

IBM Encryption Expert installation and setup and integration with DB2

Lab Exercises



An IBM Proof of Technology

Catalog Number

Contents

LAB 1	SETUP OF NETWORKING	6
	1.1 STARTING THE VM IMAGE.....	6
	1.2 ADD A VIRTUAL NETWORK	6
	1.3 TEST NETWORKING	8
LAB 2	INSTALLING ENCRYPTION EXPERT SERVER	9
	2.1 INSTALL THE ENCRYPTION EXPERT SERVER.....	9
	2.2 GENERATE THE CERTIFICATE AUTHORITY.....	10
	2.3 LOGIN AND SET DEFAULT ADMIN PASSWORD.....	12
	2.4 INSTALL THE LICENSE KEY	15
LAB 3	CREATING A SECURITY DOMAIN AND USERS	18
	3.1 CREATE A SECURITY DOMAIN, DOMAIN ADMINISTRATOR, AND SECURITY ADMINISTRATOR.....	18
LAB 4	ADMINISTERING HOSTS, POLICIES, AND KEYS	24
	4.1 CREATE AN ENCRYPTION KEY	24
	4.2 INSTALL AND REGISTER HOST	25
	4.3 ENABLE AGENT COMMUNICATION	30
	4.4 CREATE A POLICY	31
LAB 5	ENCRYPTING DATA THE BASICS	49
	5.1 CREATE A GUARD POINT AND APPLY A POLICY	49
	5.2 TEST POLICY ACTIONS	51
	5.3 APPLY USER AUTHENTICATION.....	55
LAB 6	ENCRYPTING DB2 DATA	65
	6.1 CREATE A DB2 POLICY.....	65
	6.2 APPLY THE DB2-POLICY TO A DB2 DATABASE	68
LAB 7	ENCRYPTING DB2 BACKUPS.....	72
APPENDIX A.	NOTICES	79
APPENDIX B.	TRADEMARKS AND COPYRIGHTS	81

Overview

In the following exercises participants will gain hands on experience with implementing IBM Encryption Expert and integration of the product in a DB2 environment. The exercises will focus on the main tasks required of an implementation with focus on understanding the how the technologies work and can be used to protect important assets.

Introduction

To follow the lab exercises no prior knowledge of Encryption Expert or DB2 are required. However, having a basic understanding of how encryption technologies work and the need for encryption key management are useful in understanding how the technologies can be leveraged to solve data security requirements.

Requirements

All lab material is based on two provided VM Ware images:

Rh5-u3-i386-server – Is a 32 bit Linux server that will be the administration server portion of the solution

Rh5-u3-x64-agent – Is a 64 bit Linux server that will be the DB2 server where the encryption of data will take place.

To run these VM Ware images you will need VM Ware Workstation 6.5 or higher and a Windows host machine capable of running 64bit software. It is not required that your Windows Host OS be 64bit but your processor architecture must support 64bit processing.

To check if your system can support running the 64 bit guest download and execute a utility from VM Ware or may have been provided as part of the PoT download.

Processor Check for 64-Bit Compatibility:

http://downloads.VMware.com/d/details/processor_check_5_5_dt/dCpiQGhkYmRAZQ==




In addition to being 64 bit capable you may need to set a BIOS setting to enable hardware assisted virtual technology. To detect if your chipset is capable and is turned on you can download the following tool from Microsoft or it may have been provided as part of the PoT download.

VT Bios check:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0ee2a17f-8538-4619-8d1c-05d27e11adb2&displaylang=en>

Icons

The following symbols appear in this document at places where additional guidance is available.

Icon	Purpose	Explanation
	Important!	This symbol calls attention to a particular step or command. For example, it might alert you to type a command carefully because it is case sensitive.
	Information	This symbol indicates information that might not be necessary to complete a step, but is helpful or good to know.
	Trouble-shooting	This symbol indicates that you can fix a specific problem by completing the associated troubleshooting information.

Lab 1 Setup of networking

The VMware images (guests) are configured to use static IP addresses. To ensure proper communication the guests will be configured to use a custom host-only based network. At the conclusion of this lab the Linux guests will be able to ping each other by hostname while the Windows host OS will be able to ping the Linux guests by their IP addresses.

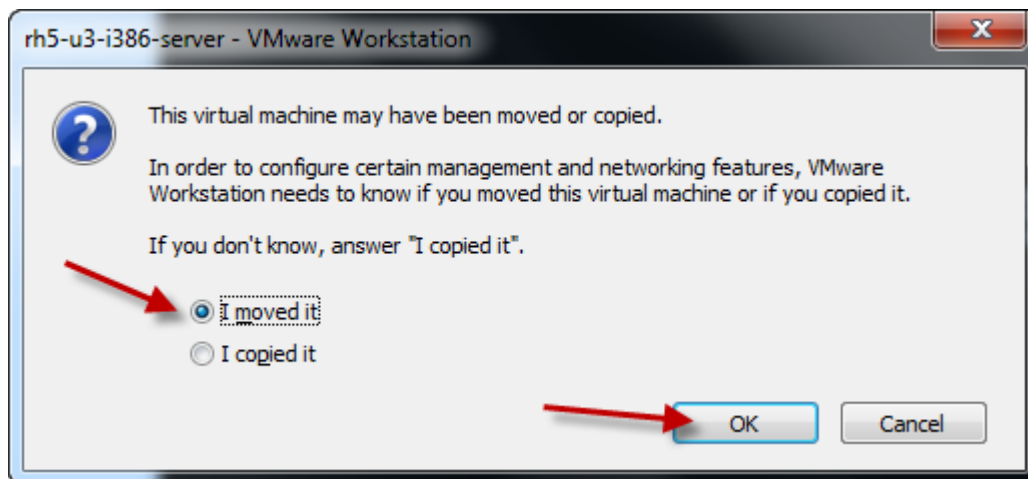


Important!

Ensure the requirements are met before beginning Lab 1.

1.1 Starting the VM Image

Wait to start the image until after the virtual network is added (1.2). However if prompted with the following dialog during startup, **I moved it** must be selected:



1.2 Add a virtual network

The Linux guests are configured to use a virtual VMware virtual switch (VMnet2) with an IP address range of 192.168.100.xxx. Configure the virtual switch as follows:

1. Open the Virtual Network Editor, **Edit > Virtual Network Editor**



VMware Workstation 7.1 screen capture

The included screen captures are based on VMware Workstation 7.1 other version GUI interfaces may look different.



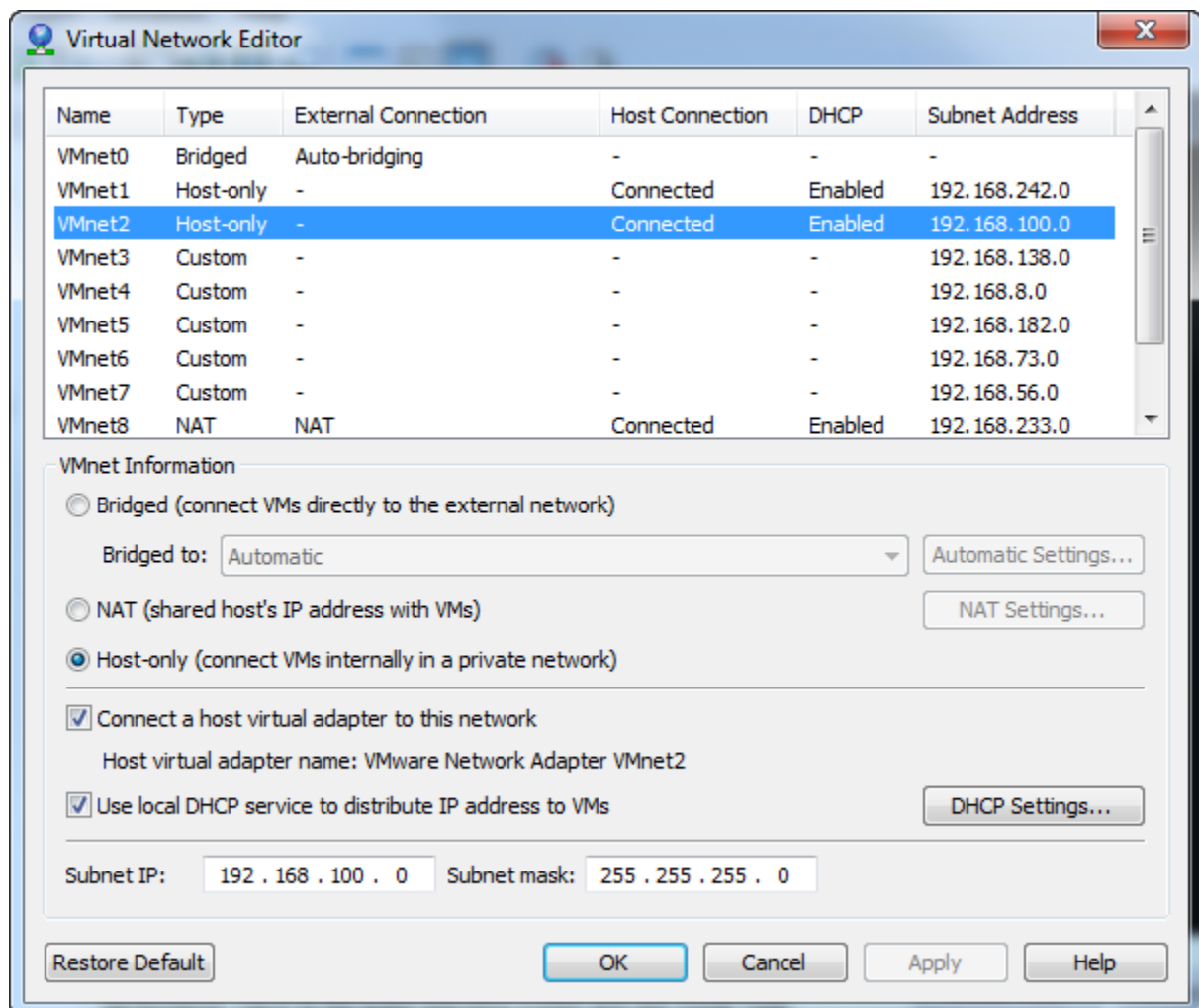
Troubleshooting

If are using VMWare Player 3.1 the Virtual Network Editor, vmnetcfg.exe must be added. The executable vmnetcfg.exe is available as one of the download files included with images. Place the vmnetcfg.exe file in c:\program files\VMware\vmware player directory and launch the virtual network editor from there.

__2. Alter VMnet2 adding the following attributes

- Type – Host-only
- Subnet IP – 192.168.100.0
- Subnet Mask – 255.255.255.0

The output should be similar to the following VMware workstation 7.1 capture.



1.3 Test networking

All networking must be working in order to perform the succeeding labs. Test communication between the guests and host.

1.3.1 Test guest connectivity

__1. Login into each guest and perform the following steps:



ID and Password

Root's password is "password".

__a. From each guest, ping each guest by hostname and IP address

```
ping rh5-u3-i386-server
```

```
ping 192.168.100.10
```

```
ping rh5-u3-x64-agent
```

```
ping 192.168.100.11
```

1.3.2 Test host (Windows) connectivity

__b. From the Windows host ping the guests by IP address

```
ping 192.168.100.10
```

```
ping 192.168.100.11
```



Console or SSH interface

All commands can be performed from either the guest's terminal windows or you can use a SSH application such as putty to establish connectivity and perform the commands.

Lab 2 Installing Encryption Expert server

The Encryption Expert server is the management piece of the solution and serves as the management interface and data store for the security solution objects. Other than installation, all management is performed via a web browser.

2.1 Install the Encryption Expert server

- __1. Login via a terminal or SSH session

ID = root

Password = password

- __2. Change to the software installation directory

```
cd /software/Server
```

- __3. Make the installer executable

```
chmod 744 install_vor_server
```

- __4. Execute the installation script

```
./install_vor_server
```

- __5. When prompted accept the licensing terms, advance the licensing text using the space bar.

**Important!**

Installation will take several minutes. The installer may seem to hang on **installing database** and **configuring database**. Do not stop the install.

An example of a successful installation:

```

root@rh5-u3-i386-server:/software/Server
WARRANTIES INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OF

"third-party" RIGHTS, AND ANY WARRANTIES ARISING OUT OF CONDUCT OR INDUSTRY
PRACTICE.
10.  TERMINATION OF LICENSE. In the event that You fail to comply with this
EULA, Vormetric may terminate the license and You must destroy all copies of
the Software (with all other rights of both parties and all other provisions
of this EULA surviving any such termination).

Do you accept the terms of the above license agreement? (y/n)          y

[##-----] Installing database
[###-----] Installing application server
[#####---] Installing Security Server components
[#####-] Configuring database
[#####] Cleaning up
Security Server installation complete.

You can now ssh login as cliadmin/cliadmin123 to access the
CLI interface to configure this security server. Run command
"system security genca" to complete the configuration.

[root@rh5-u3-i386-server Server]#

```

2.2 Generate the certificate authority

The Security Server uses certificates to validate the authenticity of the communicating agent as well as encrypt any information sent and received from the agent. To start this process the certificate authority must be generated.

The Security Server includes a limited shell interface. To use this interface a user, cliadmin, was created during the installation. Interfacing with the host should be limited to this ID where possible and most administration should be performed outside of initial setup should be done via the browser administration. One important step to securing the security server is to perform a hardening routine to limit the available access to the system. Documentation on hardening is provided in the administration guide. General guidance is to make the Encryption Expert Server as much like a black box as possible and to limit access to the system from both users and processes as much as possible.

__1. Su to the cliadmin user

```
su - cliadmin
```



The cliadmin interface

The cliadmin interface has a very limited command structure. To see what commands you can run enter a “?”. Use the “up” command to return to a previous level of the commands

__2. Change to system commands

```
system
```

__3. Generate the certificate authority

```
security genca
```

When prompted to regenerate the certificates enter “yes”. Accept the default values for all further prompts (the values in square brackets) by pressing **Enter**. It is not necessary to enter any values.



The certificate values

The certificate values are not necessary as the certificates will not be registered with a external certificate authority. This is a closed system where the solution application validates the authenticity of communicating hosts.

An example of a successful certificate generation:

```

root@rh5-u3-i386-server/software/Server
[root@rh5-u3-i386-server Server]# su - cliadmin
0000:vormetric$ system
0001:system$ security genca
WARNING: All Agents and Peer node certificates will need to be re-signed after CA and
server certificate regenerated, and the security server software will be restarted
automatically!
Continue? (yes/no) [no]:yes
This computer may have multiple IP addresses. All the agents will have to connect t
o Security Server using same IP.
Enter the host name of this computer. This will be used by Agents to talk to this S
ecurity Server.
This Security Server host name[rh5-u3-i386-server]:
Please enter the following information for key and certificate generation.
What is the name of your organizational unit? []:
What is the name of your organization? []:
What is the name of your City or Locality? []:
What is the name of your State or Province? []:
What is your two-letter country code? [US]:
Regenerating the CA and server certificates now...
SUCCESS: The CA and security certificates are re-generated and the Security Server
software is restarted.

Regenerating CA will make certificates at failover servers and agents invalid. You
may need to:
- Re-sign certificates at each failover server
- Cleanup and re-register each agent
0002:system$ █

```

2.3 Login and set default admin password

After generation of the certificates, further administration is done via a Web Browser. It is recommended to use Internet Explorer for web administration as other browsers may munge the interface.



Troubleshooting

Java is required to work with some parts of GUI.

__1. Login and change the default password

__a. Open the following address

`https://192.168.100.10:8445`



Important!

The URL uses **https** for secure communication, be sure to include the “s”. when typing the URL.

__b. When prompted with a security certificate warning select, **Continue to this website**, to continue.



The warning message

The browser warning message can be ignored because there is not external Certificate Authority that can verify the certificate that was generated during the generate certificate process. All agent certificates are validated against the EE Server which is its own certificate authority.

__c. Login with the default credentials

ID = admin

Password = admin123

__d. You must change the default password,

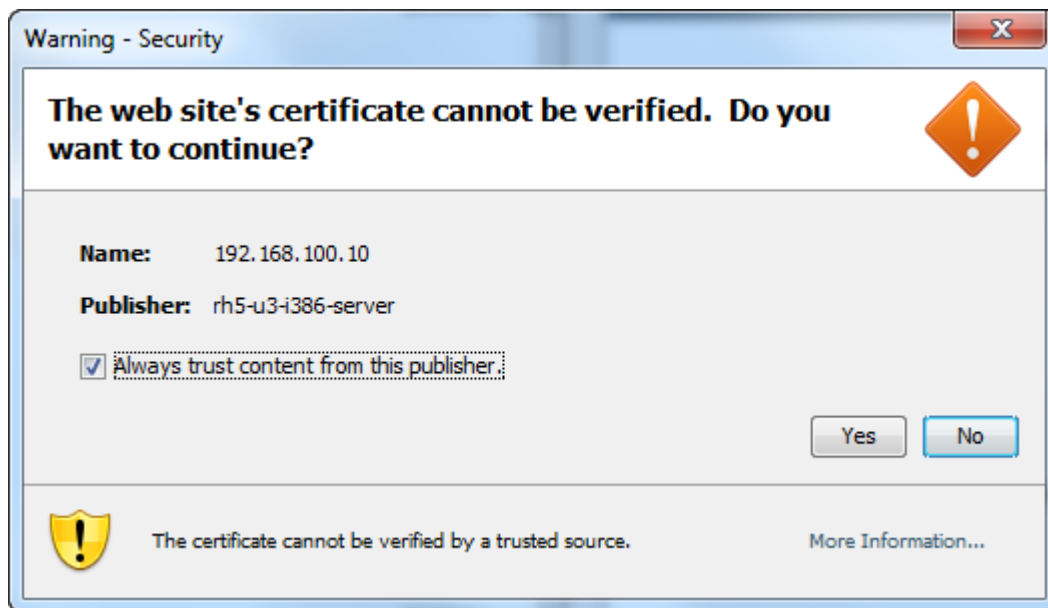
Suggestion = Admin123\$



Password changes

If you change the password to something other than what is suggested, it must be remembered. There is no way to reset the password without reinstalling the product. The default password rules are demanding but they are configurable.

- ___e. When prompted to trust the content for rh5-u3-i386-server, check the box to **Always trust content from this publisher** and click **Yes**



The default starting page is the Dashboard. Depending on security administration role a differing set of tabs across the top of the page is displayed.

An example of the dashboard for the admin role:

The screenshot shows the Vormetric Data Security Management Console interface. At the top, there is a navigation bar with the Vormetric logo and the text 'VORMETRIC'. On the right side of the navigation bar, it says 'Log Out' and 'Logged in as: admin'. Below the navigation bar, there is a main content area with a title 'Vormetric Data Security Management Console' and a help icon. The main content area displays the following information:

- Version: 4.4.0.0, Software, Single Domain, Build: uni_358v
- Server Name: rh5-u3-i386-server, Server time: 2010-08-10 09:40:16.393 PDT
- Your last login was at 9:35 AM on 08/10/2010
- HSM is disabled
- License file not found.
- [Change Password](#)
- There are currently 0 other administrators logged in to the management console.
- HA Info: rh5-u3-i386-server (Primary Server)
- The fingerprint for the CAs is E2:ED:B0:9E:B0:80:97:80:28:D0:68:D1:49:82:C5:F0:CF:B5:29:5F
- File System:/dev/sda3 Total Space:2902MB Free Space:1979MB Use:29% Mounted On:/opt

At the bottom of the dashboard, there are two summary boxes:

- Configuration Summary**: 1 Administrator(s)
- Security Summary**: (Empty)

2.4 Install the license key

The license key must be installed to add hosts to the system. A license key has been provided with image but must be pulled down to the local system for registration purposes.

2.4.1 Pull the license key to the local machine

- __1. From the command line as root, start the ftp daemon

```
service vsftpd start
```

- __2. Open a local command window **Start > Run > cmd**

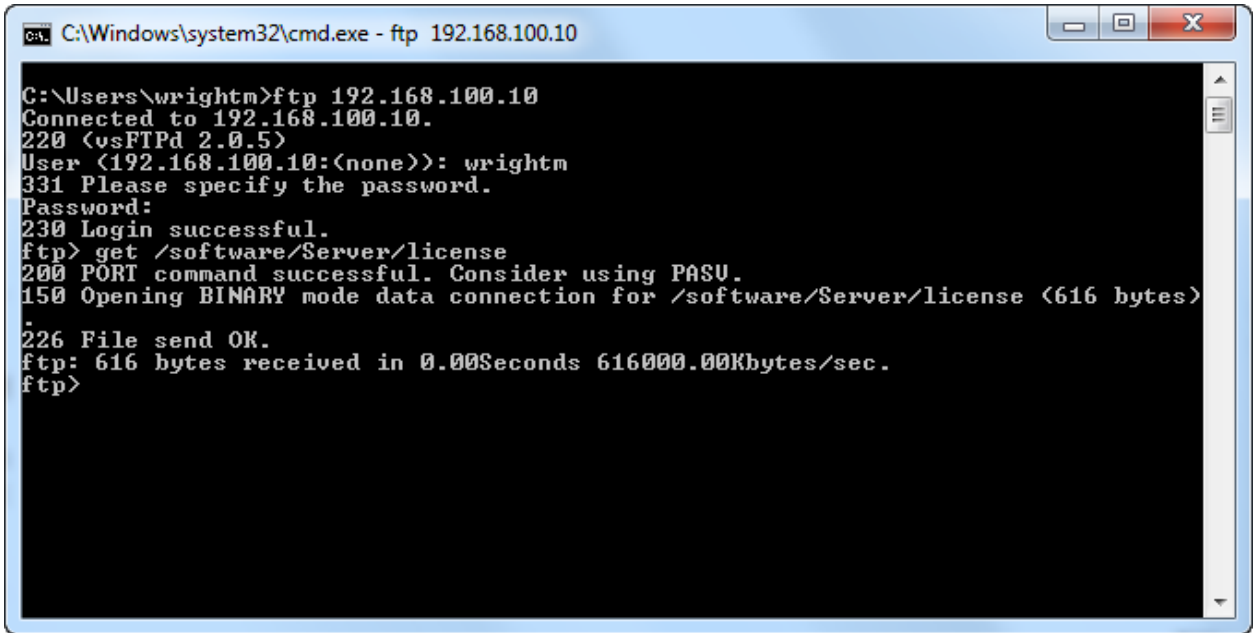
- __3. FTP the license file to the local machine

```
ftp 192.168.100.10
```

```
ID = wrightm
```

Password = password

```
get /software/Server/license
```

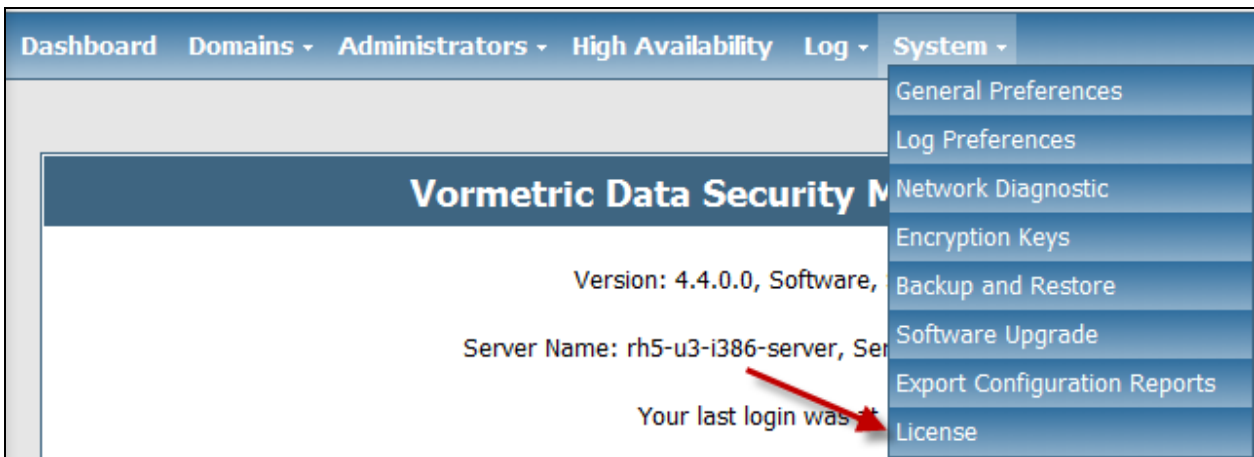


Note where you have downloaded the license file.

