostram algumas das coisas que o HPCC Systems pode fazer. A execução desses exemplos ajudará sua compreensão de Sistemas HPCC e ECL.

Exemplo ECL: Anagram1

Este exemplo pega uma STRING e gera todos os anagramas possíveis a partir dela. Este código serve de base para um segundo exemplo que analisa quais destas são palavras reais usando um arquivo de dados da lista de palavras.

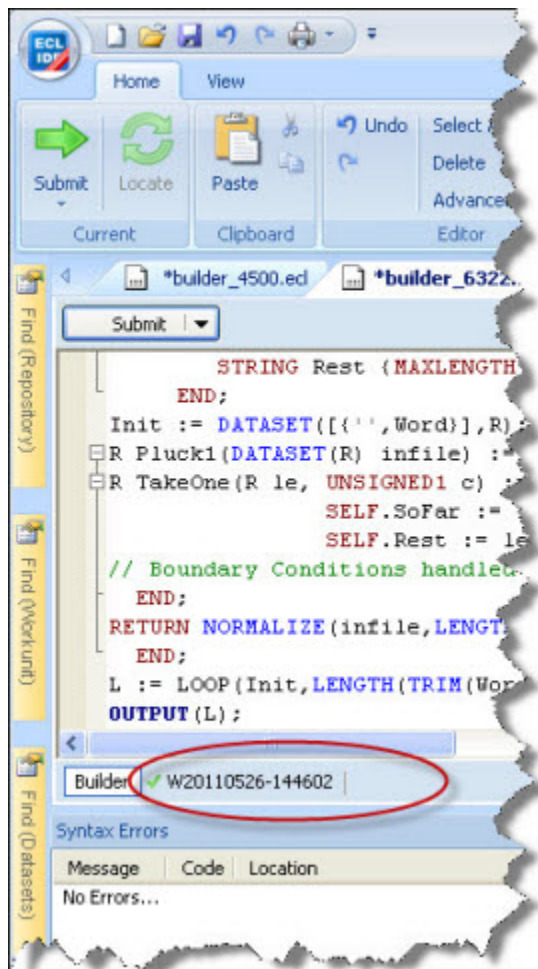
1. Abra o ECL IDE (Start >> All Programs >> HPCC Systems >> ECL IDE) e faça o login no HPCC.
2. Abrir um Nova **Janela do compilador** (CTRL+N) e escreva o seguinte código:

```
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. Selecione **thor** como seu cluster de destino.
4. Pressione o botão de verificação de sintaxe localizado na barra de ferramentas principal (ou pressione F7)

5. Pressione o botão **Submit** (ou as teclas ctrl+enter).

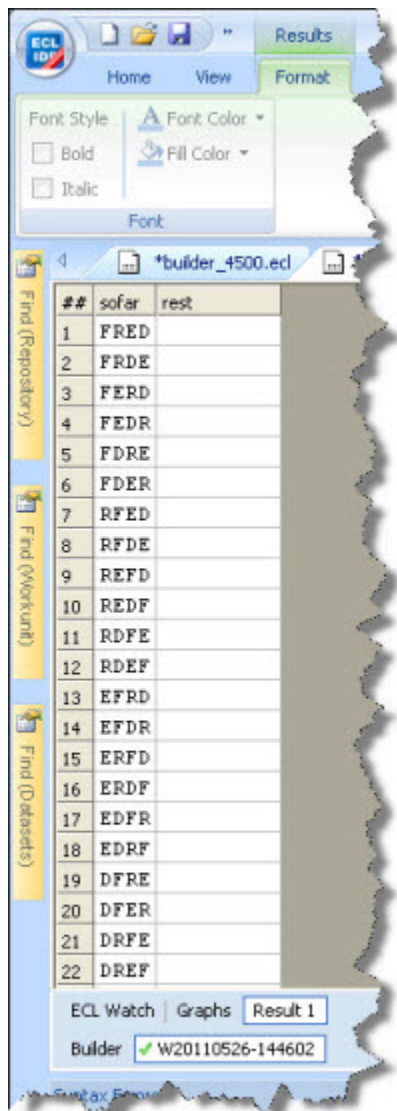
Figure 15. Tarefa concluída



A marcação na cor verde indica uma conclusão bem-sucedida.

6. Clique na aba do número da workunit e, em seguida, na aba Result 1 para ver os resultados.

Figure 16. Resultado do job concluído



##	sofar	rest
1	FRED	
2	FRDE	
3	FERD	
4	FEDR	
5	FDRE	
6	FDER	
7	RFED	
8	RFDE	
9	REFD	
10	REDF	
11	RDPE	
12	RDEF	
13	EFRD	
14	EFDR	
15	ERFD	
16	ERDF	
17	EDFR	
18	EDRF	
19	DFRE	
20	DFER	
21	DRFE	
22	DREF	

Exemplo Roxie: Anagram2

Neste exemplo, vamos baixar um arquivo de dados de código aberto com palavras do dicionário, fazer o spray (distribuir aos nós) desse arquivo para nosso cluster Thor e validar nossos anagramas em relação a esse arquivo para que possamos determinar quais palavras são válidas. A etapa de validação usa um JOIN da lista de anagramas para o arquivo do dicionário. O uso de um índice e de uma junção com chave seria mais eficiente, mas isso serve apenas como um simples exemplo.

Fazer o download da Lista de Palavras

Vamos fazer um download da lista de palavras em <http://wordlist.aspell.net/12dicts>

1. Faça o download o pacote *Official 12 Dicts*. Os arquivos estão disponíveis no formato tar.gz ou ZIP.
2. Extraia o conteúdo do pacote e salve o **2of12.txt**. (normalmente encontrado na subpasta American) para uma pasta em sua máquina local.

Carregar o arquivo de dicionário para sua Landing Zone

Nesta etapa, você copiará os arquivos de dados para um local onde eles possam ser distribuídos aos nós de seu cluster HPCC. Uma Landing Zone é um local de armazenagem anexado a sua plataforma HPCC Systems. Ela possui um utilitário em execução para facilitar o spraying (processo de distribuir dados aos nós) para um cluster.

Para arquivos de dados menores, com tamanho máximo de 2GB, você pode usar o utilitário de upload/download de arquivo no ECL Watch. Este arquivo de dados possui apenas 400 kb (aproximadamente).

Em seguida, você distribuirá (ou fará o spray) o dataset para todos os nós no cluster do HPCC. O poder do HPCC Systems vem da sua capacidade de atribuir vários processadores para trabalhar nas diferentes partes do arquivo de dados em paralelo. Mesmo que sua versão, que possui apenas um nó único, os dados precisam ser distribuídos ao cluster.

1. Em seu navegador, acesse a URL do **ECL Watch**. Por exemplo, <http://nnn.nnn.nnn.nnn:8010>, onde nnn.nnn.nnn.nnn é o endereço IP do seu ESP Server.



Seu endereço IP poderá ser diferente dos endereços fornecidos nas imagens de exemplo. Use o endereço IP fornecido pela **sua** instalação

2. No ECL Watch, clique no ícone **Files** depois clique no link **Landing Zones** no submenu de navegação.

Pressione o botão **Upload** .

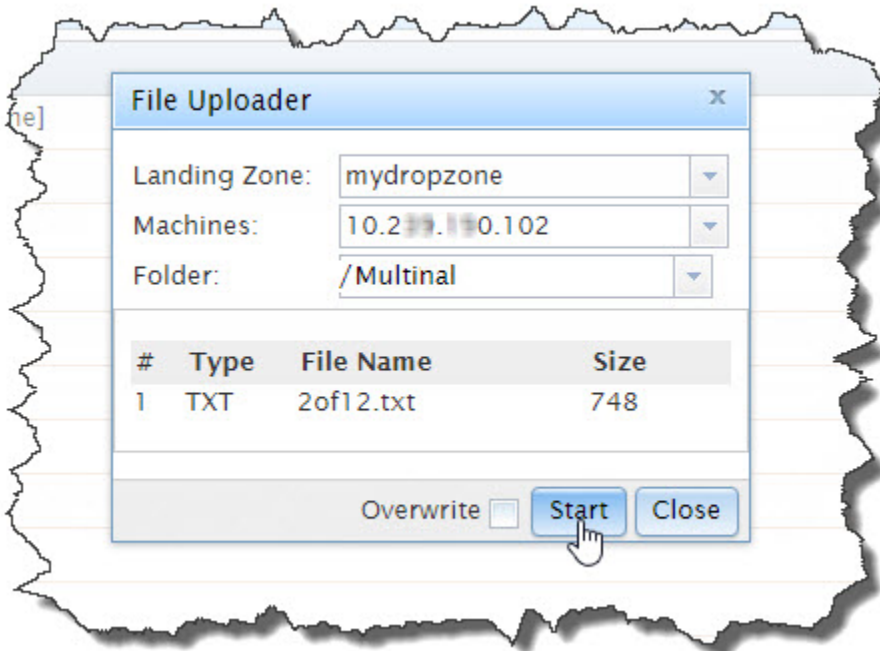
Figure 17. Upload



3. Uma caixa de diálogo será aberta. **Navegue** e selecione o arquivo a ser enviado e pressione o botão **Open** .

O arquivo selecionado deve aparecer no campo **File Name** . O arquivo de dados possui o seguinte nome: **2of12.txt**..

4. **Figure 18. Iniciar a função Enviar arquivo**



Pressione o botão **Start** para concluir o envio do arquivo.

Faça o spray do arquivo de dados para o seu *Cluster da Refinaria de Dados (Thor)*

Para usar o arquivo de dados em seu HPCC System, é preciso fazer o "spray" (distribuir) desse arquivo para todos os nós. O *spray* ou *importação* é a transferência de um arquivo de dados de um local (como a zona de entrada de arquivos) para diversas partes do arquivo ou nós em um cluster.

O arquivo distribuído ou pulverizado(sprayed) passa a ter um *logical-file-name* da seguinte forma: **~thor::word_list_csv** O sistema mantém uma lista de arquivos lógicos e as localizações do arquivo físico correspondente das partes do arquivo.

1. Abra o ECL Watch usando a URL:

http://nnn.nnn.nnn.nnn:pppp (onde nnn.nnn.nnn.nnn é o endereço IP do seu ESP Server e pppp é a porta. A porta padrão é 8010)

2. Clique no link **Files** depois clique no link **Landing Zones** no submenu de navegação. Selecione a zona de entrada de arquivos apropriada (caso haja mais de uma zona de entrada de arquivos). Clique na seta à esquerda da sua zona de entrada de arquivos para expandir.

3. Selecione o arquivo na zona de entrada de arquivos marcando a caixa ao lado dele.

4. Marque a caixa ao lado de 2of12, então pressione o botão **Delimited**.

Figure 19. Spray delimitado

The screenshot shows the 'Spray Delimited' dialog box in the HPCC Systems interface. The 'Target' section is expanded, showing the following configuration:

- Group:** mythor
- Queue:** dfusever_queue
- Target Scope:** ~thor
- Target Name:** word_list_csv

The 'Options' section is also expanded, showing the following configuration:

- Format:** ASCII
- Max Record Length:** 8192
- Separators:** \\.
- Omit Separator:** ☐
- Escape:**
- Line Terminators:** \\n,\\r\\n
- Quote:** "
- Overwrite:** ☒ **Replicate:** ☐
- No Split:** ☐ **Compress:** ☐
- Fail If No Source File:** ☐ **Record Structure Present:** ☐
- Quoted Terminator:** ☐ **Expire in (days):**

A 'Spray' button is located at the bottom right of the dialog box.

A página **DFU Spray Delimited** é exibida.

5. Selecione "mythor" na lista suspensa do Grupo de destino.
6. Preencha o Target Scope (Escopo de destino) como *thor*.

7. Preencha os demais parâmetros (caso ainda não tenham sido preenchidos).

- Máximo tamanho do registro 8192
- Separador \,
- Terminador de linhas \n,\r\n
- Aspas: '

8. Preencha o Target Name usando o restante do nome do arquivo lógico desejado: word_list_csv

9. Certifique-se de que a caixa **Overwrite** esteja selecionada.

Se disponível, certifique-se de que a caixa **Replicate** esteja selecionada. (A opção Replicate está disponível apenas em sistemas em que a replicação tenha sido ativada.)

10. Pressione o botão **Spray**.

A guia exibe a workunit DFU onde é possível ver o progresso do spray (distribuição aos nós).

Executa a consulta no Thor

1. Abrir um Nova **Janela do compilador** (CTRL+N) e escreva o seguinte código:

```
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, UNSIGNED c) := TRANSFORM
    SELF.SoFar := le.SoFar + le.Rest[c];
    SELF.Rest := le.Rest[..c-1]+le.Rest[c+1..];
  // Boundary Conditions
```

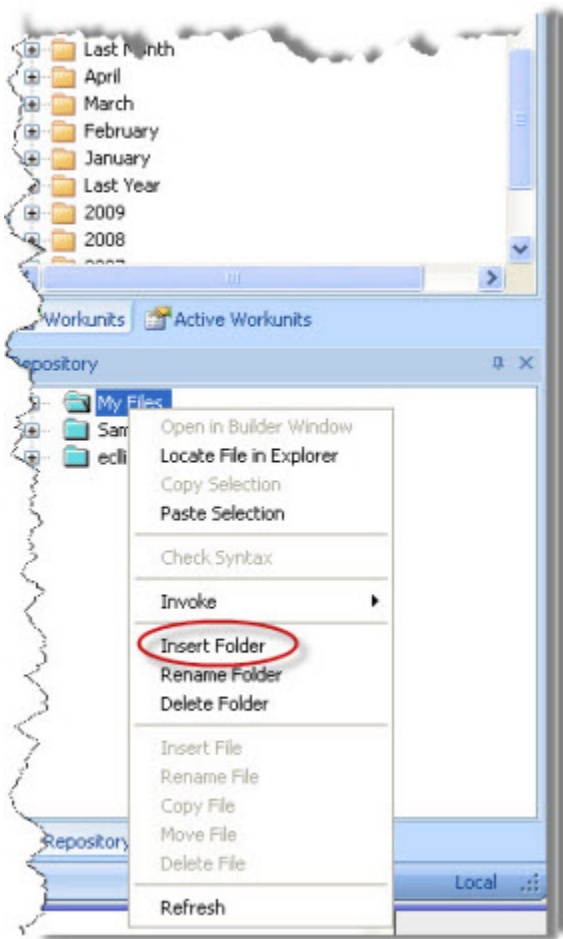
```
// handled automatically
END;
RETURN DEDUP(NORMALIZE(infile,LENGTH(LEFT.Rest),TakeOne(LEFT,COUNTER)));
END;
L := LOOP(Init,LENGTH(CleanedWord),Pluck1(ROWS(LEFT)));
ValidWords := JOIN(L,File_Word_List,
LEFT.SoFar=Std.Str.ToUpperCase(RIGHT.Word),TRANSFORM(LEFT));
OUTPUT(CleanedWord);
COUNT(ValidWords);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

2. Selecione **thor** como seu cluster de destino.
3. Pressione o botão de verificação de sintaxe localizado na barra de ferramentas principal (ou pressione F7)
4. Pressione o botão **Submit** .
5. Quando o envio estiver concluído, selecione a aba Workunit e em seguida a aba Results.
6. Examine o resultado.