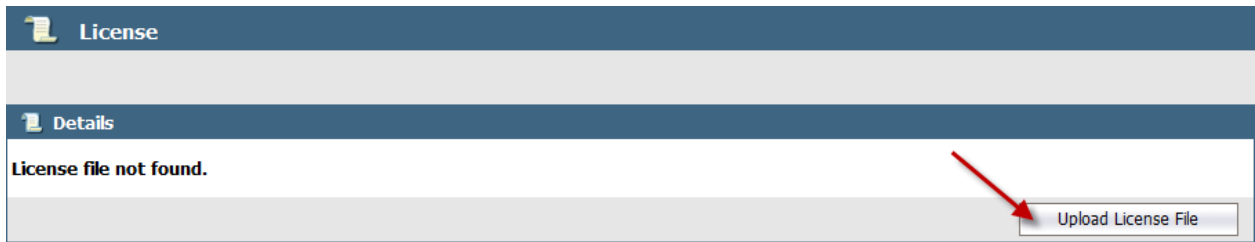
2.4.2 Install the license key

The license key is an IBM evaluation license intended for use within IBM and should not be shared with customers outside the controlled educational or PoT environment.

__1. From the **System** tab select **License**



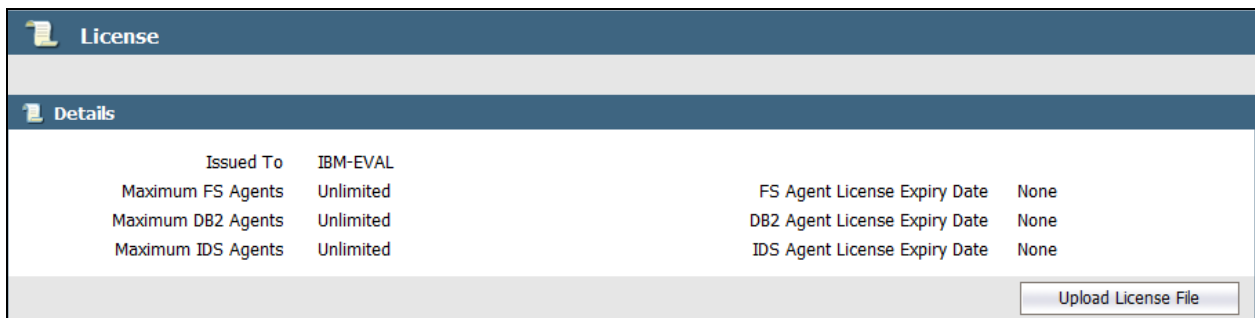
__2. Click the **Upload License File**



__3. Click the **Browse** button and navigate to and select the downloaded license file and click **Ok**



The License File detail is displayed.



Lab 3 Creating a security domain and users

Security domains are silos of security administration. It allows for large organizations that may desire or need separation of security administration to configure different users to have security roles only within their participating domain of security. For most purposes and for the lab exercises there will be a single domain, testdomin.

3.1 Create a security domain, domain administrator, and security administrator

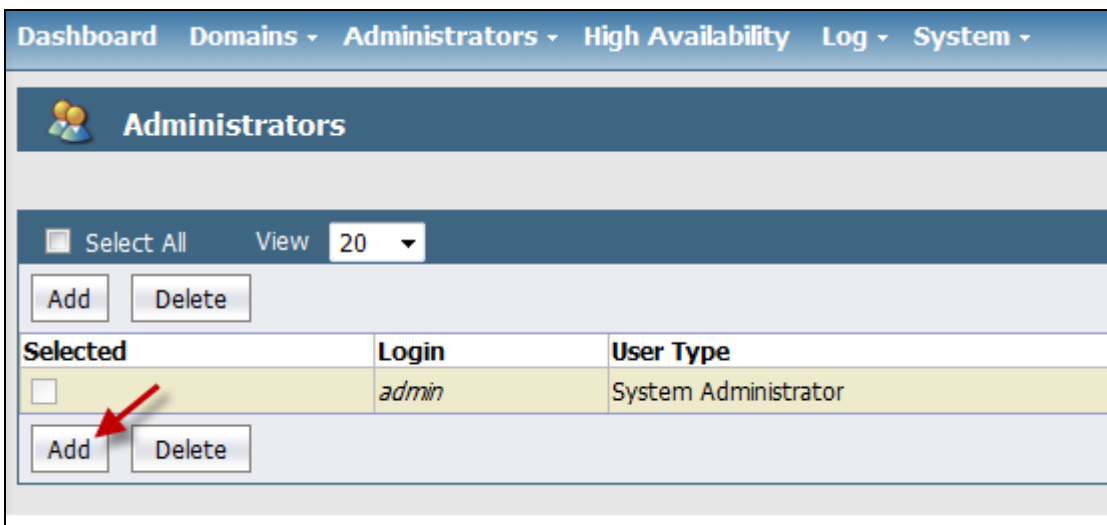
There are three administrator types System, Domain, and Security.

- System administrators are responsible for adding administrator IDs to the system, configuring the system's logging and high availability, and creating domains.
- Domain administrators are responsible for assigning roles to IDs within a domain
- Security administrator and responsible for implementing their assigned roles (ie.. creating keys, creating polices, managing hosts).

Security administrators perform the more regular routines of implementing encryption on managed systems.

3.1.1 Create a domain administrator

- __4. If not already done so login as admin
- __5. Select the **Administrators** tab
- __6. Click the **Add button**



__7. Create the domain administrator account with the following details and click **Ok**

Login = domadmin

Description = domain administrator

Password = Domadmin123\$

User Type = Domain Administrator

Add Administrator

Details

* Login: domadmin

Description: domain administrator

* Password: [Masked]

* Confirm Password: [Masked]

User Type:

- System Administrator
- Domain Administrator
- Security Administrator
- Domain and Security Administrator
- All

OK Cancel

3.1.2 Create a security administrator

__1. Select the Administrators tab

__2. Click the **Add button**

__3. Create the security administrator account with the following details and click **Ok**

Login = secadmin

Description = security administrator

Password = Secadmin123\$

User Type = Security Administrator

Add Administrator

Details

* Login: secadmin

Description: security administrator

* Password: [masked]

* Confirm Password: [masked]

User Type:

- System Administrator
- Domain Administrator
- Security Administrator
- Domain and Security Administrator
- All

OK Cancel

3.1.3 Create domain and add users to domain

- __1. Click the **Domains** tab
- __2. Click the **Add** button

Dashboard Domains Administrators High Availability Log System

Domains

Select All View 20

Add Delete

Selected	Name	Description	Domain Adm
Add Delete			

- __3. Enter the following domain information and click the **Assign** button
- Domain Name = testdom
- Description = test domain

Add Domain

*Domain Name: testdom

Description: test domain

Domain Administrator: Assign

Ok Cancel

- __4. Select the radio button next to the **domadmin** ID and click the **Assign to Domain** button

Dashboard Domains Administrators High Availability Log System

Administrators

View 20

Assign to Domain

Selected	Login
<input checked="" type="radio"/>	domadmin

Assign to Domain

- __5. Click the **Ok** button to finish domain creation

Add Domain

*Domain Name: testdom

Description: test domain

Domain Administrator: Assign

Ok Cancel

- __6. Log out by clicking the **Log Out** link

VORMETRIC

Dashboard Domains Administrators High Availability Log System

Log Out

Logged in as: admin

The admin ID does not have the ability to administrate encryption. This enforces the concept of a separation of duties.

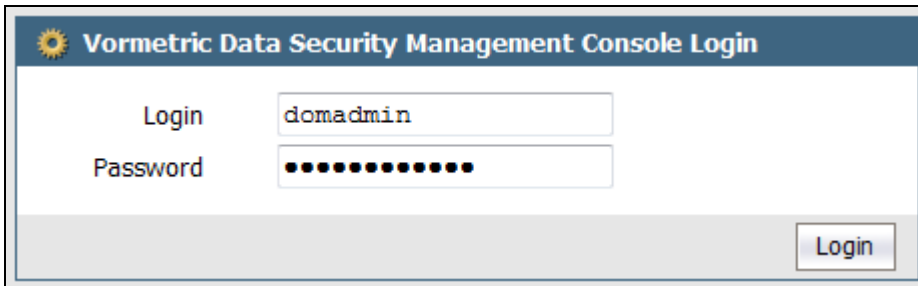
3.1.4 Add secadmin to the testdom security domain

The domain administrator domadmin has the responsibility of adding security administrators to the security domain and assigning them a security role. In this section secadmin will be granted all the security roles which is not necessarily a model for separation of duties but will allow for evaluation of all the security roles.

__7. Login as the domain administrator

ID = domadmin

Password = Domadmin123\$



__8. Change the password as required

Old Password = Domadmin123\$

New Password = Admin123\$

Confirm New Password = Admin123\$

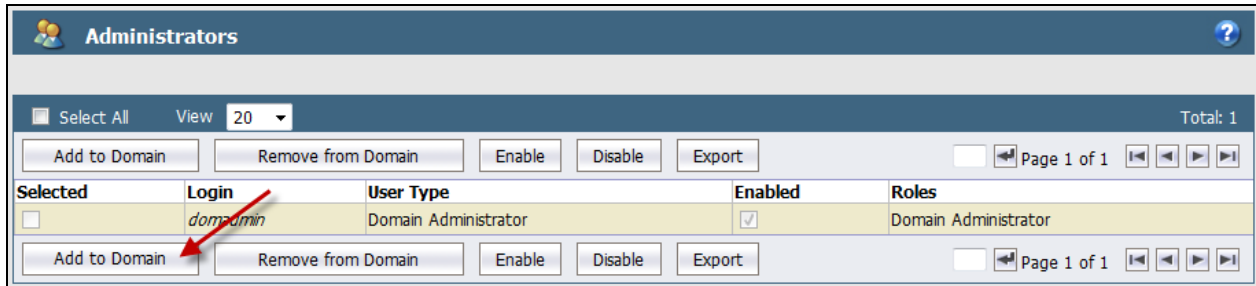
__9. Click the **Administrators** tab



Change in tabs

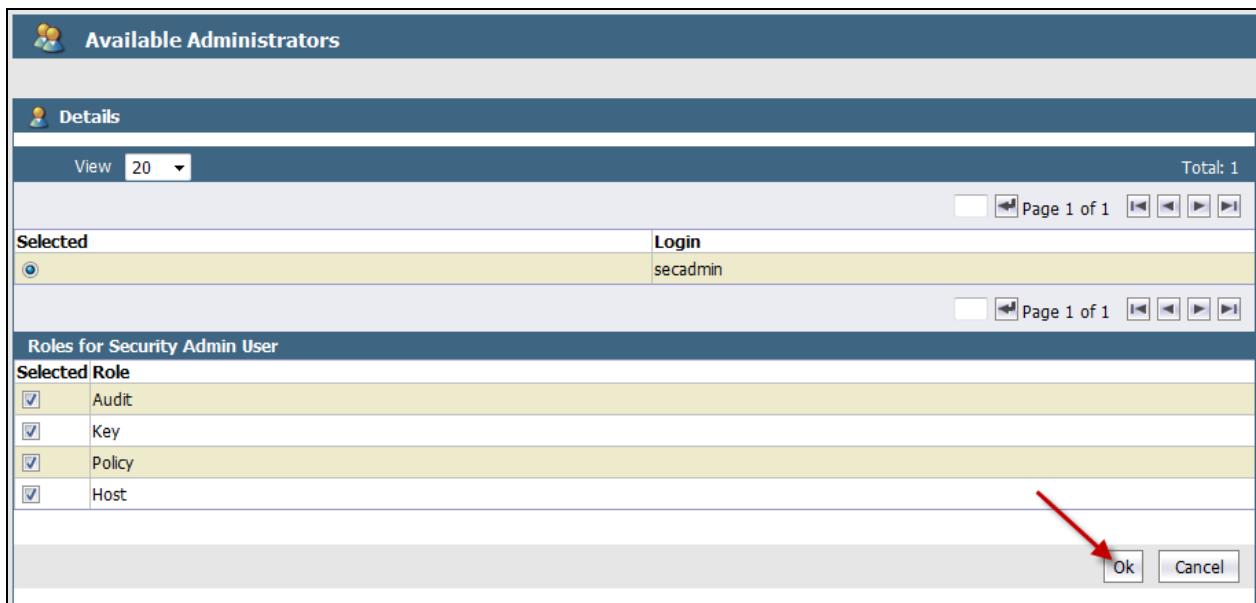
Note the change in number of tabs. As the security roles changes these tabs will vary based upon role.

__10. Click the **Add to Domain** button



__11. Select the radio button for **secadmin**

__12. Add a check for all the **Security Admin User** roles and click **OK**



__13. Log out by clicking the **Log Out** link

Lab 4 Administering hosts, policies, and keys

Hosts, policies and keys are the foundational components for implementing encryption. Most administration tasks involve creating, managing, or monitoring these components.

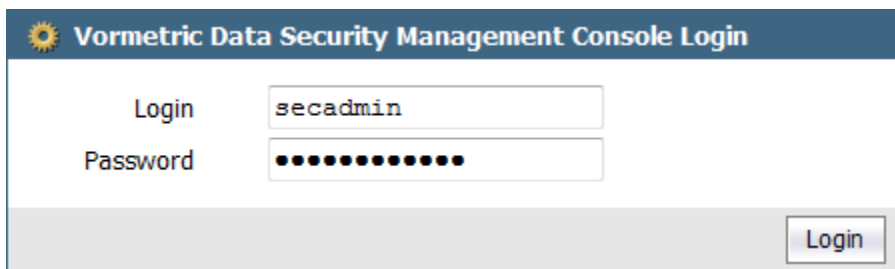
4.1 Create an encryption key

4.1.1 Login

__1. Login as the security administrator

ID = secadmin

Password = Secadmin123\$



__2. Change the password as required

Old Password = Secdmin123\$

New Password = Admin123\$

Confirm New Password = Admin123\$

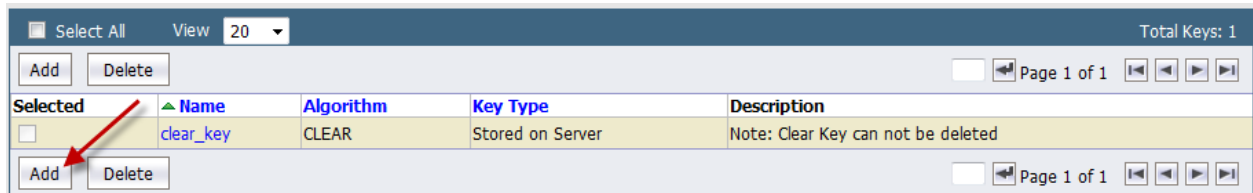
4.1.2 Create a key

Key management is an essential part of any encryption solution. Keeping the keys secure is as important or more important than the strength of the encryption algorithm. Within the EE solution the key security is maintained by the EE Server. The encryption keys are never exposed to any administrator or user. All transmission and persistence of the keys themselves are encrypted. In short the keys are known by name only and the key's value is never exposed.

- __1. Click on the **Keys** tab



- __2. Click the **Add** keys button



- __3. From the **Symmetric** tab, add the following key definition and click **Ok**

Name = test-aes256-key

Description = test aes 256 key

The image shows the Symmetric key definition form. The 'Ok' button is highlighted with a red arrow. The form fields are: Name (test-aes256-key), Description (test aes 256 key), Algorithm (AES128), Key Type (Cached on Host), Unique to Host (checkbox), and Key Creation Method (Generate).

4.2 Install and register host

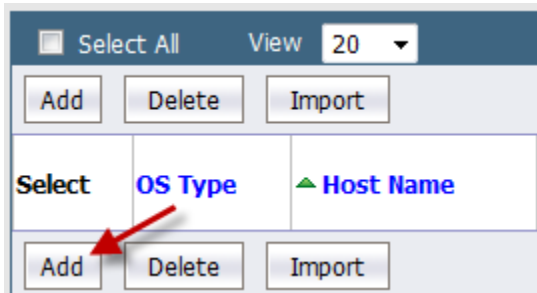
Each host that will communicate with the EE Server must be registered. The registration process produces a digital certificate and exchanges certificates with the host. Digital certificates have two functions they allow for encrypted communication between the host and agent and also provide assurances that the communication is coming from this host.

4.2.1 Add a host

__1. Click the **Hosts** tab



__2. Click the **Add** button



__3. Add a Host with the following description and click **Ok**

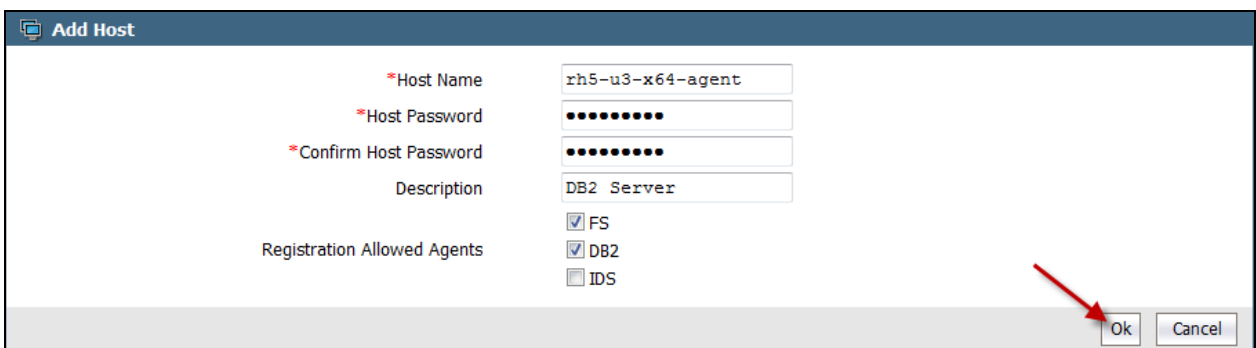
Host Name = rh5-u3-x64-agent

Host Password = Admin123\$

Confirm Host Password = Admin123\$

Description = DB2 Server

Check FS and DB2



4.2.2 Install agent and register host

Agent installation automatically attempts to perform registration as well. If registration fails there is no need to reinstall the agent registration can be stated by running the register_host script included during

the install. The installer installs the file system agent as well as the optional DB2 and IDS agents that are used for creating encrypted backups.