Compilar e Publicar a consulta para o Roxie

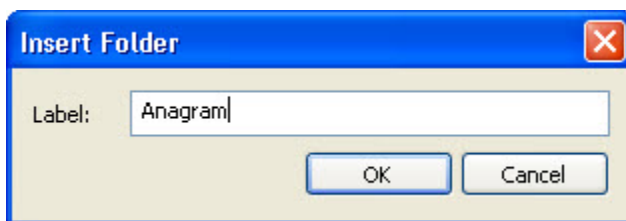
1. Clique com o botão direito na pasta **My Files** na janela Repository, e selecione a opção **Insert Folder** no menu pop-up.

Figure 20. Insert Folder



2. Digite **Anagram2** para o rótulo e pressione o botão OK.

Figure 21. Inserir o título da pasta

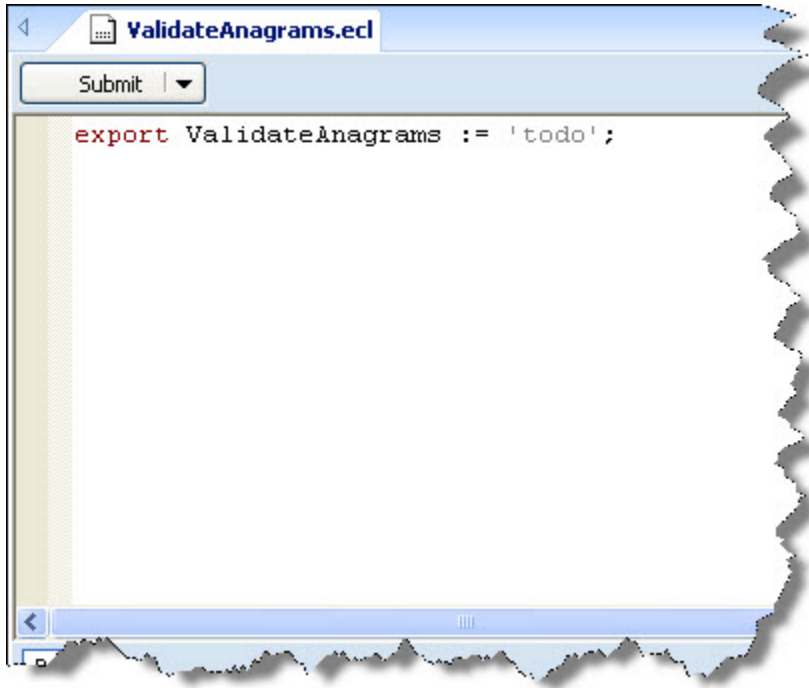


3. Clique com o botão direito na pasta **Anagram** e selecione **Insert File** no menu pop-up.

4. Digite **ValidateAnagrams** para o rótulo e pressione o botão OK.

Uma janela do compilador será aberta.

Figure 22. Janela do compilador



5. Escreva o seguinte código (ele pode ser copiado de outra janela do compilador):

```
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;

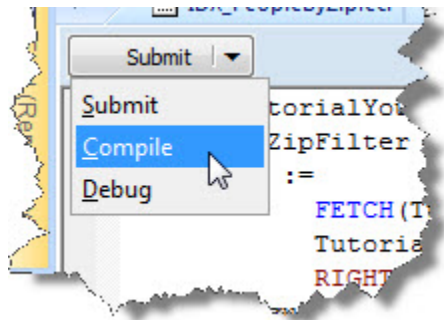
STRING CleanedWord := SortString(TRIM(Std.Str.ToUpperCase(Word)));

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. Selecione **Roxie** como seu cluster de destino.
7. Pressione o botão de verificação de sintaxe localizado na barra de ferramentas principal (ou pressione F7)
8. Na janela do compilador, no canto superior esquerdo **do botão Submit** há uma seta suspensa ao lado. Selecione a seta para exibir a opção **Compilar**.

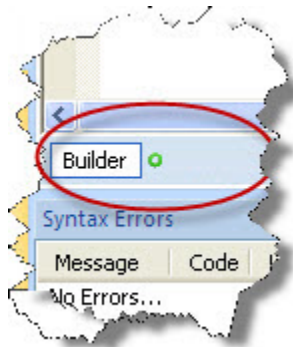
Figure 23. Compilar



9. Selecione **Compilar**
10. Quando o envio estiver concluído, selecione a aba Workunit e em seguida a aba Results.

11.Quando a workunit for concluída, ela exibirá um círculo verde indicando que foi compilada.

Figure 24. Compilada

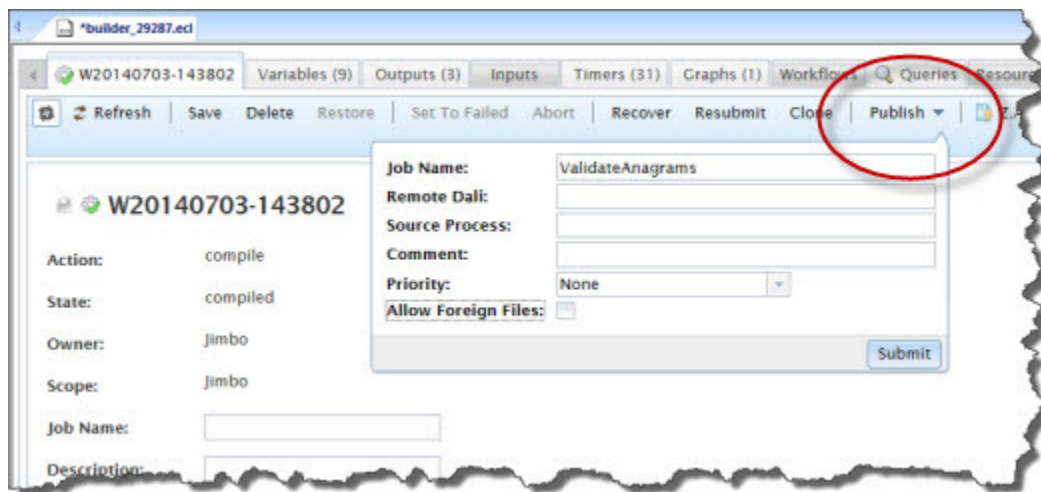


Publicar uma consulta Roxie

Agora vamos publicar a consulta em um cluster Roxie.

1. Selecione a aba workunit para o ValidateAnagrams que você acabou de compilar.
2. Selecionar a aba ECLWatch.
3. Pressione o botão **Publish** , preencha a caixa de diálogo e pressione o botão **Submit**.

Figure 25. Publicar Consulta



Uma mensagem de confirmação será exibida quando a consulta for publicada com sucesso.

Executar a consulta Roxie no WsECL

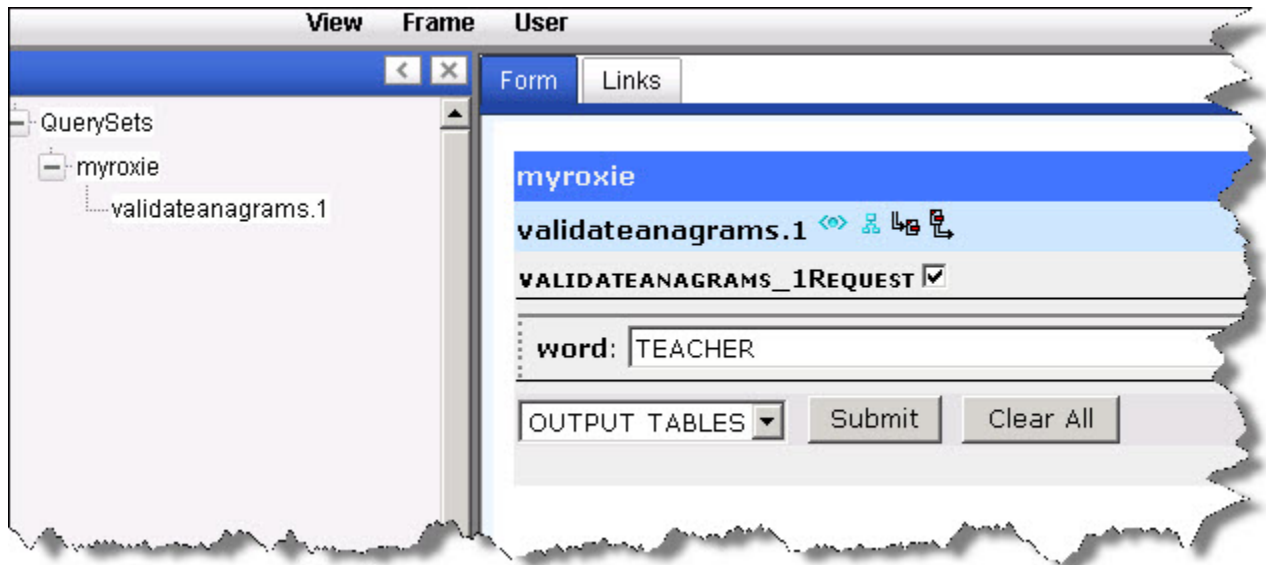
Agora que a consulta foi publicada em um cluster Roxie, podemos executá-la usando o serviço WsECL. WsECL é uma interface Web para consultas em uma plataforma do HPCC . Use a seguinte URL:

<http://nnn.nnn.nnn.nnn:pppp> (onde nnnn.nnn.nnn.nnn é o endereço IP do seu ESP Server e pppp é a porta. A porta padrão é 8002)

1. Clique no sinal + ao lado de **myroxie** para expandir a árvore.
2. Clique no link **ValidateAnagrams.1** .

O formulário do serviço será exibido.

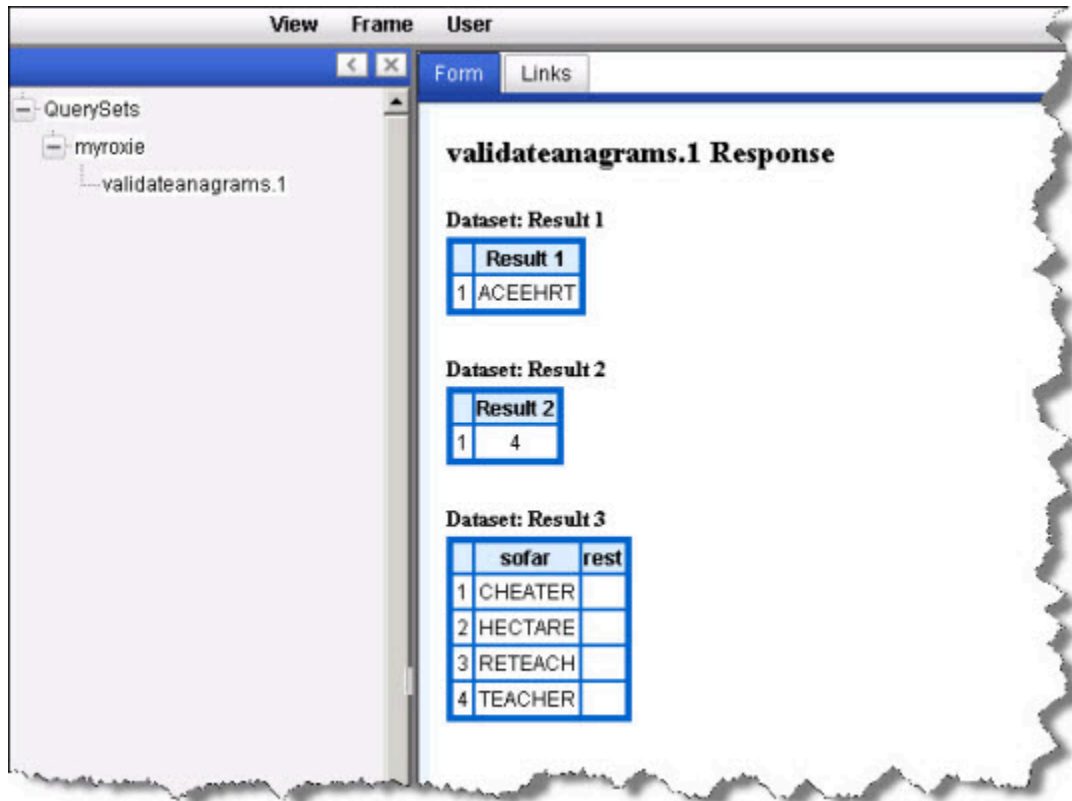
Figure 26. RoxieECL



3. Selecione Tabelas de resultado (Output Tables) na lista suspensa.

4. Forneça uma palavra para que seja feito o anagrama (p.ex., TEACHER) e pressione o botão Submit.
Os resultados serão exibidos.

Figure 27. RoxieResults

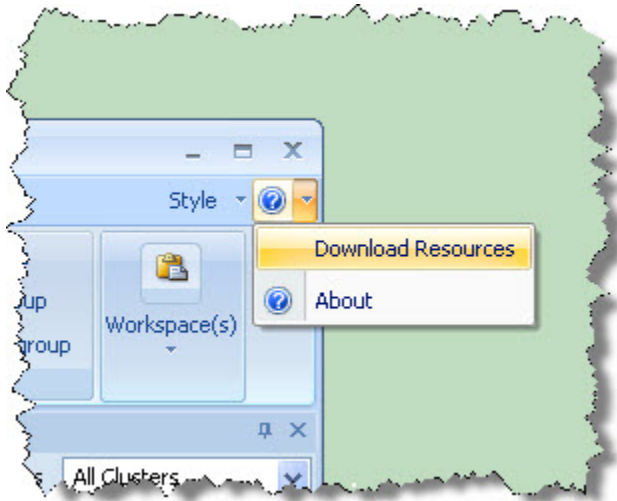


Próximos passos

O menu no ECL IDE disponibiliza vários documentos que fornecem detalhes sobre os vários aspectos do HPCC.

Você pode acessar estes documentos a partir do menu Help (Ajuda): Help >> Documentation.

Figure 28. Menu Help



Você também pode localizar essa documentação no menu Iniciar: **Start** menu :

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

Para se familiarizar com o que o seu sistema é capaz de fazer, recomendamos realizar as seguintes etapas:

- O **Tutorial de Dados**
- O **exemplo** da Teoria dos seis graus de separação de Kevin Bacon
- Ler **Como usar o Gerenciador de Configurações** para aprender como configurar uma plataforma do HPCC usando a Advanced View (Visão Avançada)
- Use suas novas habilidades para processar seu próprio dataset massivo!

O portal do HPCC Systems® também é um recurso valioso para obter mais informações, incluindo:

- Vídeos tutoriais
- Exemplos adicionais
- Informe técnico
- Documentação

Anexo

Scripts de exemplo

Para configuração de vários nós, primeiramente é preciso instalar os pacotes em cada nó. Essa instalação pode ser feita manualmente ou você pode usar os scripts para copiar e instalar os pacotes. A cópia e a instalação em cada nó não é algo prático em um sistema grande que contenha muitos nós. Por isso, fornecemos alguns scripts para você usar ou para servirem de exemplo na preparação de seu próprio script.

Os scripts estão instalados no diretório `/opt/HPCCSystems/sbin`. Os scripts devem ser executados como `sudo` ou um usuário com os privilégios apropriados em todos os nós. Os scripts são capazes de processar multitarefas.



Lembre-se de que você deve ter privilégios suficientes para usar `sudo` como administrador, a fim de usar o script `install-cluster.sh`. Para usar os scripts `hpcc-push.sh` ou `hpcc-run.sh` scripts, é preciso usar `sudo` como usuário do **HPCC**.

install-cluster.sh

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

<package-name>	Nome do pacote do HPCC a ser instalado. Obrigatório
-h	Ajuda Opcional.
-k, --newkey	Quando especificado, o script gera e distribui chaves ssh para todos os hosts. Opcional.
-p, --pushkeydir	Lança a chave ssh existente para a máquina remota. Opcional. Use -k ou -p, mas não ambos.
-n, --concurrent	Quando especificado, denota o número de execuções simultâneas. O padrão é 5. Opcional.

Você pode executar esse script como qualquer usuário com permissões suficientes de execução. Porém, quando o nome do usuário e senha forem solicitados, você deve informar as credenciais de um usuário com direitos sudo suficientes para executar comandos como administrador em todos os nós.