__1. Logon to the rh5-u3-x64-agent

ID = root

Password = password

__2. Change to the directory where the agent is located

```
cd /software
```

__3. Make the installer executable

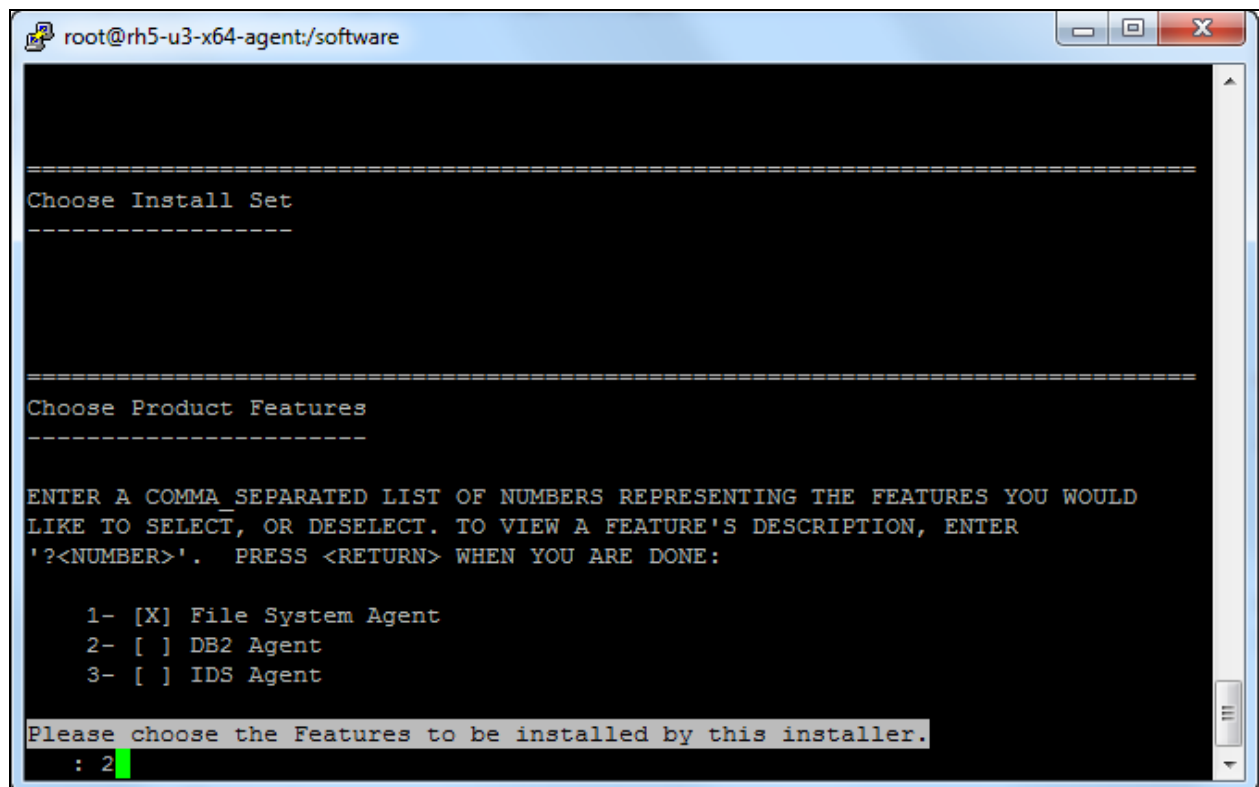
```
chmod 744 vee-agent-linux-4.4.0-736.bin
```

__4. Execute the installer with the option to perform a non-graphical install

```
./vee-agent-linux-4.4.0-736.bin -i console
```

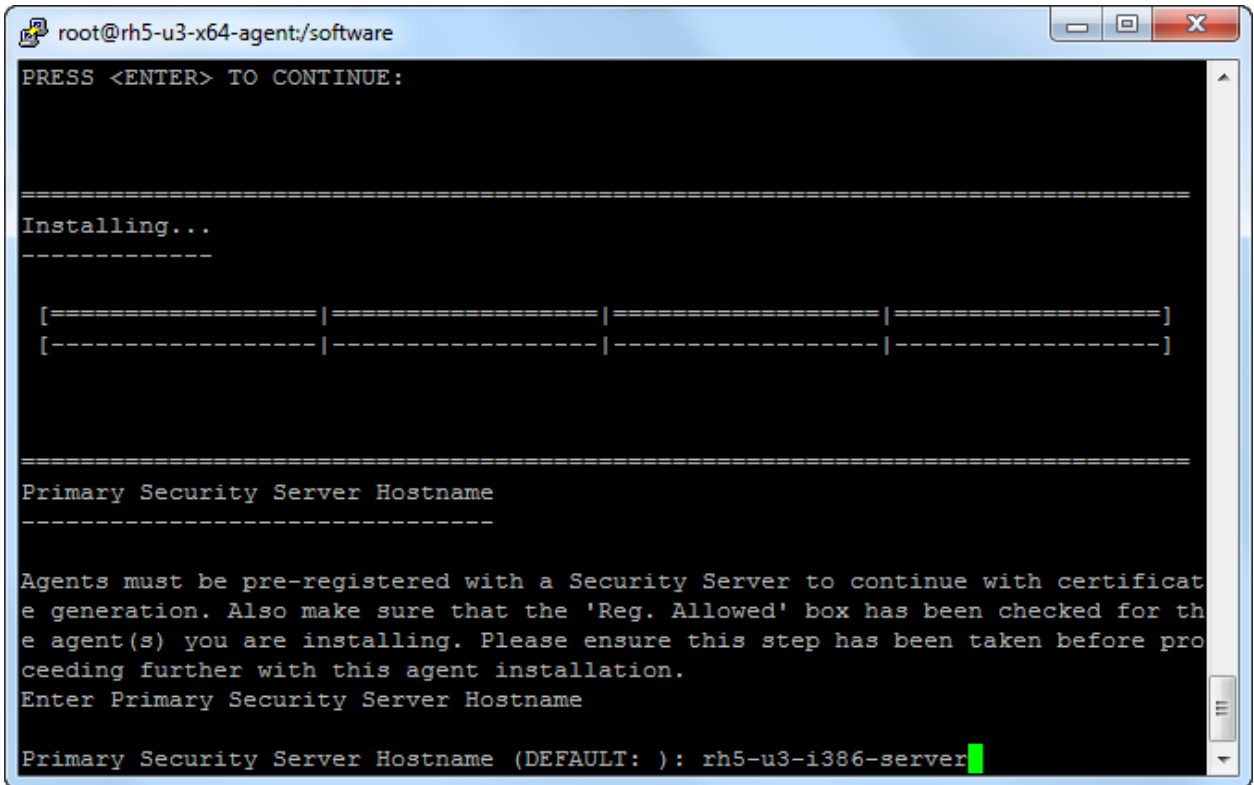
__5. Press **Enter** scroll through the license agreement and enter **Y** to accept

__6. When prompted, **Please choose the Features to be installed by this installer.** Type **1,2** to add install the file system agent and the DB2 agent.

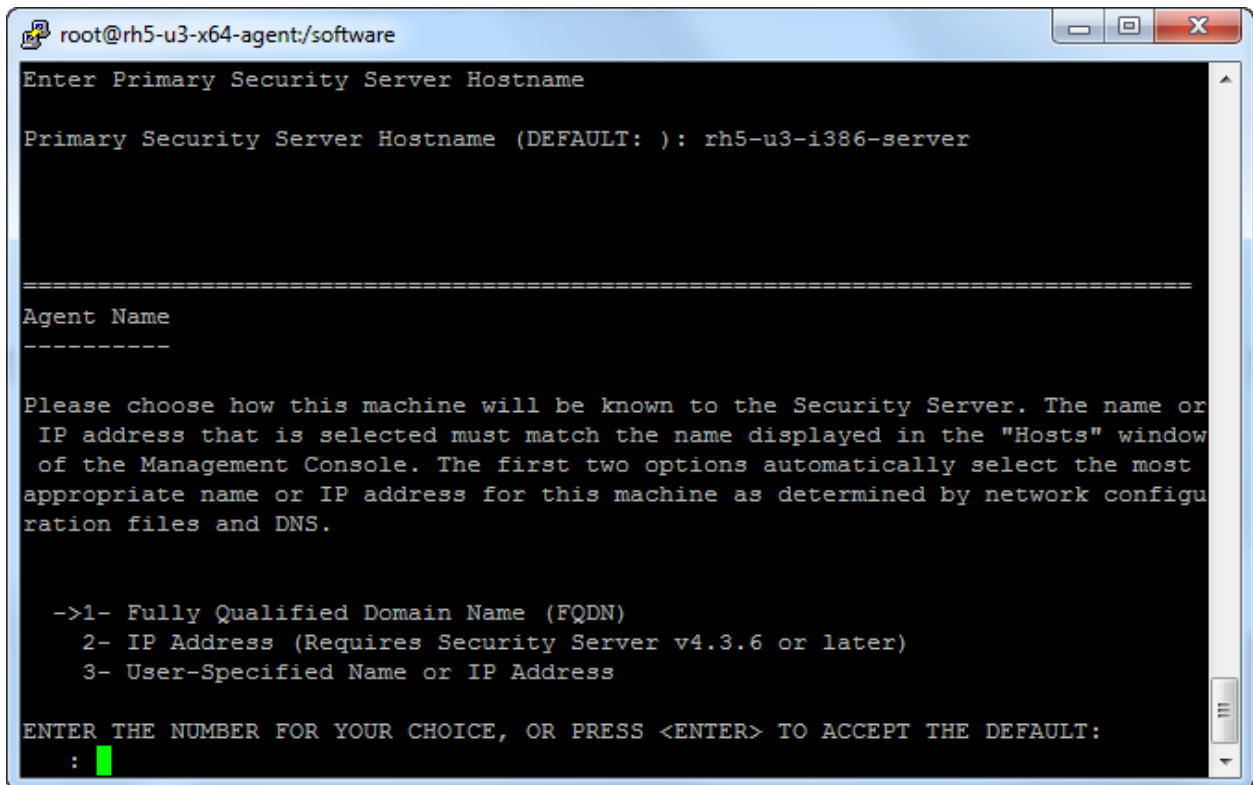
A terminal window titled 'root@rh5-u3-x64-agent:/software' showing the Veeam agent installation process. The screen displays two sections: 'Choose Install Set' and 'Choose Product Features'. Below these, instructions state: 'ENTER A COMMA SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER '?<NUMBER>'. PRESS <RETURN> WHEN YOU ARE DONE:'. A list of features is shown: '1- [X] File System Agent', '2- [] DB2 Agent', and '3- [] IDS Agent'. At the bottom, a prompt reads 'Please choose the Features to be installed by this installer.' followed by ': 2' and a green cursor.

__7. Press enter again to confirm your choice

- __8. Press enter again to continue
- __9. Enter **rh5-u3-i386-server** when prompted for the **Primary Security Server Hostname**



- __10. Accept the default option by pressing **Enter** when prompted for the **Agent Name**



```
root@rh5-u3-x64-agent:/software
Enter Primary Security Server Hostname

Primary Security Server Hostname (DEFAULT: ): rh5-u3-i386-server

=====
Agent Name
-----

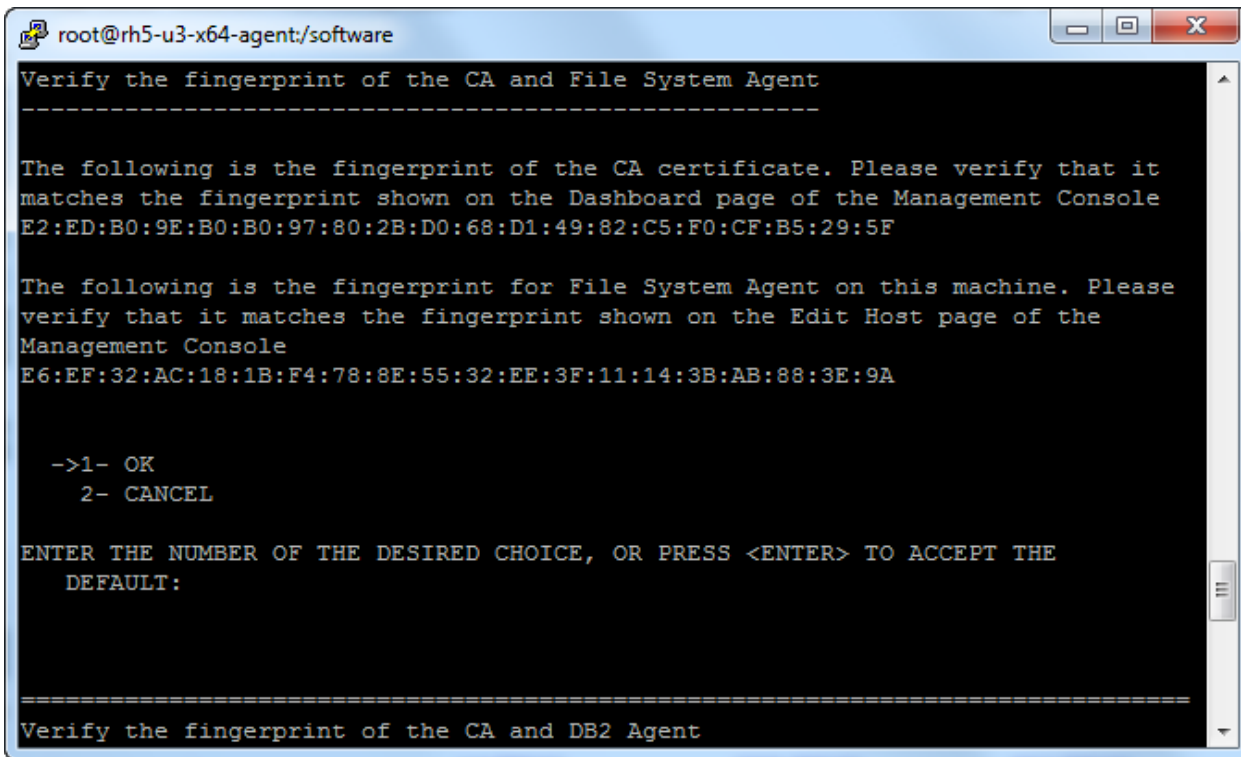
Please choose how this machine will be known to the Security Server. The name or
IP address that is selected must match the name displayed in the "Hosts" window
of the Management Console. The first two options automatically select the most
appropriate name or IP address for this machine as determined by network configu
ration files and DNS.

->1- Fully Qualified Domain Name (FQDN)
   2- IP Address (Requires Security Server v4.3.6 or later)
   3- User-Specified Name or IP Address

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
: █
```

- __11. Accept the default choice by pressing the enter key for all subsequent prompts

As the agent software is installed a set of fingerprints are generated in the form of hex strings.



These strings can be checked with the values displayed on the EE server to ensure there are no man-in-the-middle attacks.

- __12. Press enter to exit the Installer

The EE agent software is now installed and registered. The EE agent components, file system agent and DB2 agent, need to be explicitly allowed to communicate with the EE Server before security administration can take place.

4.3 Enable agent communication

Once registration is complete the communication enabled option must be enabled for the host to be able to communicate with the EE server for the purpose of security administration.

- __1. Click on the **Hosts** tab
- __2. Click the newly registered host, **rh5-u3-x64-agent**

Select All View 20 Total Hosts: 1										
Add Delete Import Page 1 of 1										
Select	OS Type	Host Name	FS Agent		DB2 Agent		IDS Agent		Description	Sharing
			Reg. Allowed	Comm. Enabled	Reg. Allowed	Comm. Enabled	Reg. Allowed	Comm. Enabled		
<input type="checkbox"/>	Linux	rh5-u3-x64-agent	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	DB2 Server	
Add Delete Import Page 1 of 1										

- __3. Check the **Communication Enabled** check boxes and click **OK**

Agent Information				
Agent	Version	Certificate Fingerprint	Registration Allowed	Communication Enabled
FS	4.4.0.0-Build736v	E6:EF:32:AC:18:1B:F4:78:8E:55:32:EE:3F:11:14:3B:AB:88:3E:9A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DB2	4.4.0.0-Build736v	33:F6:01:9E:AF:27:04:7D:AA:85:B1:2B:66:06:66:A2:A6:50:03:21	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IDS			<input type="checkbox"/>	<input type="checkbox"/>

Encryption administration can now be applied to the DB2 Server.

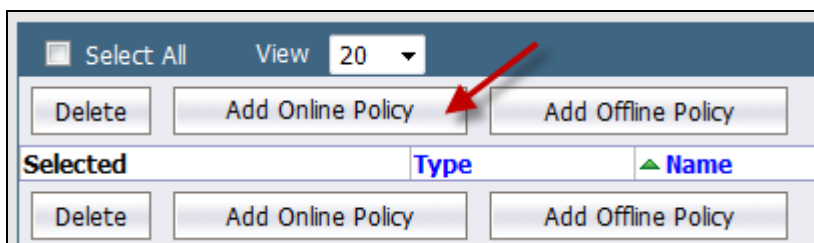
4.4 Create a policy

Policies are the central component for security administration. Policies are composed of rules which govern IO activity at the Guard Point. Rules are composed of 5 attributes and an effect. Rules are tested in order and when all the attributes of a policy rule are met then the rules effect is triggered. No other subsequent rules are tested.

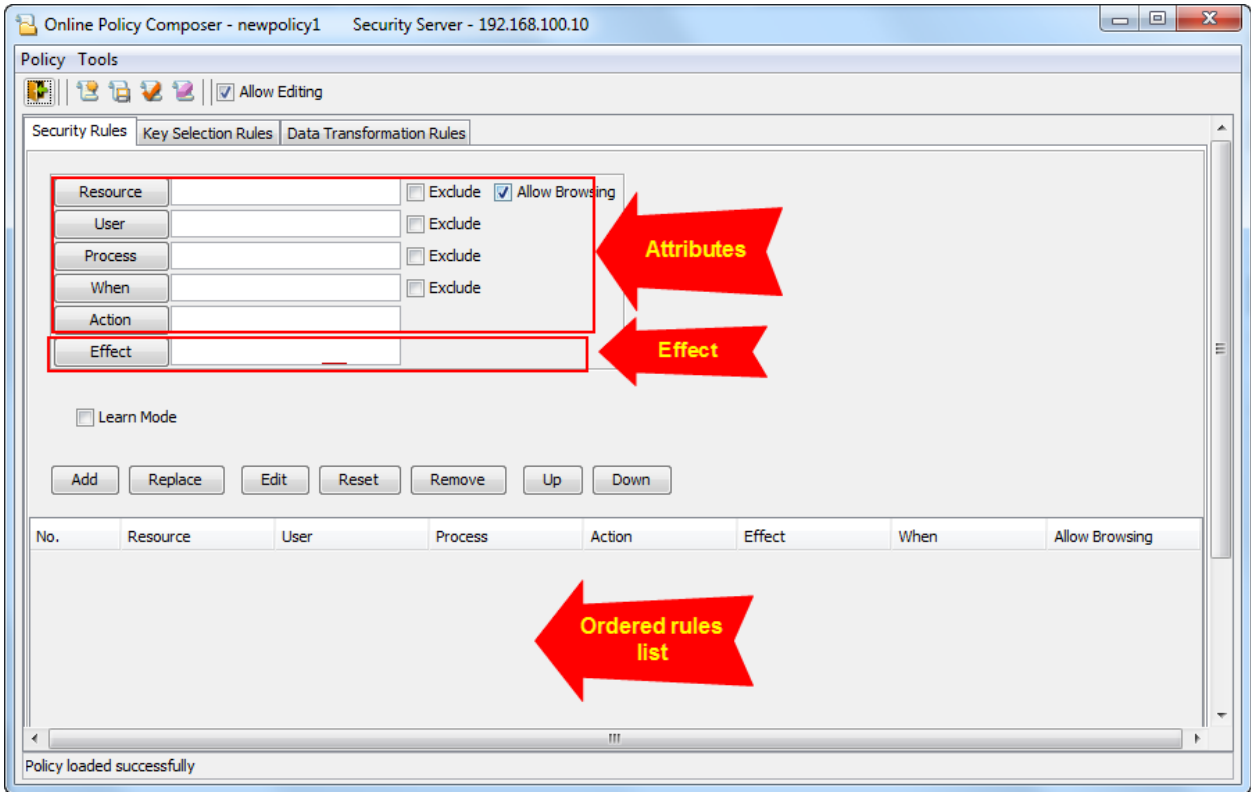
- __1. Open the policy editor, click **Policies > Manage Policies**



- __2. Click the **Add Online Policy** button



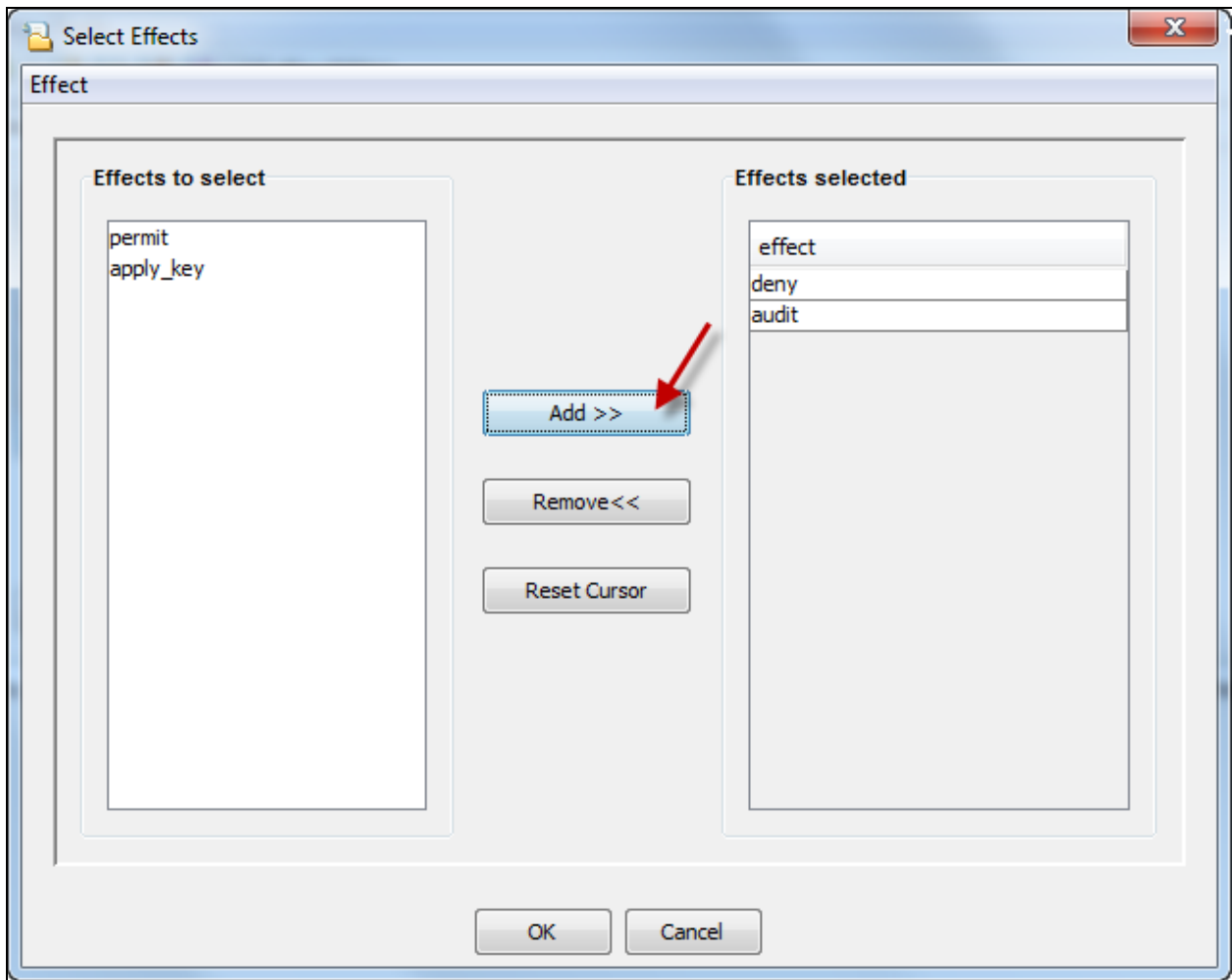
The Policy Editor has two sections, one to edit rules and the second to list and order the rules.



__3. Add “catch-all” rule

The “catch-all” rule is always the last rule in the policy. It is the rule that states that if none of the rules above it match all the attributes then this rule is guaranteed to match. The behavior of the rule is almost always to **Deny**, and **Audit** the IO.

- __a. Click the **Effect** button
- __b. Select **deny** and **audit** and click the **Add** button



- __c. Click the **Ok** button
- __d. Click the **Add** button to add the rule

No.	Resource	User	Process	Action	Effect	When	Allow Browsing
1					deny audit		on

Note, that blanks in a rule definition mean “any” or could be considered wild cards. A pseudo reading of the rule could be, “For every **Resource** (file), for every executing **User**, for every executing **Process**, for every IO **Action**, **deny** and **audit** the IO. The **When** attribute is relative to time but is not commonly used.

- __4. Add a rule that governs the VI editor

- __a. Click the **Reset** button to clear the previous rule definition

The screenshot shows a configuration window with several input fields and checkboxes. The fields are: Resource, User, Process, When, Action, and Effect. The Effect field contains the text "deny audit". To the right of the Resource, User, Process, and When fields are checkboxes labeled "Exclude" and "Allow Browsing". The "Allow Browsing" checkbox is checked. Below the fields is a "Learn Mode" checkbox, which is unchecked. At the bottom of the window are buttons for "Add", "Replace", "Edit", "Reset", "Remove", "Up", and "Down". A red arrow points to the "Reset" button. Below the buttons is a table with the following structure:

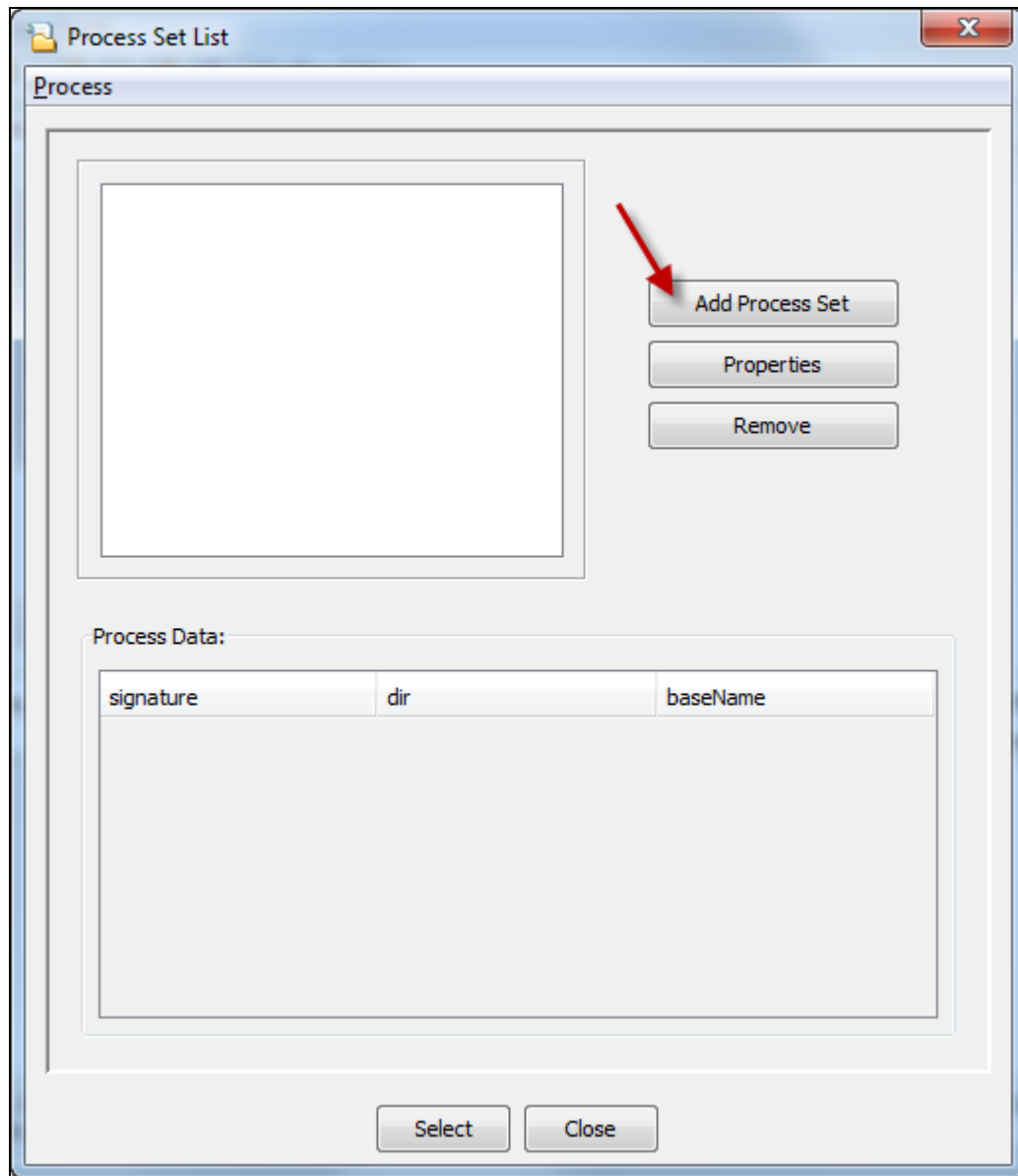
No.	Resource	User	Process	Action
1				

- __b. Click on the **Process** button, to add a process attribute

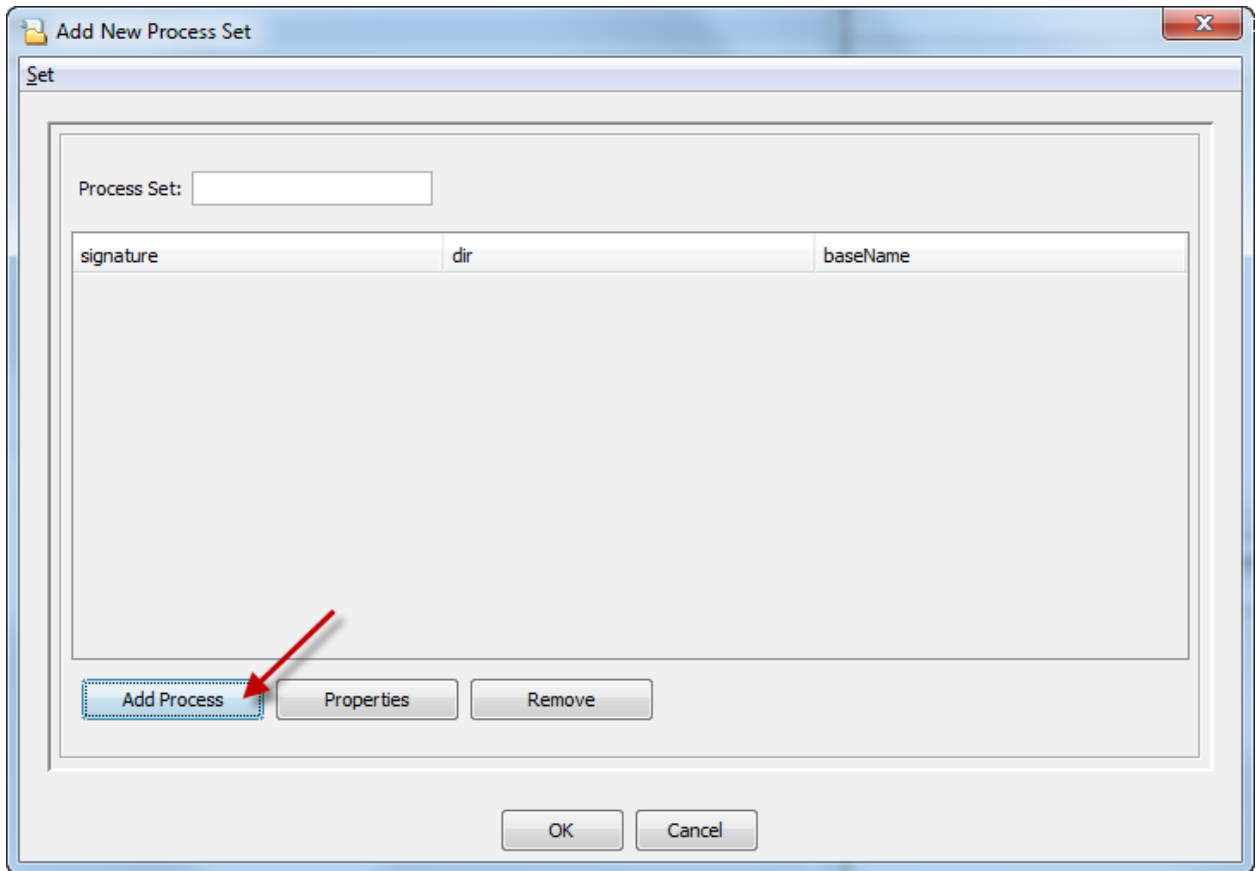
The value of the Process attribute is a set of processes (executables). There are no defined process sets.

This screenshot is identical to the one above, but with a red arrow pointing to the "Process" button in the configuration window. The "Process" button is highlighted with a blue border and a dotted outline.

__c. Click the **Add Process Set** button



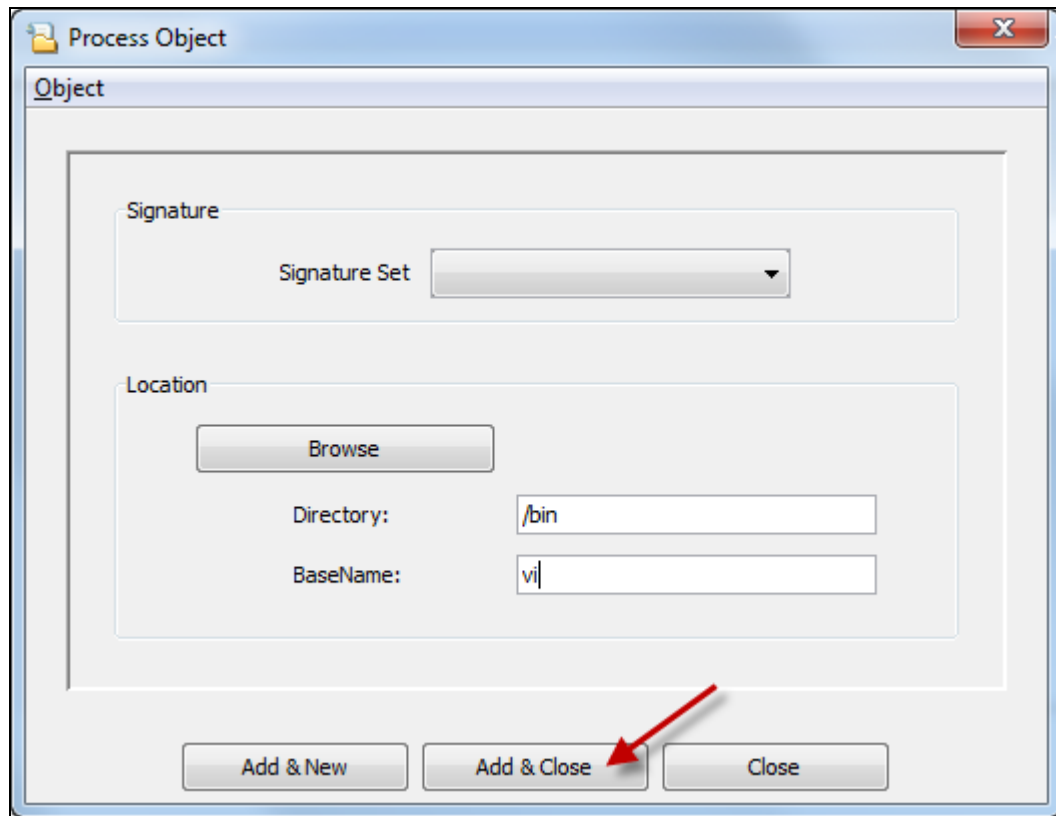
__d. Click the **Add Process** button



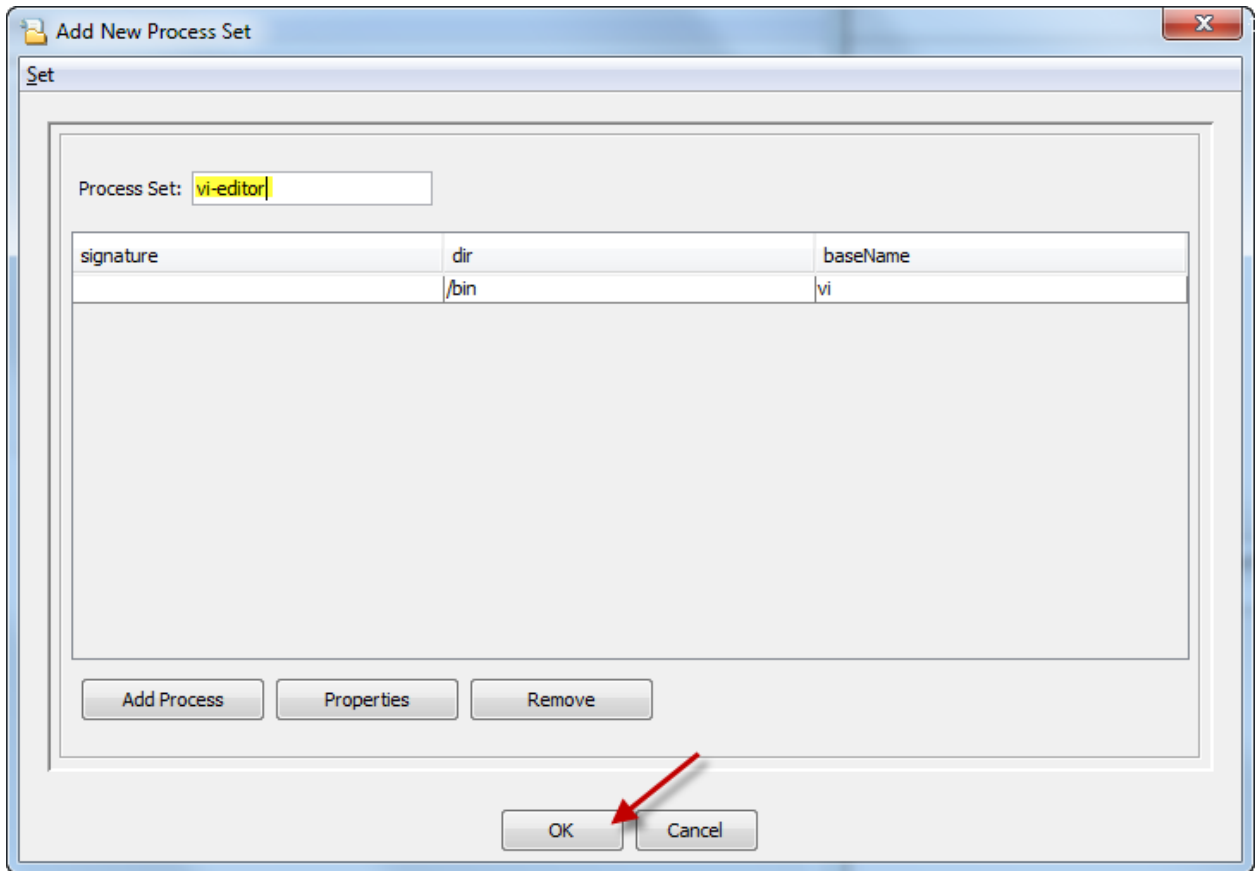
__e. Type the following information **Process Object** fields and click **Add & Close**

Directory = /bin

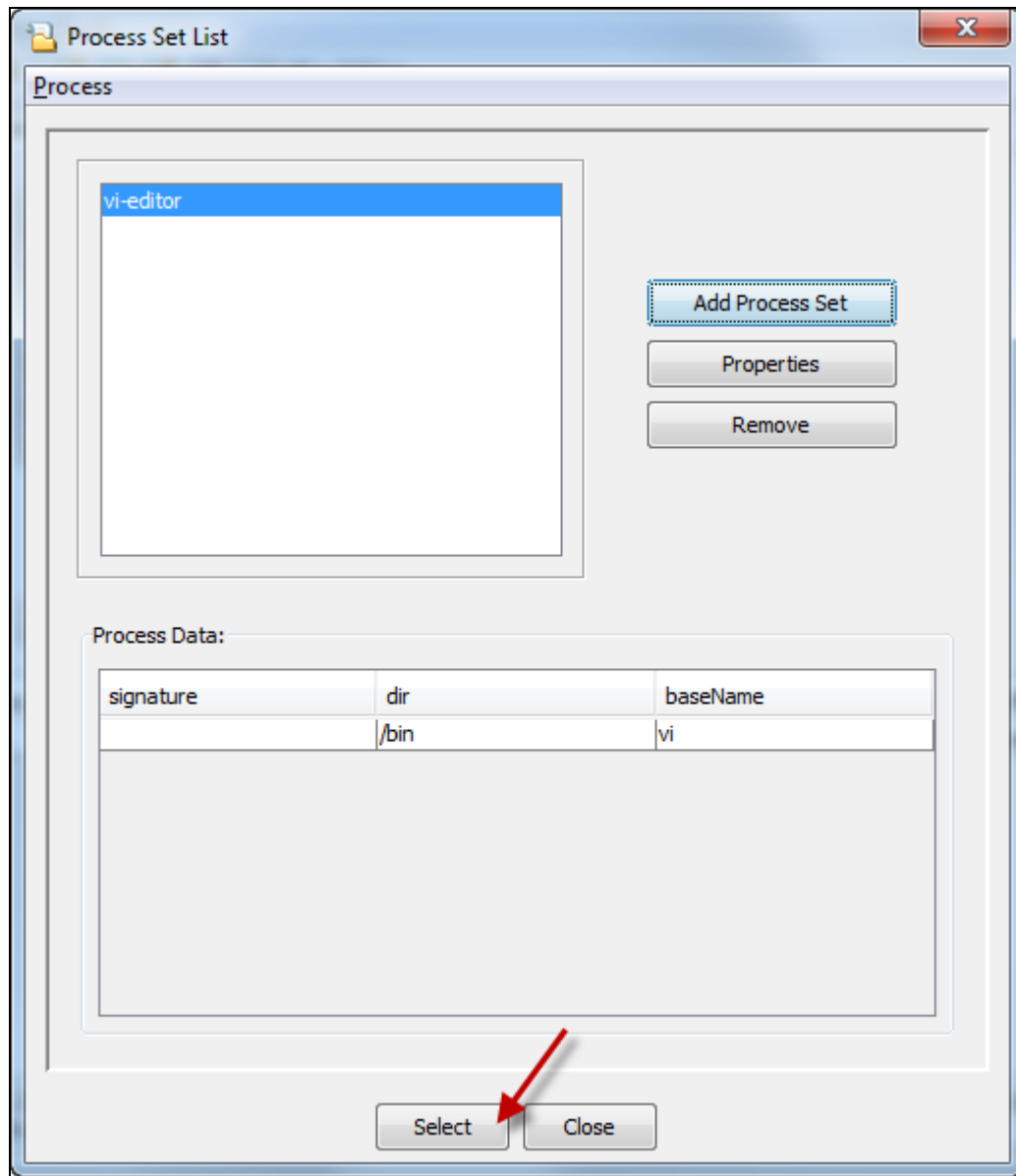
Basename = vi



__f. Change the **Process Set** name to **vi-editor** and click **OK**

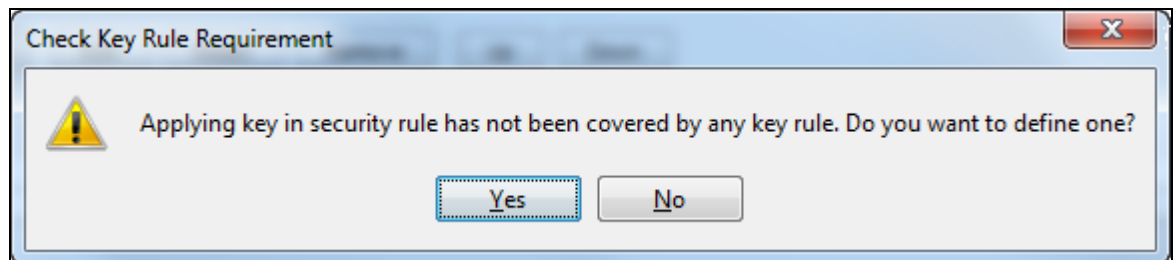


- __g. With the vi-editor selected, click the **Select** button

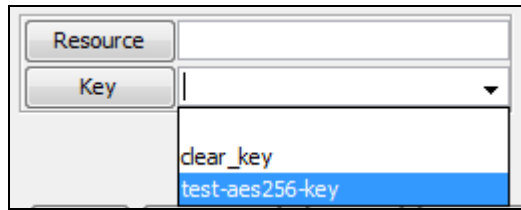


- __h. Change the **Effect** to **permit apply_key** and click the **Add** button

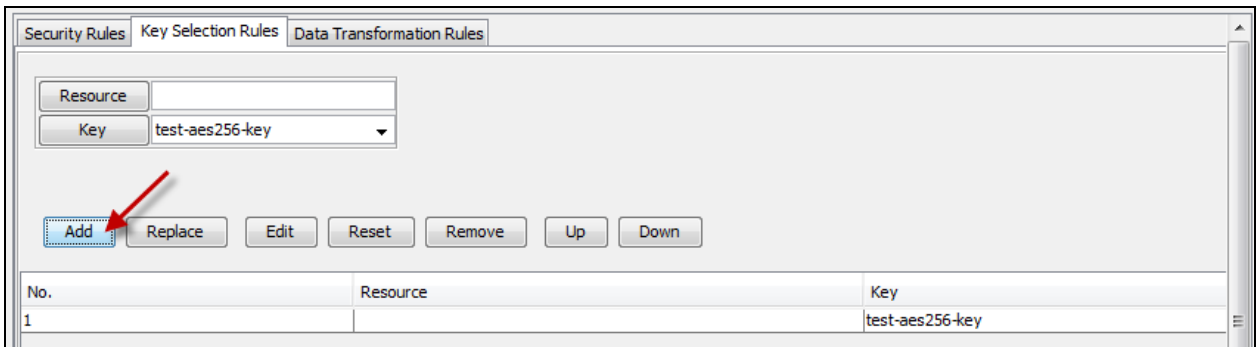
The prompt to define key rule is displayed.