Antes de usar esse script, você precisa ter criado e definido um arquivo `environment.xml` (usando o assistente ou o modo avançado do Gerenciador de Configurações). Este script:

- Lê o arquivo ativo `environment.xml` e reúne uma lista de nós sobre os quais irá agir.
- Instala o(s) pacote(s) da plataforma do HPCC em todos os nós especificados.
- Força e implementa o arquivo de ambiente (`environment.xml`) para todos os nós especificados.
- Opcionalmente, se você especificar a opção -k ele também gera as chaves ssh exigidas e as implementa (como requerido) em todos os nós especificados.
- Opcionalmente, se você especificar a opção -p ele força as chaves ssh existentes para todos os nós especificados. Você pode usar uma das opções -k e -p, porém não as duas.
- Opcionalmente, se você especificar a opção -n <value>, ele gera várias execuções simultâneas. O padrão é 5.

Exemplos:

Este exemplo instala os pacotes da plataforma do HPCC nos nós remanescentes e força o arquivo ativo environment.xml para esses nós:

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

(onde *n.n.nnnn* é o número da compilação)

Este exemplo instala os pacotes da plataforma do HPCC em todos os nós e força o arquivo ativo environment.xml para esses nós: Ele também gera chaves ssh e as força para todos os nós.

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

(onde *n.n.nnnn* o número da compilação)

Este exemplo instala os pacotes da plataforma do HPCC e força o arquivo ativo environment.xml para 8 nós simultâneos:

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

(onde *n.n.nnnn* o número da compilação)

deploy-java-files.sh

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

-c	Quando especificada, essa opção adiciona o diretório de destino ou o caminho de arquivo jar para classpath no environment.conf.
-e	Quando especificado, isso denota que o destino deve ser removido do classpath.
-H	Lista IP do Host Quando especificada, segmentará endereços IP especificados, um endereço IP por linha. Se esta opção não for usada, executará na lista IP gerada no environment.xml
-n	Quando especificado, denota o número de linhas de execução (threads) simultâneas. O padrão é 5. É preciso ter python instalado, caso contrário essa opção será ignorada e a ação será executada sequencialmente em cada host.
-r	Redefine o classpath. Quando especificado, redefinirá o classpath para <install_directory>/classes. Se usado juntamente com -t, adiciona as novas entradas ao classpath após a redefinição.
-s	Arquivo ou diretório fonte.
-t	Diretório de destino O padrão é <install_directory>/classes. Se for apenas para adicionar ao classpath, o valor pode corresponder ao caminho completo do arquivo java jar.
-u	O nome do usuário a ser usado para o acesso do ssh ao sistema remoto. Forneça esta opção quando o usuário especificado não usa uma senha para executar o ssh/scp. Se essa opção não for especificada, você terá que fornecer um nome de usuário e senha. Recomendamos não usar <hpcc user> para evitar problemas de segurança.
-x	Quando especificada, essa opção exclui a execução no host atual.

O **script deploy-java-files.sh** é usado para implementar arquivos java (fonte) nos hosts do cluster HPCC e atualizar a variável classpath no environment.conf.

Esse script executa um comando em todos os endereços IP ou nomes de host no arquivo ativo environment.xml. Os endereços IP são definidos no momento da edição do ambiente no Gerenciador de Configurações.

Este script grava em um arquivo de log:

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

Exemplos:

Para implementar arquivos java do /home/hpcc/development/java/ no sistema local para /home/hpcc/java/ em todos os hosts no cluster e atualizar o classpath com 10 execuções simultâneas:

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

Para implementar arquivos java do /home/hpcc/java/ no sistema local para /home/hpcc/java em todos os hosts no cluster, exceto no sistema local:

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

Para atualizar o classpath de um cluster:

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

Para implementar arquivos java em uma lista de 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	Arquivo ou diretório fonte.
-t	Arquivo ou diretório de destino.
-n, --concurrent	Quando especificado, denota o número de execuções simultâneas. O padrão é 5. Opcional.
-x	Quando especificada, essa opção exclui a execução no host atual.

Esse script "envia" arquivos do nome do arquivo e do caminho de origem para o nome do arquivo e caminho de destino de todos os endereços IP no ambiente.xml ativo.

Para usar esse script, as chaves ssh precisam estar configuradas de maneira adequada em todos os nós, sendo também necessário usar sudo.

Os endereços IP foram definidos no momento da edição do ambiente no Gerenciador de Configurações.

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

Por exemplo:

```
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	Componente do HPCC. Por exemplo, mydali, myroxie, mythor, etc.
-n, --concurrent	Quando especificado, denota o número de instâncias simultâneas a serem executadas. O padrão é 5. Opcional.
-S, --sequentially	Quando especificado, o comando é executado de maneira sequencial, um host por vez.
-s	Quando especificado, salva o resultado em um arquivo denominado <ip address>.

Para usar esse script, as chaves ssh precisam estar configuradas de maneira adequada em todos os nós, sendo também necessário usar sudo como usuário do hpcc.

Esse script executa um comando em todos os endereços IP no arquivo ativo environment.xml.

Os endereços IP foram definidos no momento da edição do ambiente no Gerenciador de Configurações. Esse script suporta todos os parâmetros do hpcc-init e do dafilesrv.

Exemplos:

Este exemplo inicia todos os componentes nos nós

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

Este exemplo inicia todos os componentes em todos os nós usando 8 execuções simultâneas

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

Este exemplo inicia todos os componentes do esp type nos nós

```
sudo /opt/HPCCSystems/sbin/hpcc-run.sh -c esp -a hpcc-init start
```

Este exemplo inicia todos os componentes com um nome de componente myesp nos nós

```
sudo /opt/HPCCSystems/sbin/hpcc-run.sh -c myesp -a hpcc-init start
```

Este exemplo inicia a aplicação auxiliar dafilesrv

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

update-keys

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

- s Key SSH Privada.
- p Key SSH Pública.
- g Gera novas id_rsa keys privadas/publicas e irá sobrescrever qualquer key para usar as novas geradas.
- n Número atual de threads, padrão é 5.

Este script tem a intenção de auxiliar administradores com o deploy de keys SSH do HPCC Systems pelos clusters. As keys SSH são usadas primariamente para inicialização de componentes como Thor e certos plug-ins como Spark. As keys SSH são mais importantes em um ambiente físico e menos em ambiente de cloud.

Exemplos:

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

Este exemplo gera novas keys SSH privadas/publicas e sobrescreve qualquer keys existente e distribui as keys para os componentes.

Desinstalando a plataforma HPCC

Para desinstalar a plataforma do HPCC, preencha os comandos apropriados para o seu sistema. Se necessário, faça esse procedimento em cada nó em que a plataforma esteja instalada.

Centos/Red Hat

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

Ubuntu/Debian

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

Aplicações Auxiliares

Talvez seja necessário parar ou iniciar manualmente as aplicações auxiliares executadas em todos os nós.

Normalmente esse processo é iniciado automaticamente na primeira vez que o serviço hpcc-init é executado.

Digite os comandos a seguir para parar ou iniciar a aplicação auxiliar:

- dafilesrv

```
sudo systemctl dafilesrv@dafilesrv.service stop  
sudo systemctl dafilesrv@dafilesrv.service start
```

hpcc-init

Sistemas init baseados no System V não suportam as chamadas systemd utilizadas pelo HPCC Systems. Continuaremos a apoiar o antigo estilo de chamada System V. init.d.

hpcc-init [option] command

option	<ul style="list-style-type: none">• <i>-c componentname, --component=componentname</i> Especifica o componente sobre o qual o comando será executado. Se omitido, o padrão é: todos os componentes da máquina. <i>-c componenttype, --component=componenttype</i> Especifica o tipo de componente sobre o qual o comando será executado. Caso seja configurado mais de um tipo, o comando será executado sobre todos eles. Se omitido, o padrão é: todos todos os componentes da máquina.• <i>--componentlist</i> Fornece uma lista de todos os nomes de componentes no nó atual, como especificado no arquivo do ambiente.• <i>--typelist</i> Fornece uma lista de todos os tipos de componentes no nó atual, como especificado no arquivo do ambiente.• <i>-h, --help</i> Exibe uma página de ajuda
command	<ul style="list-style-type: none">• <i>start:</i> Inicia o(s) componente(s)• <i>stop</i> Para o(s) componente(s)• <i>status</i> Exibe o status do(s) componente(s)• <i>restart</i> Reinicia o(s) componente(s)• <i>setup</i> Inicializa os arquivos de configuração do componente, mas não inicia o(s) componente(s).

A função **hpcc-init** é usada para iniciar, parar, reiniciar, configurar ou verificar o status de todos os componentes do HPCC.

Exemplos:

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

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

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

Serviços do sistema HPCC Systems

O HPCC Systems está estendendo o suporte e o desenvolvimento para mais serviços systemd. Pretendemos continuar com o suporte ao Cent OS 6 e outros sistemas baseados no System V através do hpcc-init. O serviço do sistema hpcc-init suportará as opções "start", "stop" e "restart".

Os relatórios e registros do sistema HPCC Systems serão diferentes do tipo hpcc-init anterior. Os logs systemd não possuem nenhuma saída para STDOUT/STDERROR, em vez disso, são registrados em /var/log/syslog. Para visualizar a saída:

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

ou

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

O systemd exibe o status do serviço no seu próprio formato.

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

É diferente da saída de

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

Os serviços HPCC Systems iniciados no systemd serão listados como ativo no systemd. Eles podem ser listados como "sudo systemctl list-units [PATTERN ...]". Para removê-los da lista de serviços ativos do systemd, você deve executar o serviço de parada a partir de "service" ou "systemctl" (como mostrado acima), mesmo que já esteja parado diretamente pelo comando stop /etc/init.d/<hpcc-init|dfilesrv> .

HPCC Systems removerá automaticamente os serviços da lista de ativos e do diretório /etc/systemd/system/.

Unity Launcher Icon (Inicializador de Unidade)

A plataforma do HPCC suporta o uso de um ícone do Inicializador de unidade Ubuntu (Unity Launcher).

A partir de um ícone no Inicializador de unidade da versão do Ubuntu para desktop, é possível iniciar, interromper, reiniciar ou consultar o status de um sistema de nó único instalado.

Observação: Atualmente, esse recurso é útil apenas em um sistema de nó único. As versões futuras podem vir a operar de outra forma e ser compatíveis com HPCC System®.

Para adicionar o ícone:

1. Use a busca no Dash Home para localizar o ícone da aplicação no HPCC Systems®.

Figure 29. Ícone da Aplicação HPCC.



2. Clique e arraste o ícone para a barra do Inicializador de Unidade.

Figure 30. Inicializador de unidade



3. Solte-o na barra.

Observação: Na versão 12.04 ou mais recente do Ubuntu é possível mover o ícone para qualquer posição na barra arrastando e soltando na posição desejada.

Para Usar o Ícone:

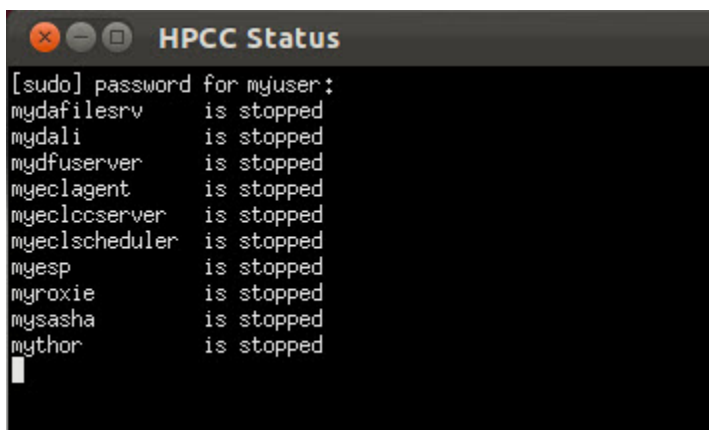
1. Clique no ícone com o botão direito e selecione a ação desejada no menu.

Figure 31. Menu contextual



2. O resultado será exibido em uma janela do terminal.

Figure 32. Resultados



```
[sudo] password for myuser:
mydafilesrv      is stopped
mydali           is stopped
mydfuserver      is stopped
myeclagent       is stopped
myeclccserver    is stopped
myeclscheduler   is stopped
myesp            is stopped
myroxie          is stopped
mysasha          is stopped
mythor           is stopped
```

3. Feche a janela ao terminar.

Executando o ECL IDE pela primeira vez

Siga essas etapas para executar o ECL IDE sob WINE no Linux.