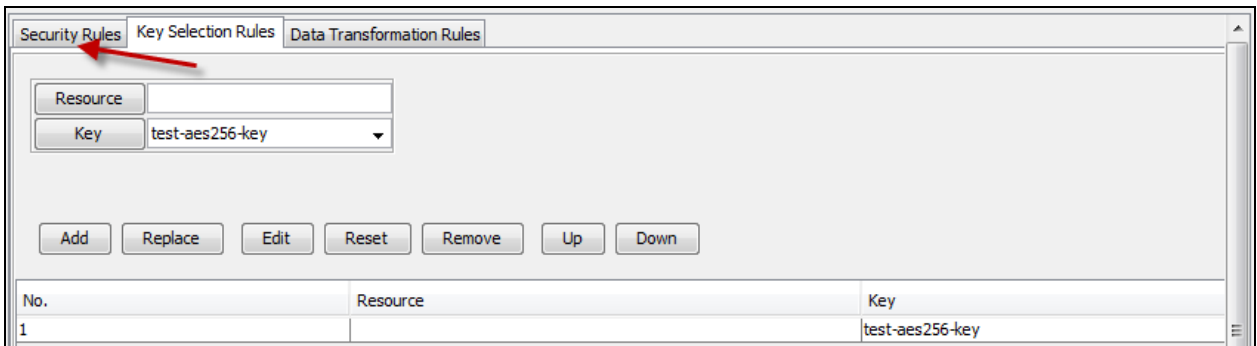
- __i. Click the **Yes** button
- __j. From the **Key Selection Rules** tab, **Key** drop-down menu tab select the test-aes256-key



- __k. Click the **Add** button

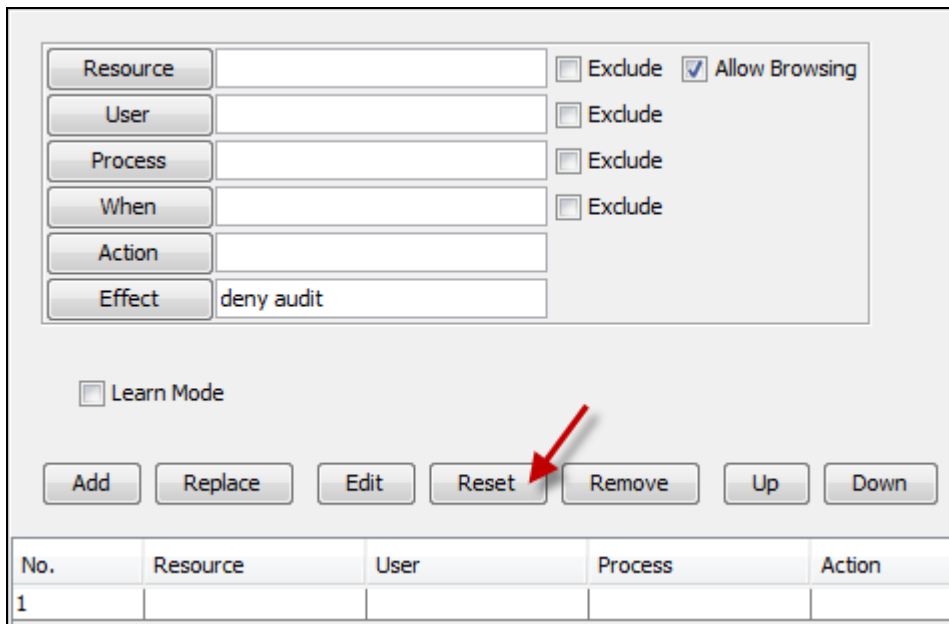


- __l. Click the **Security Rules** tab



- __5. Add a rule that governs the cat

- __a. Click the **Reset** button to clear the previous rule definition



The screenshot shows a rule configuration window with the following fields and options:

- Resource: [] Exclude Allow Browsing
- User: [] Exclude
- Process: [] Exclude
- When: [] Exclude
- Action: []
- Effect: deny audit

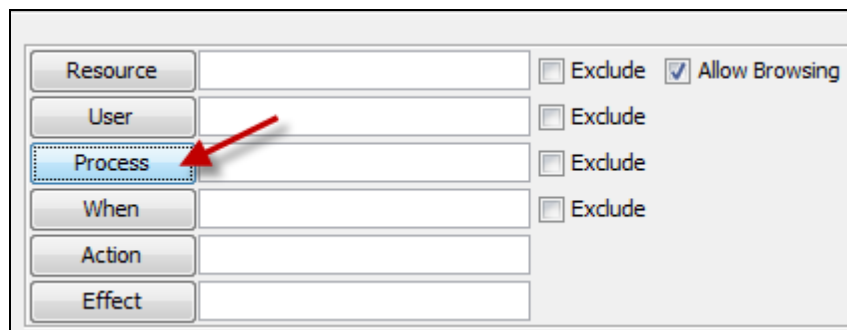
Below the fields is a checkbox for Learn Mode.

A row of buttons is located below the checkboxes: Add, Replace, Edit, **Reset** (highlighted with a red arrow), Remove, Up, and Down.

No.	Resource	User	Process	Action
1				

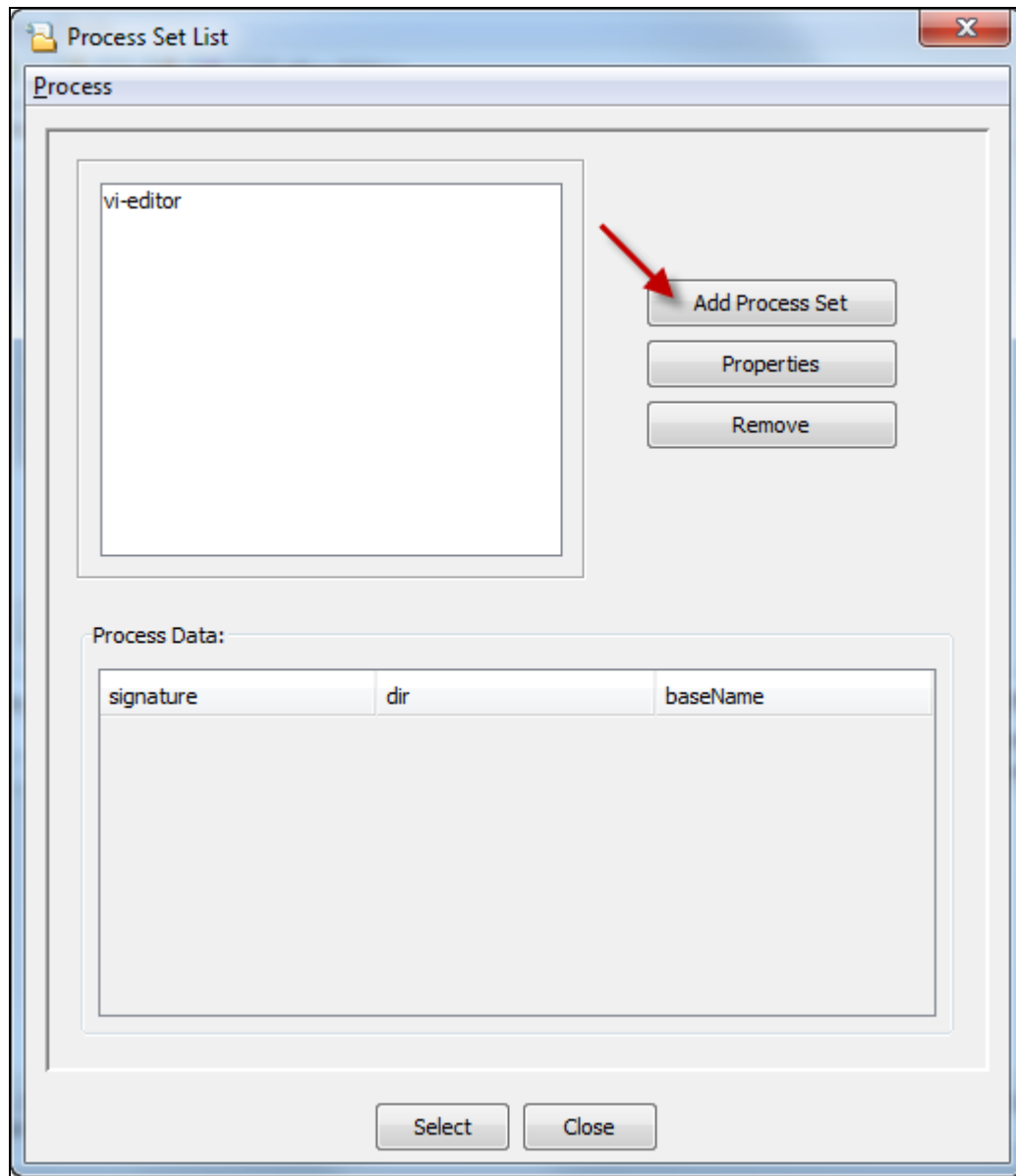
- __b. Click on the **Process** button, to add a process attribute

The value of the Process attribute is a set of processes (executables). There are no defined process sets.

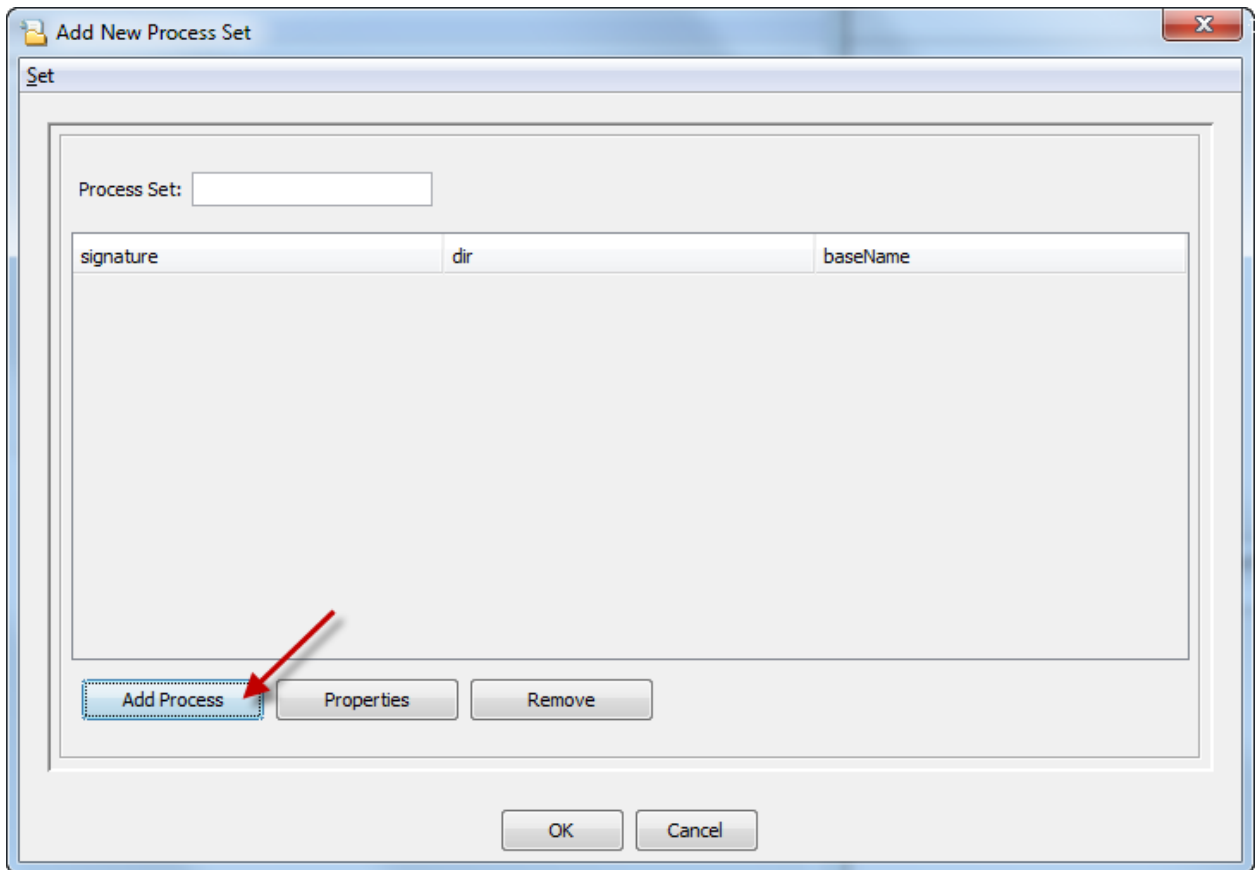


The screenshot shows the same rule configuration window as above, but with the **Process** button highlighted by a red arrow.

__c. Click the **Add Process Set** button



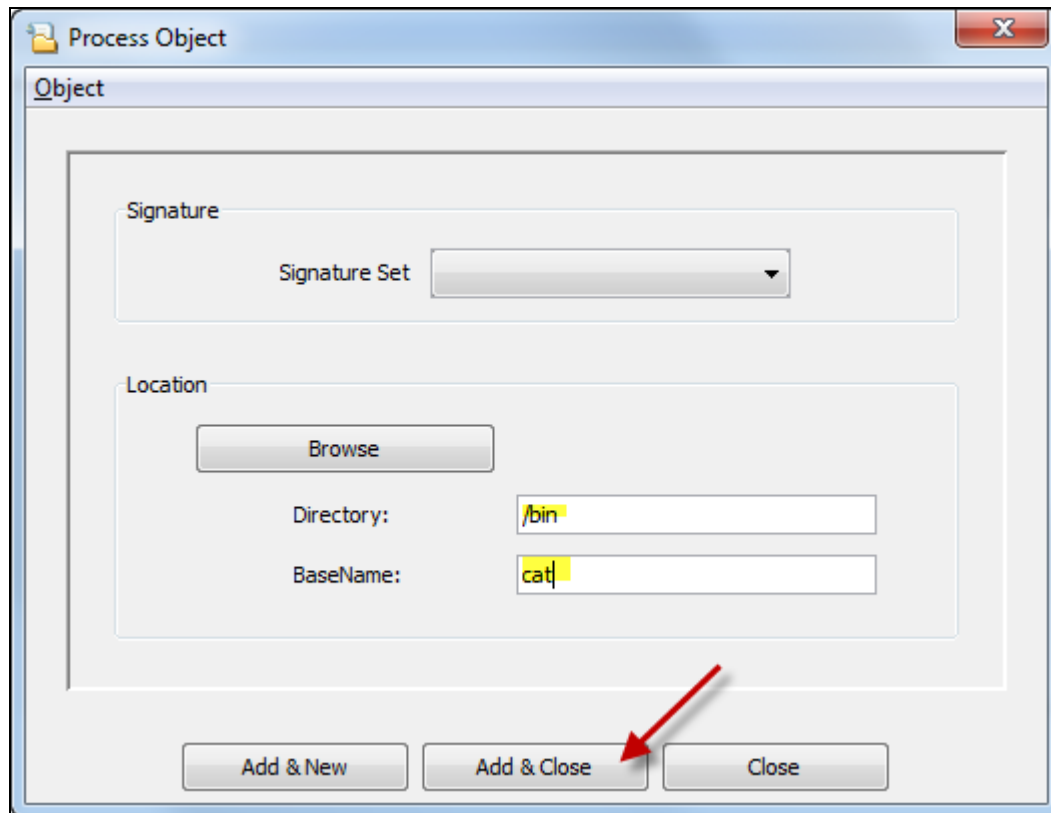
__d. Click the **Add Process** button



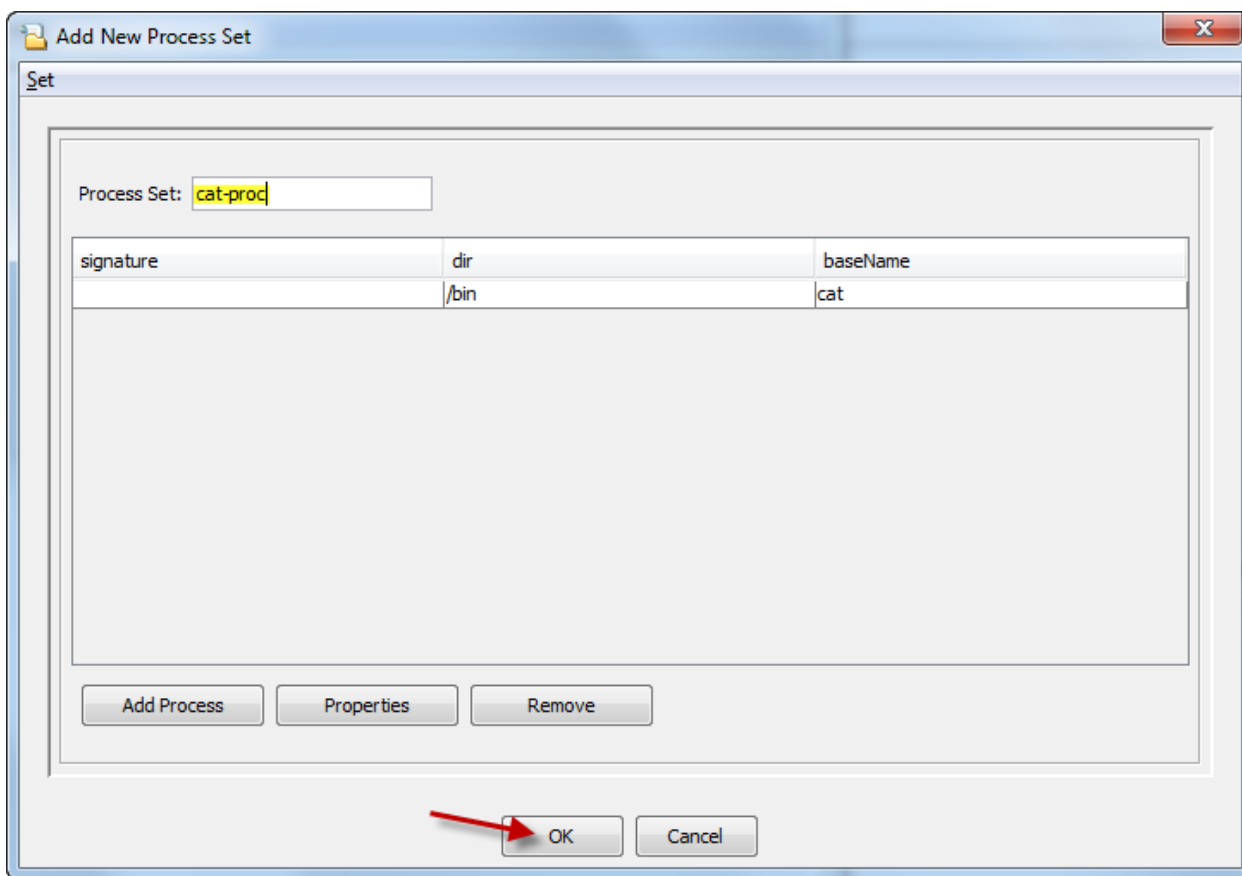
- __e. Type the following information **Process Object** fields and click **Add & Close**

Directory = /bin

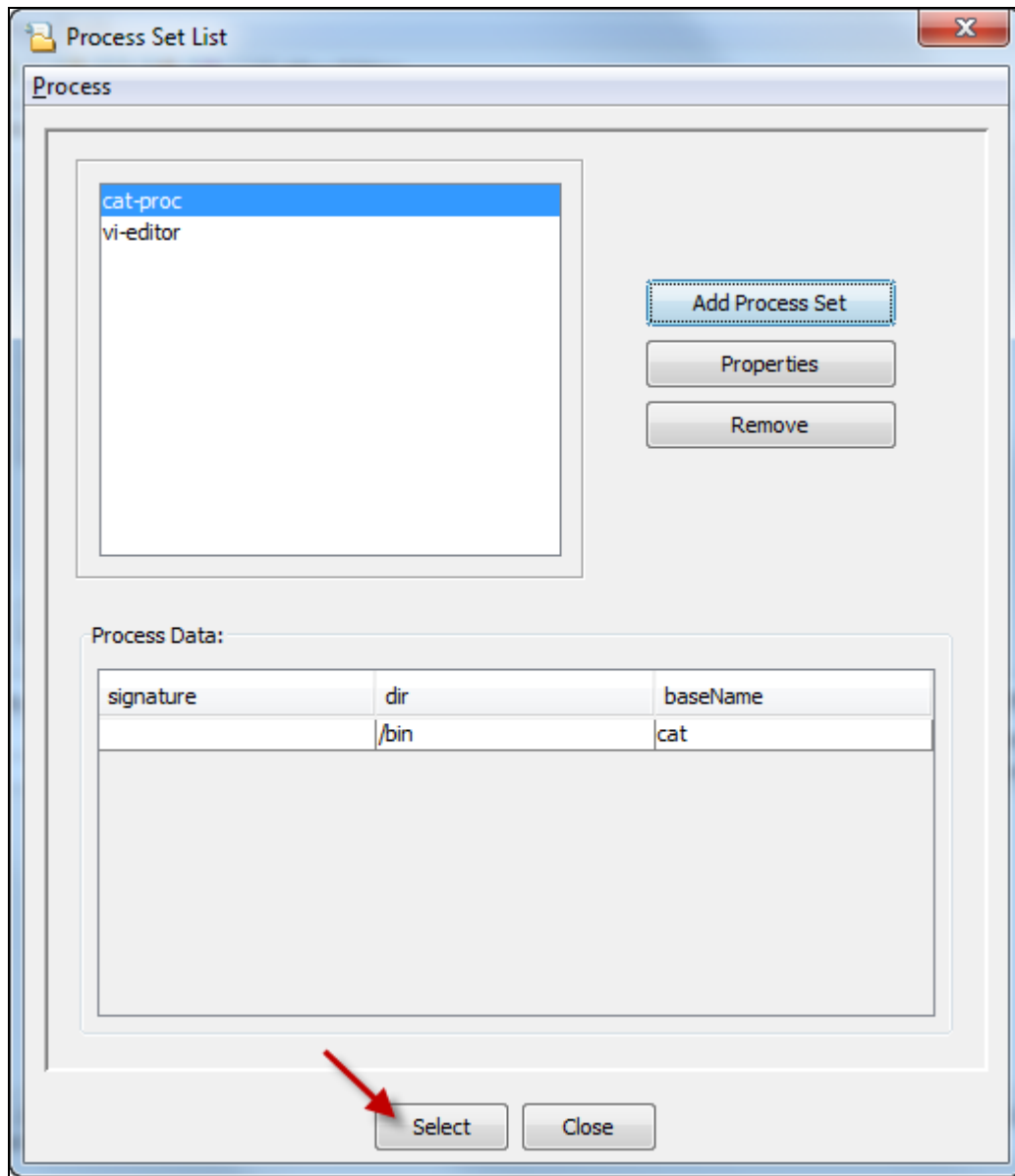
Basename = cat




__f. Change the **Process Set** name to **cat-proc** and click **OK**

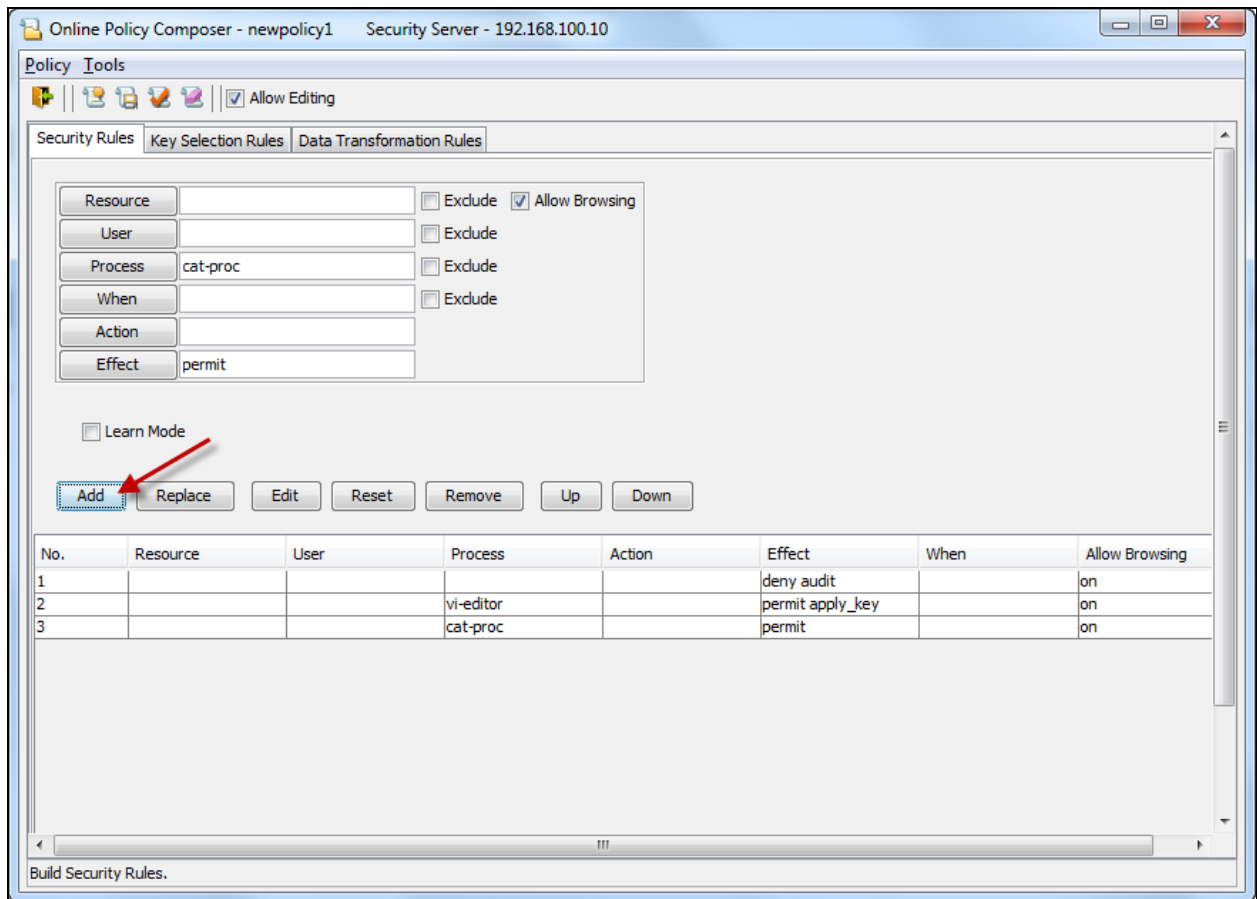


- __g. With the **cat-proc** selected, click the **Select** button



- __h. Change the **Effect** to **permit** and click the **Add** button

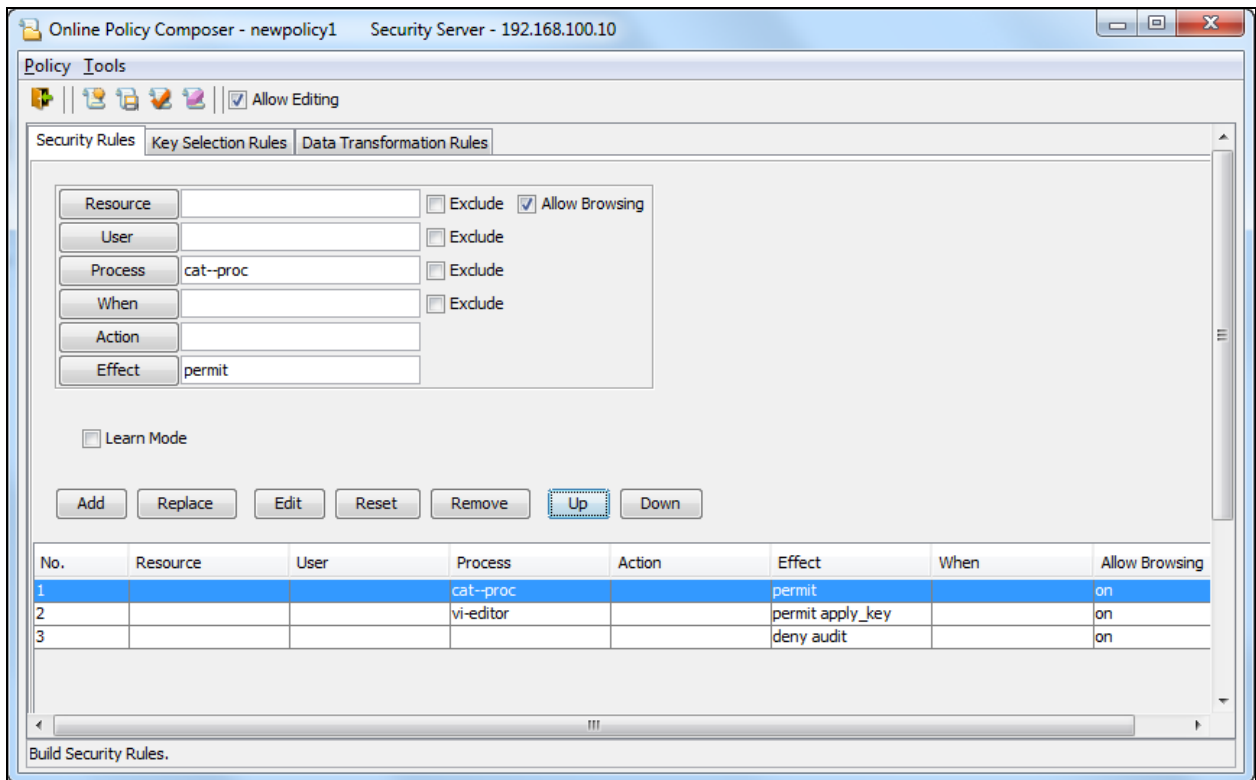
 **Important!** Do not include the **apply_key** effect. Cat will be use to demonstration reading files without unencrypting the data.




__6. Reorder the rules.

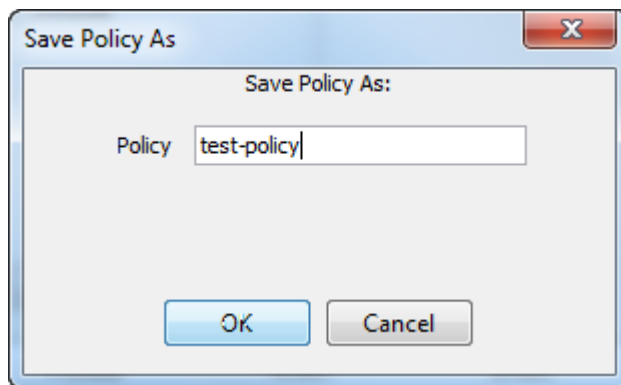
- __a. Highlight the **vi-editor** rule and click the **Up** button to move the rule to the top of the list
- __b. Highlight the **cat-proc** rule and click the **Up** button to move the rule to the top of the list


The policy should look as follows:



__7. Save and name the Policy

- __a. Click the  icon to save the policy
- __b. Name the policy **test-policy** and click the **OK** button



Exit the policy editor by clicking the  icon

Once a policy has been created it can be applied to a host to protect a point within the file system, the guard point.

Lab 5 Encrypting data the basics

Encrypting data is a function of applying the encryption key to clear text data to produce encrypted text. This is accomplished with EE by creating a guard point. A guard point is directory within the file system where a encryption policy is applied. Once the policy is applied all IOs to that directory and all subdirectories are evaluated according to the policy rules.

5.1 Create a guard point and apply a policy

- __1. Click the **Hosts** tab

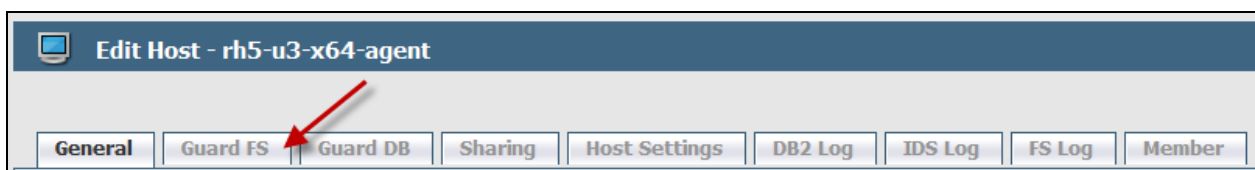


- __2. Click the **rh5-u3-x64-agent** host

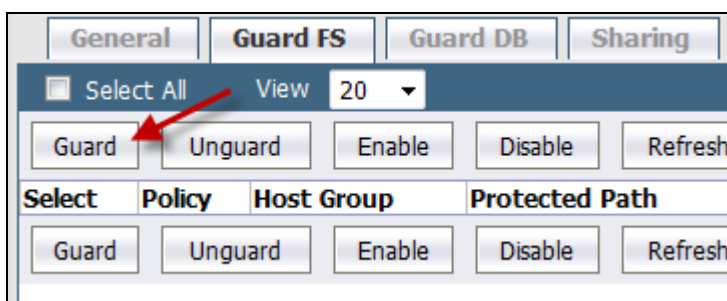
Select	OS Type	Host Name
<input type="checkbox"/>	Linux	rh5-u3-x64-agent

A red arrow points to the 'rh5-u3-x64-agent' host name in the table.

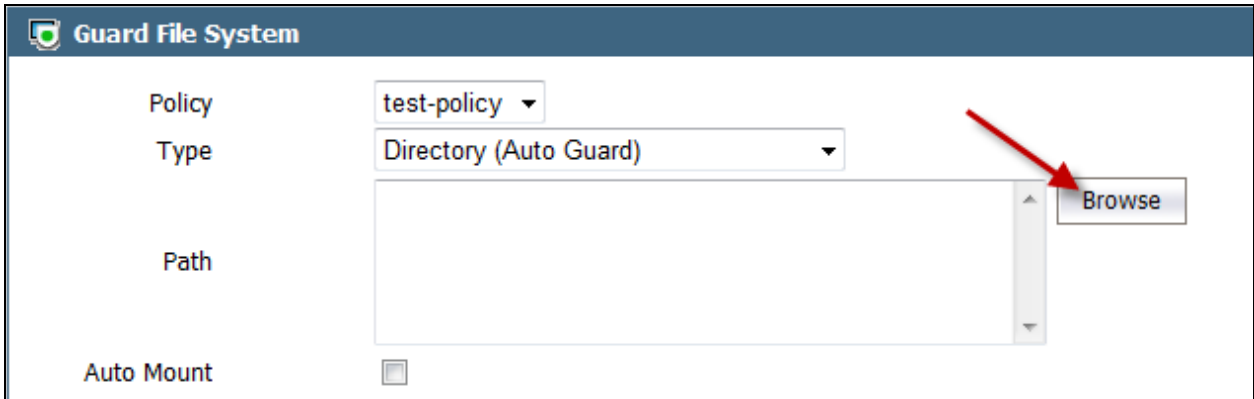
- __3. Click the **Guard FS** tab



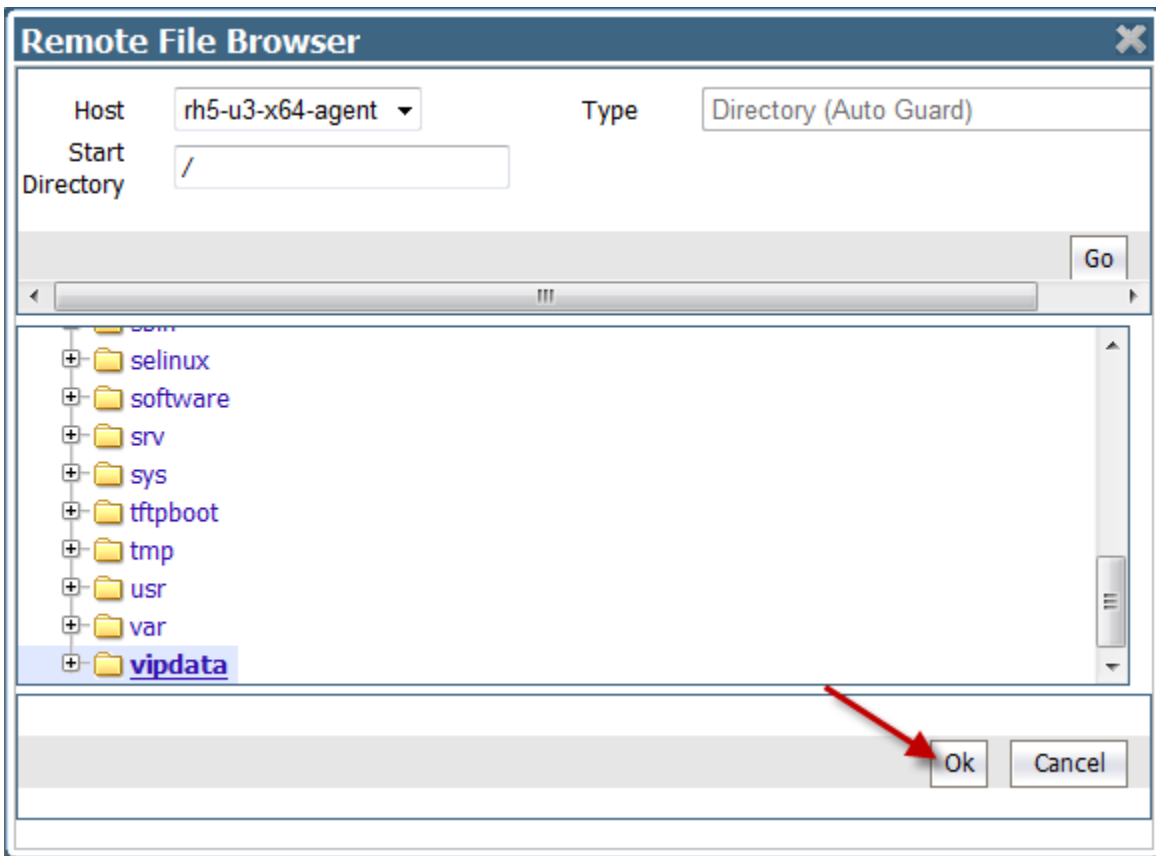
- __4. Click the **Guard** button



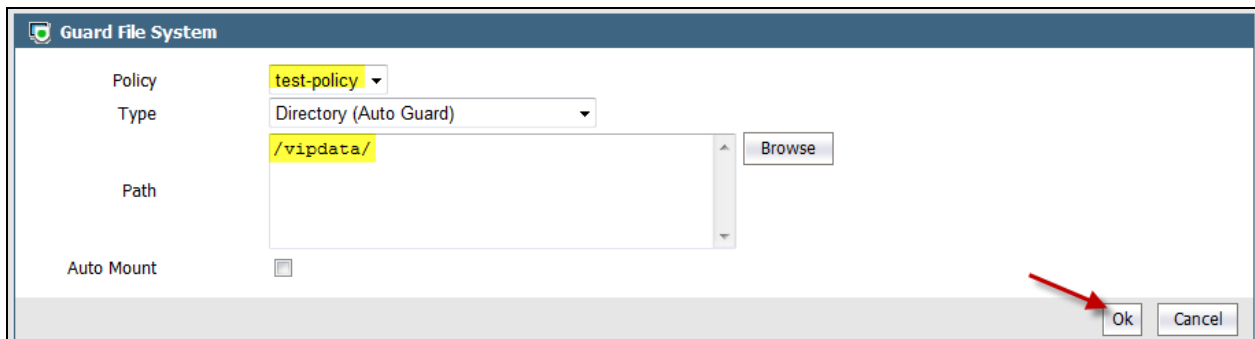
__5. Click the **Browse** button



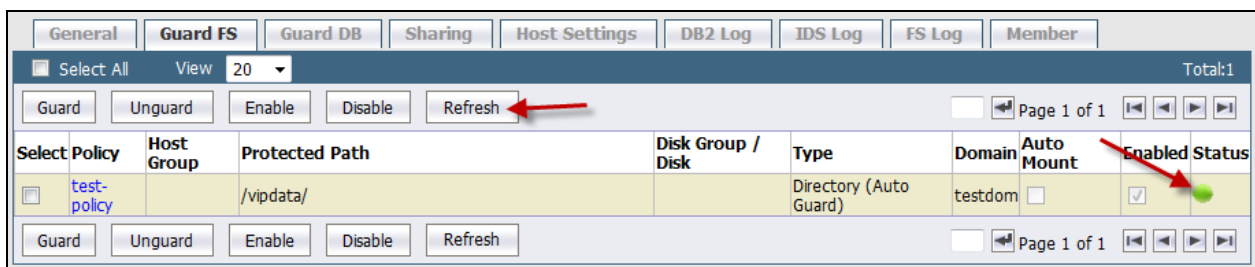
__6. Select the **vipdata** directory and click the **Ok** button



- __7. Ensure **test-policy** is the chosen policy and **/vipdata/** path is displayed, click the **Ok** button



- __8. Click the **Refresh** button until the **Status** light is green



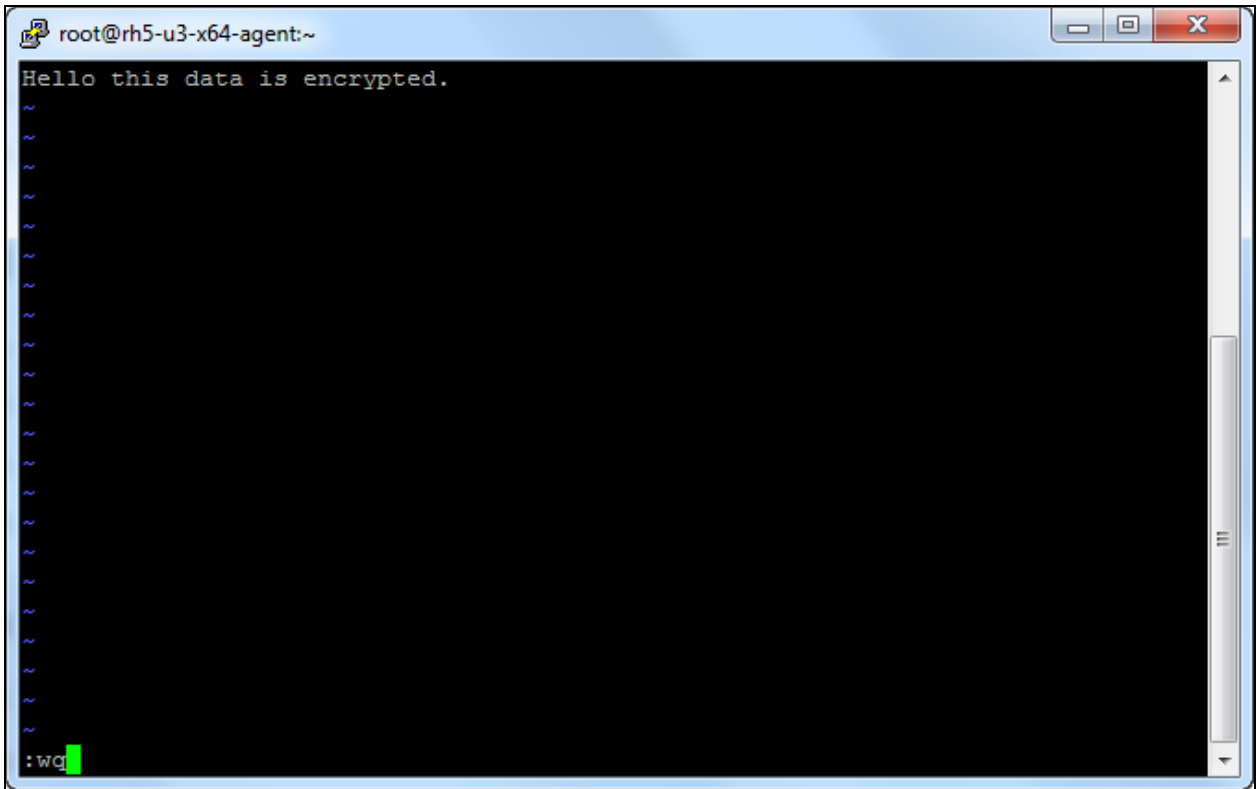
Your guard point is now defined and can be tested.