1. Instale o wine1.2 (correspondente à versão 1.1.31 do Wine) e suas dependências.
2. Faça o download do msxml3.msi da Microsoft (Pacote de Serviço 7 ou mais recente).
<http://www.microsoft.com/en-us/download/details.aspx?id=3988>
3. Instale o msxml3.msi no Wine (clique duas vezes no arquivo msi e o Wine fará a instalação).
4. Abra “Configurar Wine” (Configure Wine) (Applications/Wine/Configure Wine):
5. Selecione a aba Libraries.
6. Em “New override”, localizado na lista suspensa da biblioteca, selecione *msxml3*, então pressione o botão Add.
7. Selecione *msxml3* na lista de Substituições existentes e pressione Edit.
8. Selecione a opção *Native (Windows)* e pressione o botão OK .
9. Pressione o botão OK para fechar a janela de configurações do Wine.
10. Instale o HPCC ECL IDE (clique duas vezes no arquivo setup.msi e o Wine fará a instalação).

Suporte a Linguagem Externa

Esta seção abrange as etapas para adicionar o suporte à uma linguagem externa na plataforma do HPCC . O HPCC System oferece suporte à várias linguagens de programação, porém algumas delas possuem dependências adicionais que precisam ser instaladas. O suporte à linguagem externa está incluído no pacote de instalação da plataforma, porém existem pacotes de instalação da plataforma do HPCC baseados em RPM que são explicitamente representados com **plugins**.

Sistemas baseados em RPM:

Caso tenha interesse em usar linguagens externas em sistemas baseados em RPM (CentOS/Red Hat), será preciso baixar e instalar a distribuição de instalação da plataforma apropriada **com a opção plugins** no site de download.

Para sistemas baseados em RPM, há dois pacotes de instalação diferentes disponíveis. Um pacote inclui os plugins opcionais que suportam códigos incorporados de outras linguagens. Caso queira obter suporte para outras linguagens, selecione o pacote para sua distro que começa com:

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

Sistemas baseados em Debian:

O download de plugins opcionais não é necessário para os pacotes de instalação de sistemas baseados em Debian (Ubuntu), uma vez que os plugins já estão incluídos em todos os pacotes de instalação Debian.

As linguagens externas atualmente suportadas incluem:

- C++ (suporte completo já está incluso)
- Java
- JavaScript
- Python (suporte completo já está incluso)
- R

As seções a seguir especificam o que é necessário para utilizar essas linguagens em sua plataforma do HPCC .

Além destas linguagens, você pode adicionar suporte para outras linguagens criando seu próprio plugin. Isso não é muito difícil de fazer. Por exemplo, o plugin JavaScript possui 500 linhas de código C++. Você pode usar isso como um modelo para criar o seu próprio plugin e, se desejar, poderá contribuir com a iniciativa de código aberto.

Java

É possível executar código Java externo na plataforma do HPCC . O Java compilado pode ser usado como .class (ou .jar) e ser acionado pelo ECL como qualquer função ECL .

Para extrair as assinaturas JNI :

```
javap -s
```

Para configurar o Java para ser integrado à plataforma do HPCC :

1. Instale um pacote de desenvolvimento do Java, como OpenJDK ou Oracle Java SE Development Kit (JDK), no servidor.
2. Defina o Java CLASSPATH

O classpath pode ser definido de várias formas:

- Em seu perfil.
- Em seu ambiente.
- Em seu perfil JVM.
- Usando o valor do classpath no environment.conf

O arquivo de configuração padrão da plataforma do HPCC é **/etc/HPCCSystems/environment.conf** e você terá que editar esse arquivo para direcioná-lo para seu diretório de compilação Java.

Por exemplo (em um sistema Linux):

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

O classpath deve direcionar para seu diretório de compilação Java .

3. Inicie a plataforma do HPCC System® (caso já esteja em execução, reinicie) para que a nova configuração possa ser lida.

For example :

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

Para obter mais informações, consulte a seção Iniciar e parar o HPCC System no documento *Como instalar e executar a plataforma do HPCC* .

4. Testar a integração do Java .

A plataforma do HPCC Systems® vem com uma classe de exemplo Java . Alguns códigos Java podem ser executados no ECL IDE ou no ECL Playground.

Por exemplo:

```
IMPORT java;  
  
integer add1(integer val) := IMPORT(java, 'JavaCat.add1:(I)I');  
  
add1(10);
```

Se o comando for executado com sucesso, significa que o Java foi configurado corretamente para funcionar na plataforma do HPCC Systems .

Se você receber uma mensagem de erro "unable to load libjvm.so (não foi possível carregar libjvm.so)", reinstale ou tente instalar outro pacote Java .

Você pode acionar o Java do ECL assim como qualquer outra função do ECL . As funções estáticas Java podem ser facilmente prototipadas usando os tipos do ECL.

Outros exemplos de código HPCC podem ser encontrados em:

<https://github.com/hpcc-systems/HPCC-Platform/tree/master/testing/ecl/embedjava.ecl>

JavaScript

Para habilitar o suporte ao JavaScript na plataforma do HPCC Systems® :

1. Instale as dependências apropriadas à sua plataforma.

Sistemas baseados em RPM:

Em um sistema baseado em RPM (CentOS/Red Hat), instale o **v8embed**.

Sistemas baseados em Debian:

Para sistemas baseados em Debian (Ubuntu), instale o pacote **libv8-dev** .

2. Teste a integração do JavaScript.

O JavaScript realiza multitarefa e, como resultado, essa pode ser a mais rápida de todas as linguagens incorporadas atualmente suportadas.

Agora alguns códigos JavaScript podem ser executados no ECLIDE ou no ECL Playground.

Por exemplo:

```
//nothor
IMPORT javascript;

javascript.Language.syntaxcheck('1+2');

integer add1(integer val) := EMBED(javascript) val+1; ENDEMBED;

data testData(data val) := EMBED(javascript) val[0] = val[0] + 1; val; ENDEMBED;
set of integer testSet(set of integer val) := EMBED(javascript)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

add1(10);
```

Se o comando for executado com sucesso, significa que o JavaScript foi configurado corretamente para funcionar na plataforma do HPCC Systems

Outros exemplos de código HPCC podem ser encontrados em:

<https://github.com/hpcc-systems/HPCC-Platform/tree/master/testing/ecl/embedjava.ecl>

Python

A plataforma HPCC Systems suporta Python3 por padrão. Isto inclui plugins para Python2 e Python3, mas apenas um pode ser ativado com segurança por vez, enquanto as bibliotecas Python exportam o mesmo símbolos para ambas as versões. A ativação de ambos pode levar a imprevisibilidade resultados, incluindo falhas de segmentação ou símbolo indefinido erros.

Por padrão, o plugin Python2 está presente, mas desativado, e o plugin Python3 está presente e ativado. Se você deseja usar o Python2 modifique seu arquivo `environment.conf` de acordo com o exemplo no arquivo.

Um cluster atualizado a partir de uma versão mais antiga pode não ter o entradas apropriadas no arquivo `environment.conf` que suporte a versão do Python.

1. Instale o Python, caso ainda não o tenha feito. Várias distribuições já têm o Python instalado.

Python 2.6, 2.7, ou Python3, dependendo da versão padrão da sua distribuição e para coordenar com a entrada habilitada no `environment.conf`.