5.2 Test policy actions

The directory `/vipdata` is now an active guard point. All IO activity to this directory is now governed by `test-policy`. The VI editor will be able to read and write encrypted data within the guard point. The `cat` program can only read files but not unencrypt the data. No other activity should be possible within the guard point.

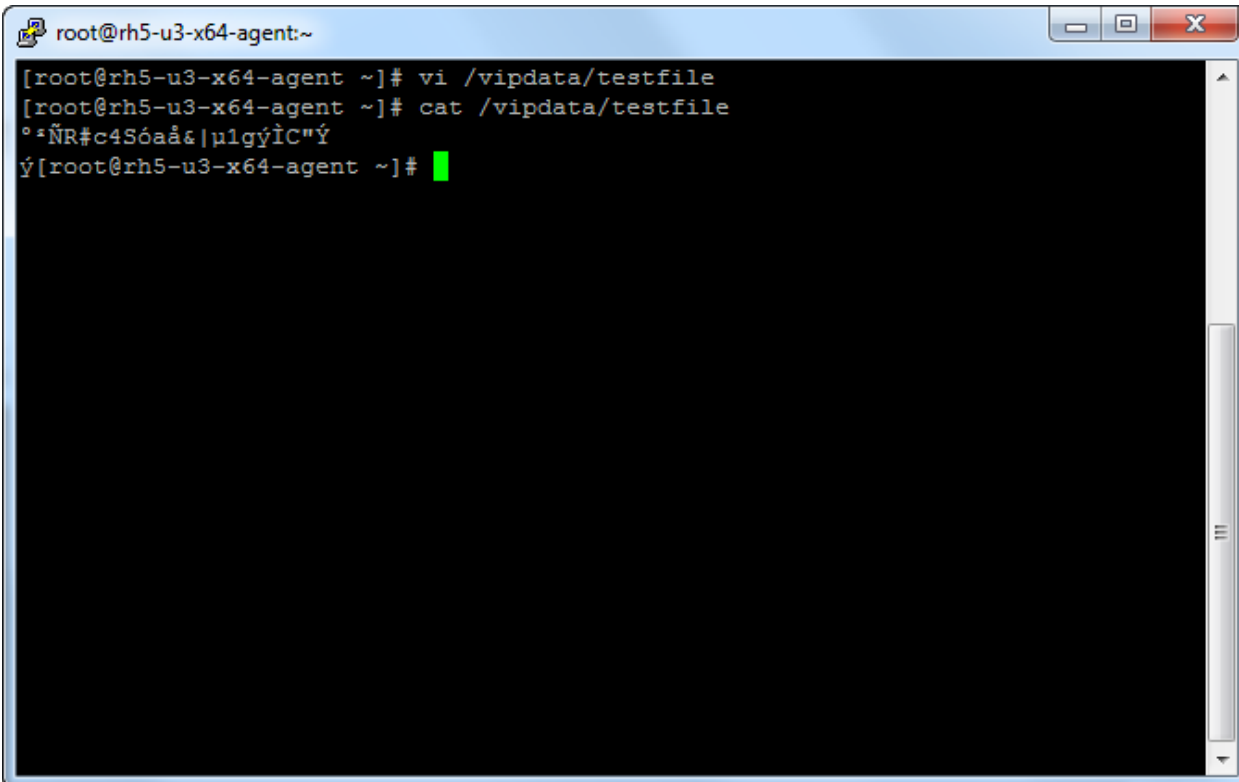
- __1. Create and edit a file with the VI
- __a. From the agent open and create a new file, **testfile**, within the guard point


```
vi /vipdata/testfile
```
 - __b. Enter some text like "hello this will be encrypted"
 - __i. Press the "i" to starting entering data
 - __ii. Type your text
 - __iii. Press the Esc to stop entering data
 - __iv. Save and exit by pressing `:"wq` [There is a ":" before the "w"] and pressing enter



__2. Try viewing the data with cat

```
cat /vipdata/testfile
```



```
root@rh5-u3-x64-agent:~  
[root@rh5-u3-x64-agent ~]# vi /vipdata/testfile  
[root@rh5-u3-x64-agent ~]# cat /vipdata/testfile  
°ÑR#c4Sóaa&|u1gyÏC"Ý  
ý[root@rh5-u3-x64-agent ~]#
```

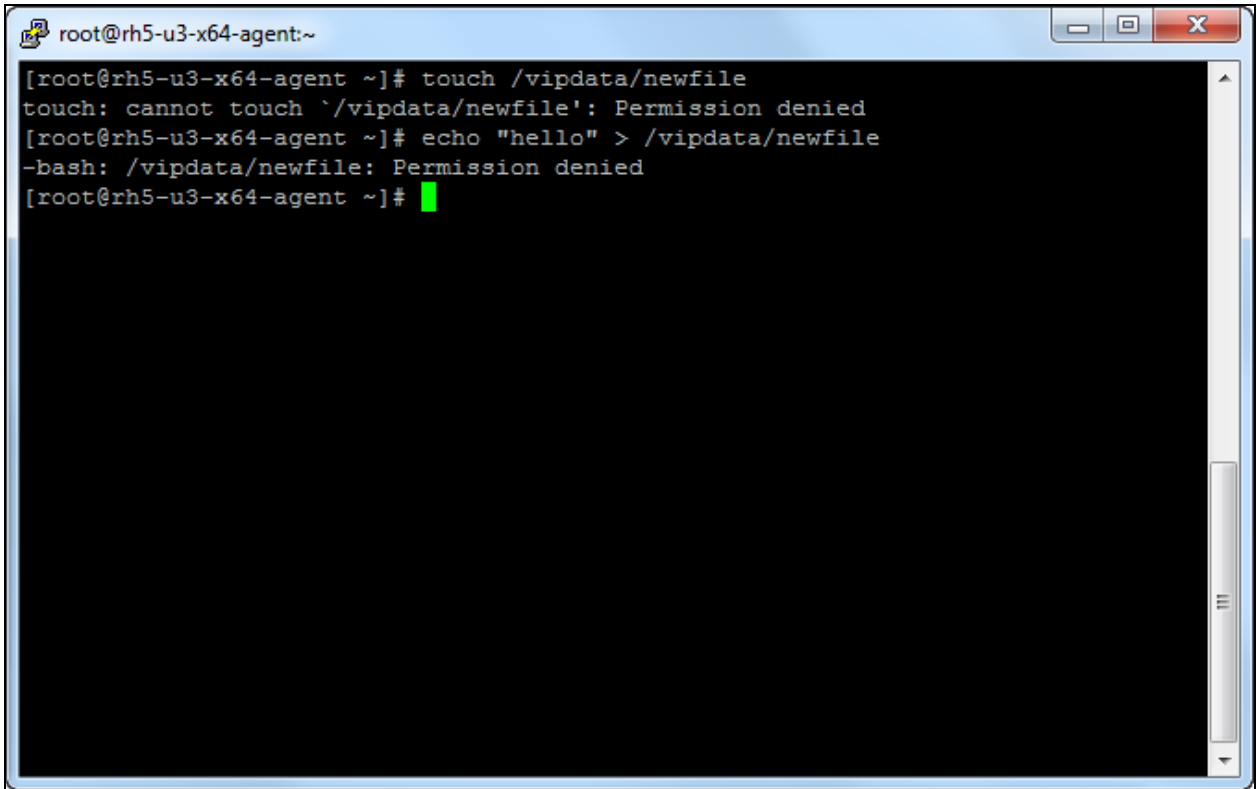
Note that the **output** is scrambled validating that the data is encrypted and cat can not unencrypted the encrypted text. The VI editor can edit the document without issue.

__3. Try creating or editing files with other processes

```
touch /vipdata/newfile
```

```
echo "hello" > /vipdata/newfile
```

All access is denied to all processes except vi and cat.



__4. View the audit records for these events

__a. From the browser, click the **Log** tab



- __b. Note the audit records show how the EE agent **DENIED** the IO. Other information is displayed like what the name of the **Policy** was, what was the name of the **User**, what was the name of the **Process**, what was the IO type (**Action**).

672	2010-08-20 07:38:03.34 PDT	E	rh5-u3-x64-agent	CGP2606E: [SecFS, 0] [ALARM] Policy[test-policy] User[root,uid=0 (User Not Authenticated)] Process [/bin/bash] Action[create_file] Res[/vipdata/newfile] Effect[DENIED Code (1P,2P,3M)]
671	2010-08-20 07:37:44.423 PDT	E	rh5-u3-x64-agent	CGP2606E: [SecFS, 0] [ALARM] Policy[test-policy] User[root,uid=0 (User Not Authenticated)] Process [/bin/touch] Action[create_file] Res[/vipdata/newfile] Effect[DENIED Code (1P,2P,3M)]

5.3 Apply user authentication

The user authentication attribute of a policy requires a little preparation. The reason being all user IDs of a system have a context of how the ID was assigned and whether the authentication of the ID can be trusted. For example an ID could have been assigned during login via SSH or at the command terminal. The ID could have not required any login and started by a daemon, such as the case of the instance owner of DB2.

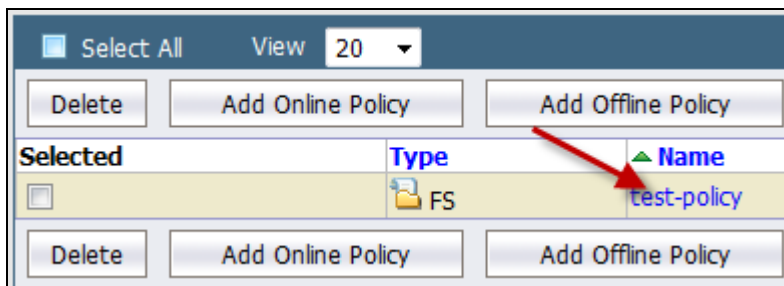
In this section, create a policy rule that allows root access to the data in vipdata only after using su to gain root ID context.

5.3.1 Alter test policy to add a rule for root

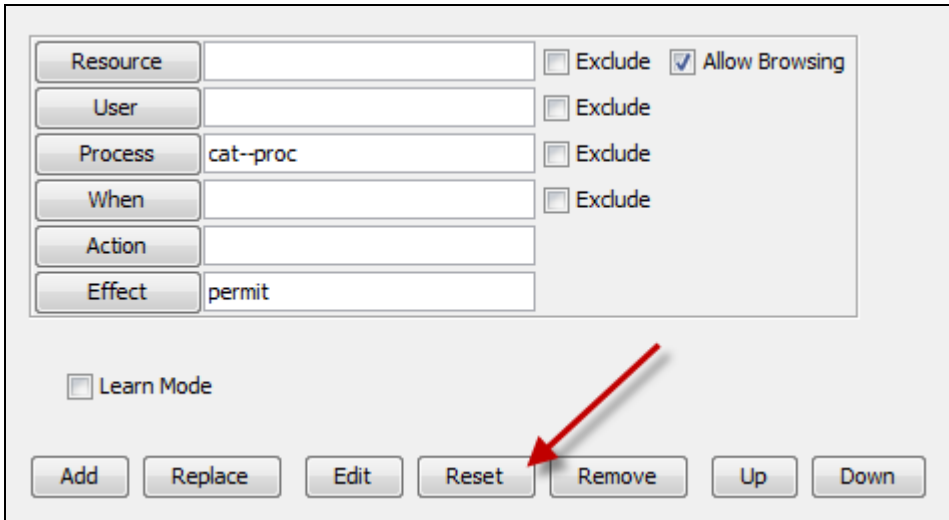
- __1. Click the **Policies** tab



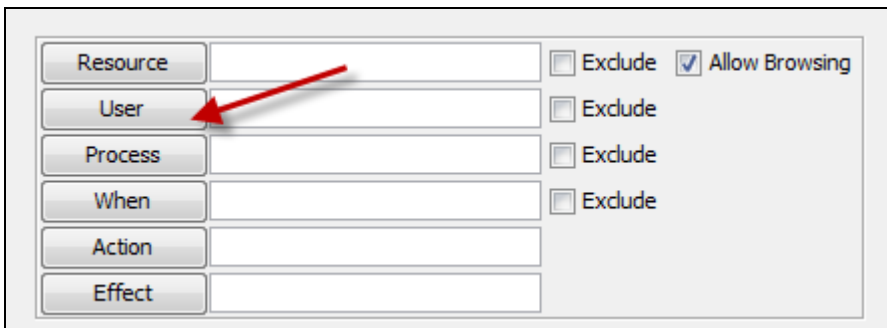
- __2. Click the **test-policy** to edit



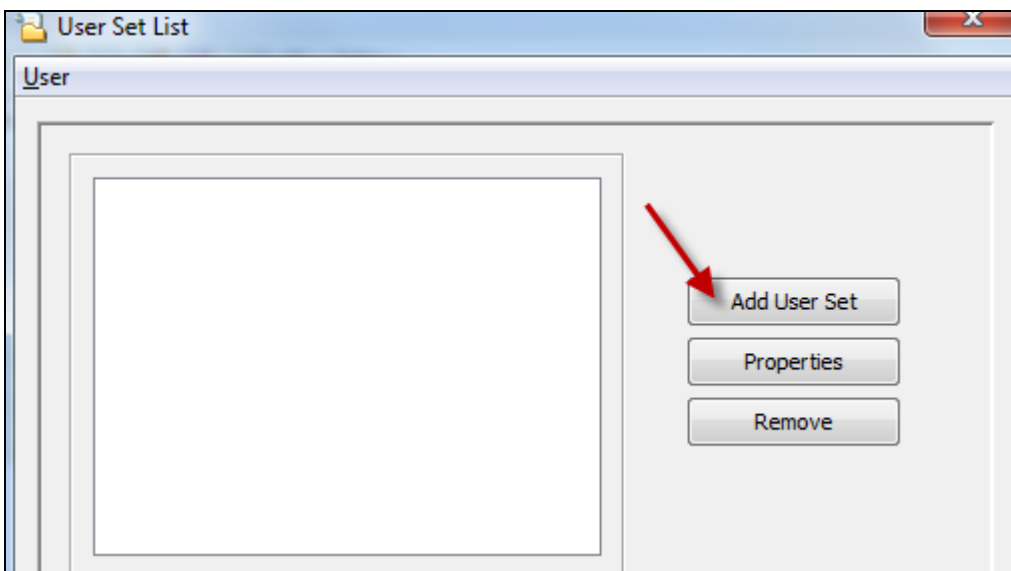
__3. Click the **Reset** button to reset the values of the rule editor



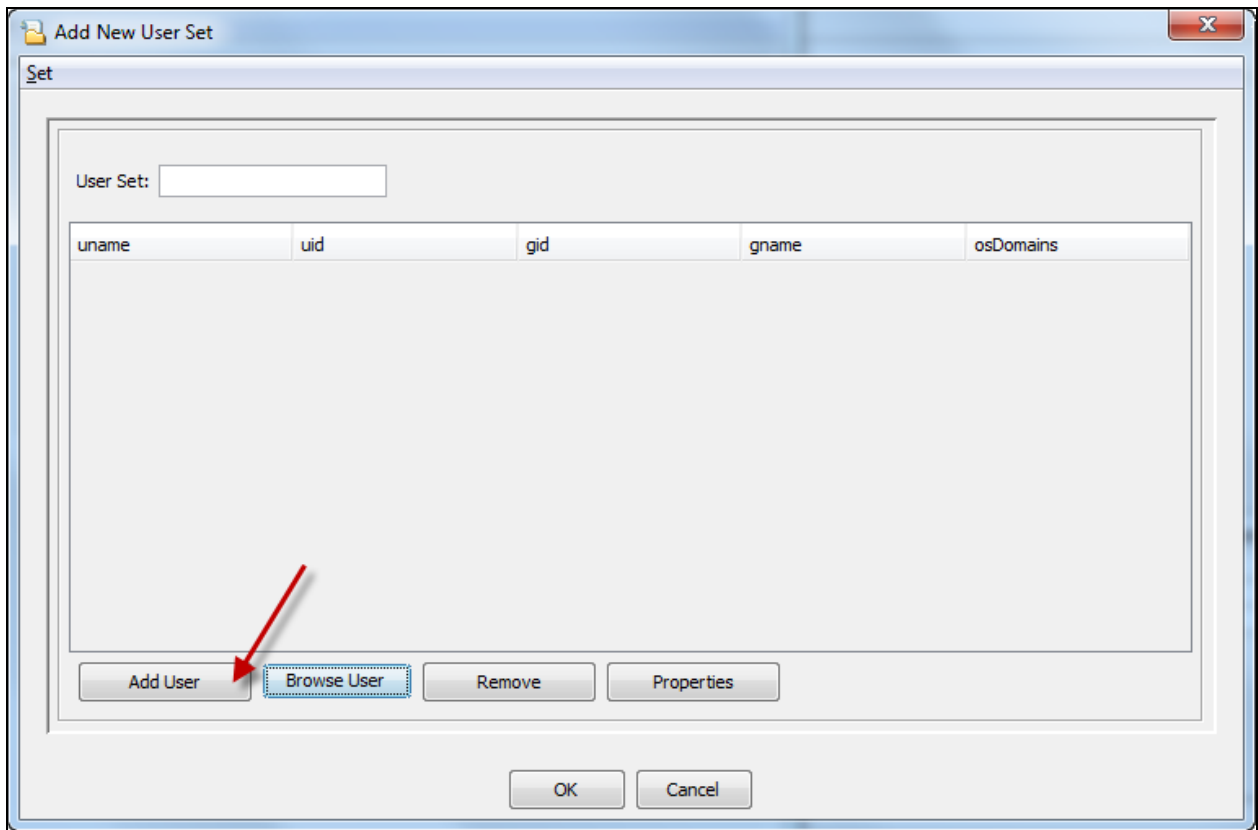
__4. Click the **User** attribute button