2. Você pode incorporar o Python nativamente dentro do ECL Program, muito parecido com `BEGINC++`

3. Chamada Python oriundas ECL como qualquer outra função ECL.

Python não desempenha multitarefa de forma eficiente (Global Interpreter Lock). Efetivamente, o python pode conter apenas uma linha de execução (thread) por vez. Os scripts são compilados toda vez que são acionados (porém com o cache mais recente, por linha de execução). O caso `IMPORT` evitará a recompilação.

4. Teste a integração do Python.

Agora alguns códigos Python podem ser executados no ECLIDE ou no ECL Playground.

Por exemplo:

```
IMPORT Python;

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

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

Se o comando for executado com sucesso, significa que o Python foi configurado corretamente para funcionar na plataforma do HPCC . Agora você pode incorporar o Python em qualquer lugar onde usaria o ECL em seu HPCC System.

Outros exemplos de código HPCC podem ser encontrados em:

<https://github.com/hpcc-systems/HPCC-Platform/tree/master/testing/regress/ecl/>

Para que o Python funcione corretamente, é importante que a versão do Python e do HPCC Systems esteja configurada corretamente para suportar a versão instalada do Python. Se você ver a mensagem de erro "Id: cannot find --lpy2embed", é provável que seu sistema esteja configurado para Python3. Da mesma forma, se você ver "Id: cannot find --lpy3embed", seu sistema está configurado para Python2.

Opções de Escopo Python

GLOBALSCOPE - Esta opção permite que atributos `EMBED` independentes compartilhem globais entre si caso especifiquem o mesmo nome para o parâmetro `GLOBALSCOPE`.

PERSIST - Esta opção controla por quanto tempo um escopo global compartilhado persistirá e, exatamente, por quanto tempo ele será compartilhado.

O valor especificado para GLOBALSCOPE pode ser qualquer string desejada, permitindo compartilhar globais entre as seções EMBED relacionadas, mantendo-as distintas das não relacionadas.

PERSIST pode adotar um dos seguintes valores:

global - Os valores persistem indefinidamente (até o processo terminar) e são compartilhados com quaisquer outras incorporações que usam o mesmo valor GLOBALSCOPE, até mesmo em outras tarefas.

query - Os valores persistem até que a consulta seja descarregada e compartilhada com outras instâncias da consulta que possam estar sendo executadas ao mesmo tempo no Roxie, porém não com outras consultas.

workunit - Os valores persistem até o final da tarefa atual ou da instância atual de uma consulta implementada por Roxie, e não são compartilhados com outras instâncias.

R

A plataforma do HPCC suporta código R incorporado. Para habilitar o suporte ao R na plataforma do HPCC Systems® :

1. Faça o download do plugin **R Embed** disponível no portal do HPCC Systems.

<https://hpccsystems.com/download/hpcc-platform>

Selecione o plugin adequado para sua distribuição.

2. Instale o plugin.

Sistemas baseados em RPM: Instalar o usando *yum install*.

Sistemas baseados em Debian: Instalar o utilizando *dkpg -i* depois *apt-get install -f*

Se você usa esses métodos para instalar plugins, todas as bibliotecas e dependências obrigatórias também serão instaladas.

3. Teste a integração do R

R não tem ciência de multitarefa, assim o plugin precisa agrupar todos os acionamentos do R para as seções críticas. Os scripts são compilados com cada acionamento do R. Este ambiente pode persistir entre os acionamentos incorporados do R em um mesmo ambiente.

Agora alguns códigos R podem ser executados no ECLIDE ou no ECL Playground.

Por exemplo:

```
IMPORT R;

integer add1(integer val) := EMBED(R)
val+1
ENDEMBED;

string cat(varstring what, string who) := EMBED(R)
paste(what,who)
ENDEMBED;

data testData(data val) := EMBED(R)
val[1] = val[2];
val;
ENDEMBED;

set of integer testSet(set of integer val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

set of unsigned2 testSet0(set of unsigned2 val) := EMBED(R)
sort(val);
ENDEMBED;

set of string testSet2(set of string val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
```

```
ENDEMBED;

set of string testSet3(set of string8 val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

set of varstring testSet4(set of varstring val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

set of varstring8 testSet5(set of varstring8 val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

set of boolean testSet6(set of boolean val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

set of real4 testSet7(set of real4 val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

set of real8 testSet8(set of real8 val) := EMBED(R)
t = val [1];
val[1] = val[2];
val[2] = t;
val;
ENDEMBED;

set of integer2 testSet9(set of integer2 val) := EMBED(R)
sort(val);
ENDEMBED;

add1(10);
cat('Hello', 'World');
testData(D'ab');
testSet([1,2,3]);
testSet0([30000,40000,50000]);
testSet2(['one','two','three']);
testSet3(['uno','dos','tre']);
testSet4(['un','deux','trois']);
testSet5(['ein','zwei','drei']);
testSet6([false,true,false,true]);
testSet7([1.1,2.2,3.3]);
testSet8([1.2,2.3,3.4]);
testSet9([-111,0,113]);

s1 :=DATASET(250000, TRANSFORM({ integer a }, SELF.a := add1(COUNTER)));
s2 :=DATASET(250000, TRANSFORM({ integer a }, SELF.a := add1(COUNTER/2)));
SUM(NOFOLD(s1 + s2), a);
```

```
s1b :=DATASET(250000, TRANSFORM({ integer a }, SELF.a := COUNTER+1));  
s2b :=DATASET(250000, TRANSFORM({ integer a }, SELF.a := (COUNTER/2)+1));  
SUM(NOFOLD(s1b + s2b), a);
```

Se o comando for executado com sucesso, significa que o R foi configurado corretamente para funcionar na plataforma do HPCC .

Outros exemplos de código HPCC podem ser encontrados em:

<https://github.com/hpcc-systems/HPCC-Platform/tree/master/testing/regress/ecl/embedR.ecl>

Mapeando Datatypes

Algumas considerações adicionais para o mapeamento dos tipos de dados no R.

No HPCC, o ECL **RECORD** é mapeado para um R *list*

Um **DATASET** incluindo um dataset aninhado, é mapeado para um R *dataframe*.

Um ECL **SET** é mapeado para um R *vector*.

Esses princípios aplicam-se à transmissão de dados do HPCC para o R ou do retorno de dados do R para o HPCC. Os exemplos de uso desses conceitos estão disponíveis em:

<https://github.com/hpcc-systems/HPCC-Platform/tree/master/testing/regress/ecl/embedR2.ecl>

Opções de Escopo R

GLOBALSCOPE - Esta opção permite que atributos EMBED independentes compartilhem globais entre si caso especifiquem o mesmo nome para o parâmetro GLOBALSCOPE .

PERSIST - Esta opção controla por quanto tempo um escopo global compartilhado persistirá e, exatamente, por quanto tempo ele será compartilhado.

O valor especificado para GLOBALSCOPE pode ser qualquer string desejada, permitindo compartilhar globais entre as seções EMBED relacionadas, mantendo-as distintas das não relacionadas

PERSIST pode adotar um dos seguintes valores:

Global - Os valores persistem indefinidamente (até o processo terminar) e são compartilhados com quaisquer outras incorporações que usam o mesmo valor GLOBALSCOPE, até mesmo em outras tarefas.

Query - Os valores persistem até que a consulta seja descarregada e compartilhada com outras instâncias da consulta que possam estar sendo executadas ao mesmo tempo no Roxie, porém não com outras consultas.

Workunit - Os valores persistem até o final da workunit, ou da instância atual de uma consulta implementada pelo Roxie, e não são compartilhados com outras instâncias.