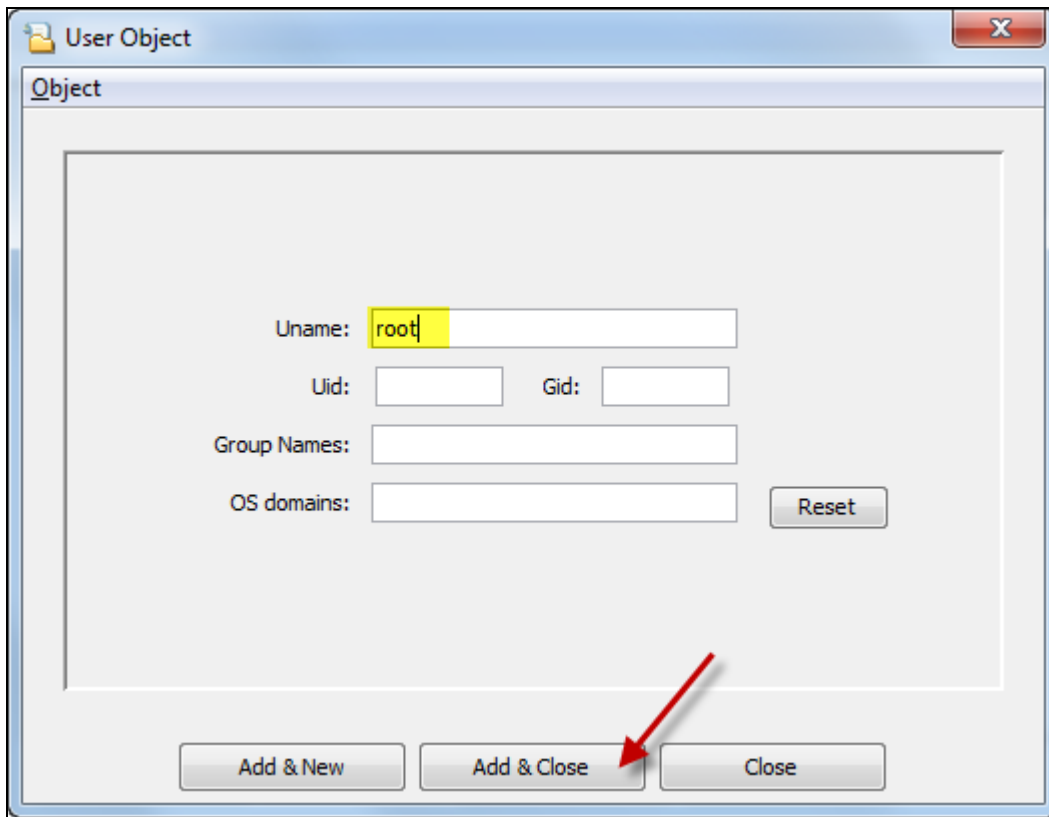
__5. Click the **Add User Set** button



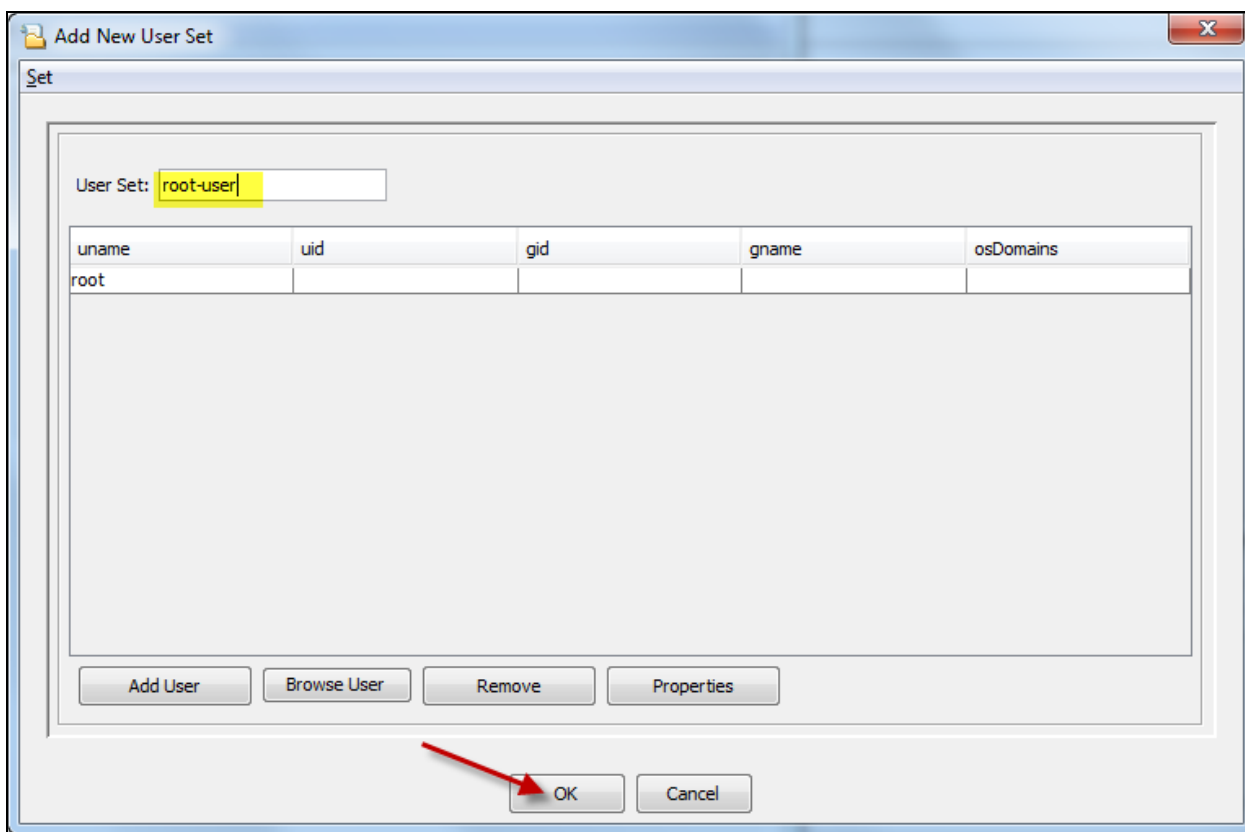
__6. Click the **Add User** button



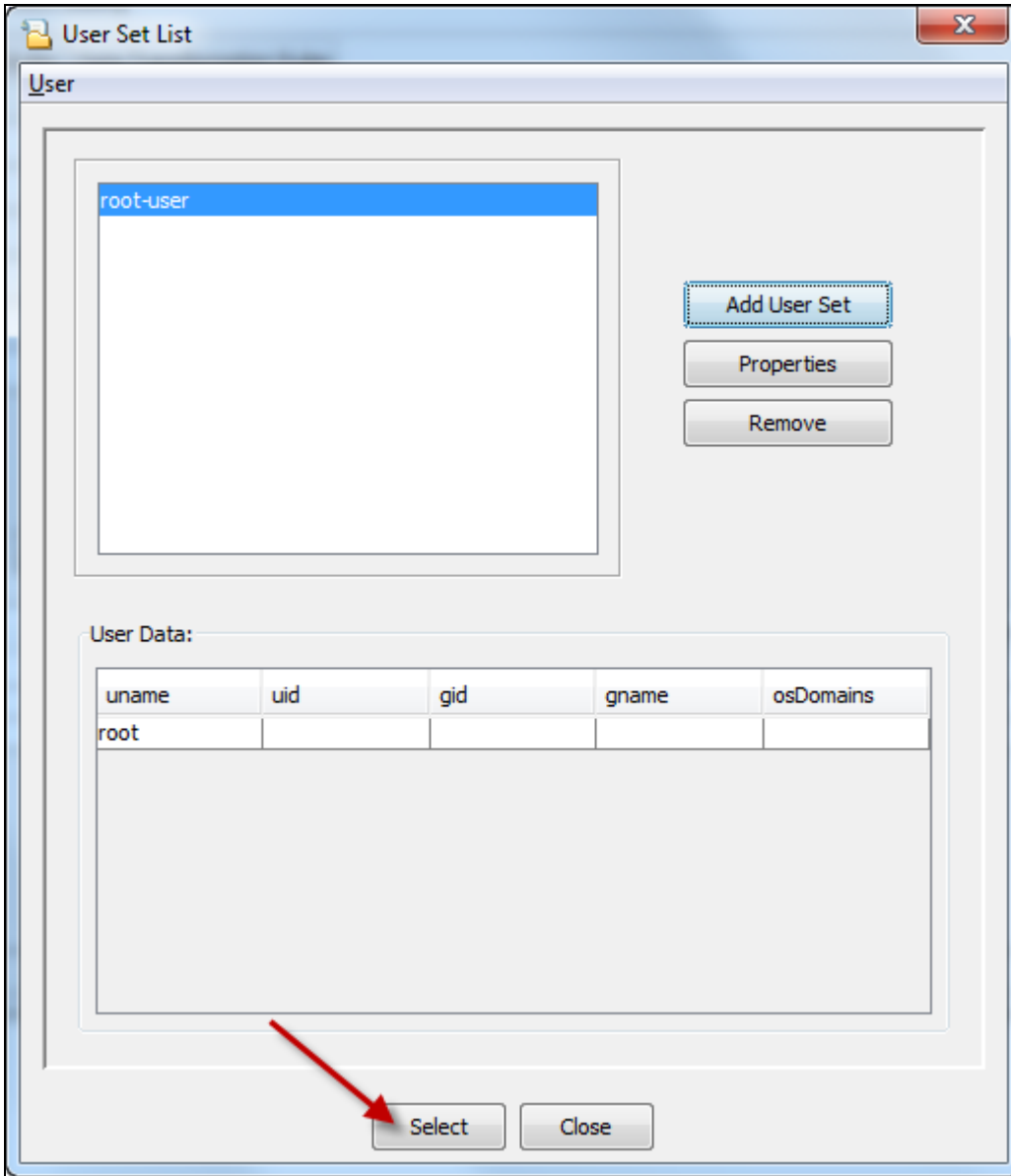
__7. Change the **Uname** value to **root** and click **Add & Close**



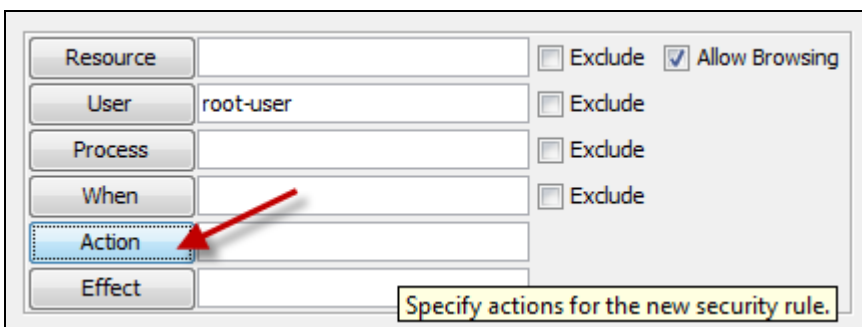
- __8. Change the **User Set** name to **root-user** and click the **OK** button



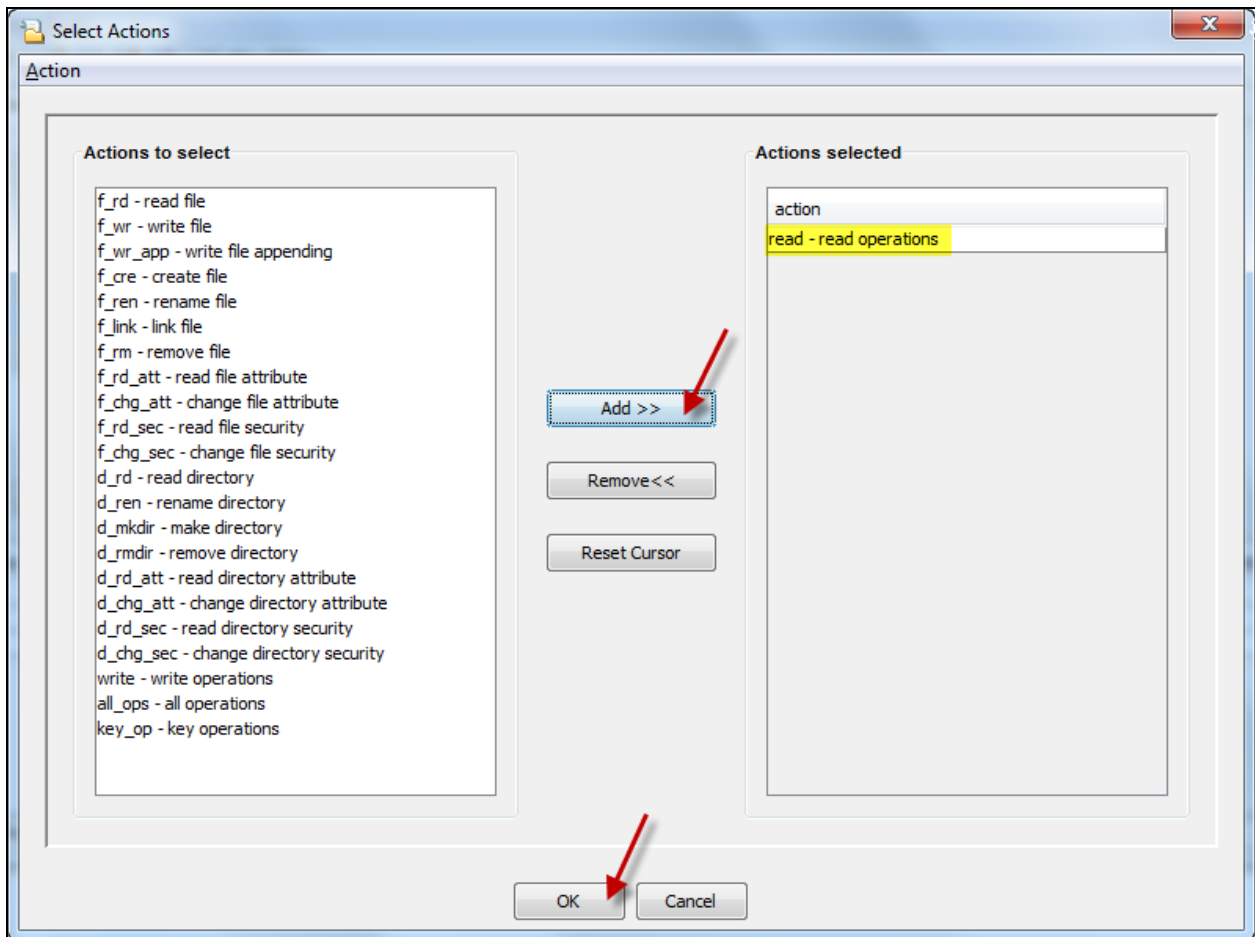
__9. Click the **Select** button



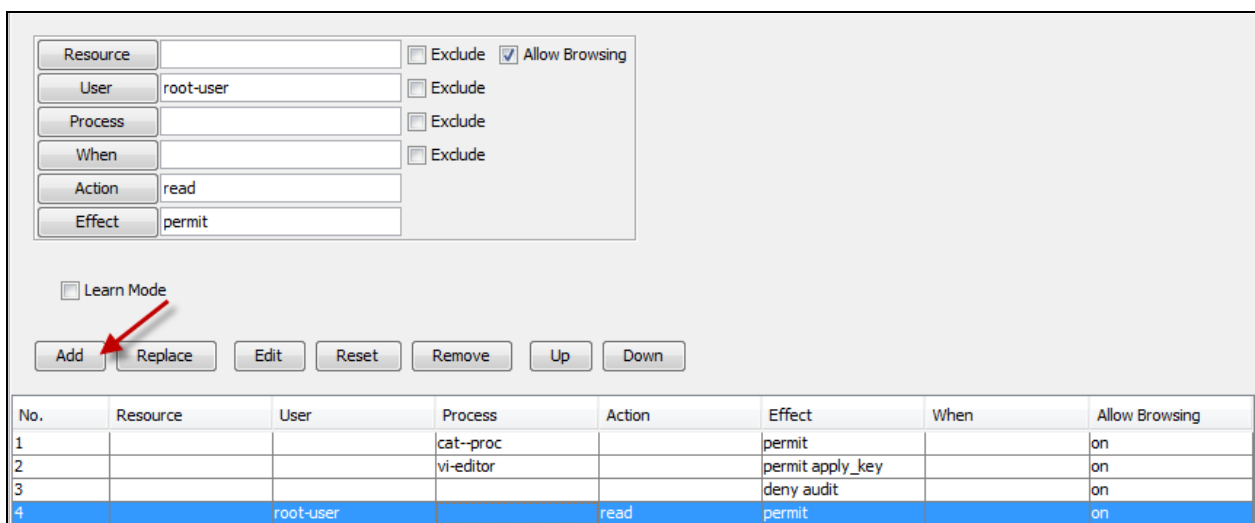
__10. Click the **Action** button



- __11. Select **read – read operations** and then click the **Add** button followed by the **OK** button




- __12. Change the **Effect** to permit
- __13. Click the **Add** button to add the new rule

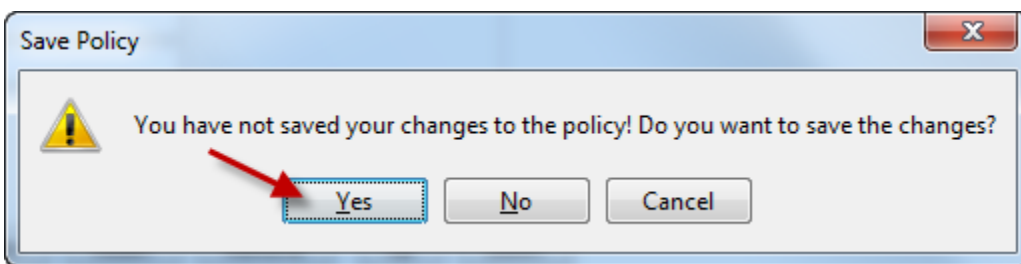


__14. Use the **Up** button to move the rule above the catch-all rule

<input type="button" value="Add"/> <input type="button" value="Replace"/> <input type="button" value="Edit"/> <input type="button" value="Reset"/> <input type="button" value="Remove"/> <input type="button" value="Up"/> <input type="button" value="Down"/>							
No.	Resource	User	Process	Action	Effect	When	Allow Browsing
1			cat-proc		permit		on
2			vi-editor		permit apply_key		on
3		root-user		read	permit		on
4					deny audit		on

The rule allows the root user to perform any read IO type using any process. However, only encrypted data will be returned because the rule lacks the **apply_key** effect.

__15. Click the  icon to exit policy editor, when prompted click the **Yes** button to save the policy and **OK** to confirm



5.3.2 Allow su to establish user attribute context

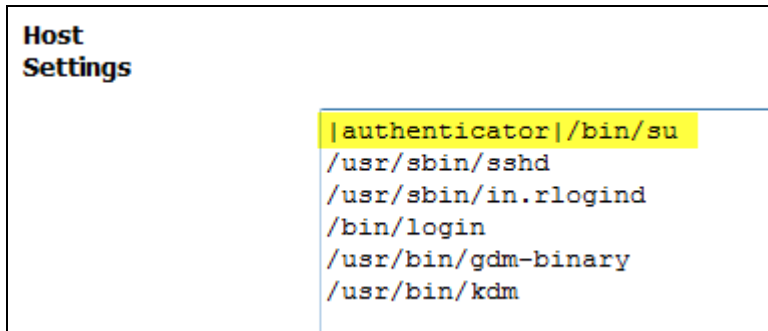
User authentication and management is a constant when dealing with data security. In this example the su utility will be the only process allowed to establish a user’s context that can be used in a user attribute of a policy. What this means is that a user can login to the system as root or another user but must use the su command to become root before the user attribute of the policy rule can be used.

- __1. Click the **Hosts** tab
- __2. Click the **rh5-u3-x64-agent** host
- __3. Click the **Host Settings** tab



The **Host Settings** already contain entries for some of the most common authenticating processes. To enable an entry a key word must be applied.

- __4. Apply the key word **authenticator** to **su** by editing the appropriate line, pretexting the entry with “[**authenticator**]”



- __5. Click the **Ok** button to enable the change

5.3.3 Test user authentication

- __1. As root, head the testfile

```
head /vipdata/testfile
```

The head utility reads the first few lines of a file. Access is denied as root does not have the right user context.

- __2. As root, cat the testfile

```
cat /vipdata/testfile
```

This works because cat is covered by a specific policy rule.

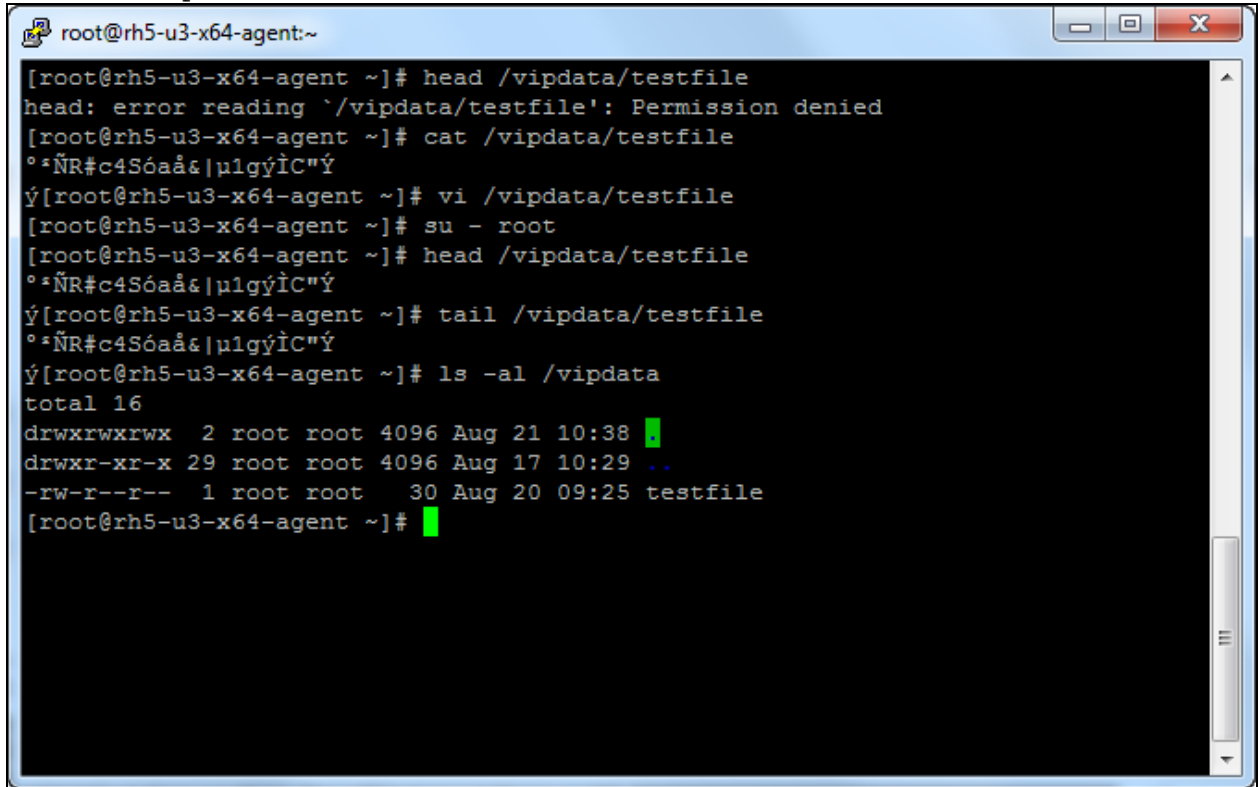
- __3. VI the file

```
vi /vipdata/testfile
```

This also works because the vi editor is covered by a specific policy rule

- __4. su to the root user and try some read operations

```
su - root  
head /vipdata/testfile  
tail /vipdata/testfile  
ls -al /vipdata
```

A terminal window titled 'root@rh5-u3-x64-agent:~' with standard window controls (minimize, maximize, close). The terminal shows the following sequence of commands and outputs:

```
[root@rh5-u3-x64-agent ~]# head /vipdata/testfile  
head: error reading `/vipdata/testfile': Permission denied  
[root@rh5-u3-x64-agent ~]# cat /vipdata/testfile  
°*ÑR#c4Sóaa&|u1gýÏC"Ý  
ý[ root@rh5-u3-x64-agent ~]# vi /vipdata/testfile  
[root@rh5-u3-x64-agent ~]# su - root  
[root@rh5-u3-x64-agent ~]# head /vipdata/testfile  
°*ÑR#c4Sóaa&|u1gýÏC"Ý  
ý[ root@rh5-u3-x64-agent ~]# tail /vipdata/testfile  
°*ÑR#c4Sóaa&|u1gýÏC"Ý  
ý[ root@rh5-u3-x64-agent ~]# ls -al /vipdata  
total 16  
drwxrwxrwx  2 root root 4096 Aug 21 10:38 .  
drwxr-xr-x 29 root root 4096 Aug 17 10:29 ..  
-rw-r--r--  1 root root   30 Aug 20 09:25 testfile  
[root@rh5-u3-x64-agent ~]#
```

Note root can now perform read-only related processes without the ability to access the data.

Lab 6 Encrypting DB2 data

Encrypting DB2 data starts with the creation of a policy. The policy should allow DB2 to interact with the encrypted data transparently while excluding any non-authorized IO access.

6.1 Create a DB2 policy

- __1. Click the **Policies** tab
- __2. Click the **Add Online Policy** button
- __3. Add the catch-all rule

No.	Resource	User	Process	Action	Effect	When	Allow Browsing
1					deny audit		on

- __4. Click the **Reset** button
- __5. Add a DB2 Process set
 - __a. Click the **Process** button
 - __b. Click the **Add Process Set** button
 - __c. Click the **Add Process** button
 - __d. Type in the following path into the **Directory** field, leave the **BaseName** field blank, click **Add & New** button

/home/db2inst1/sqllib/bin

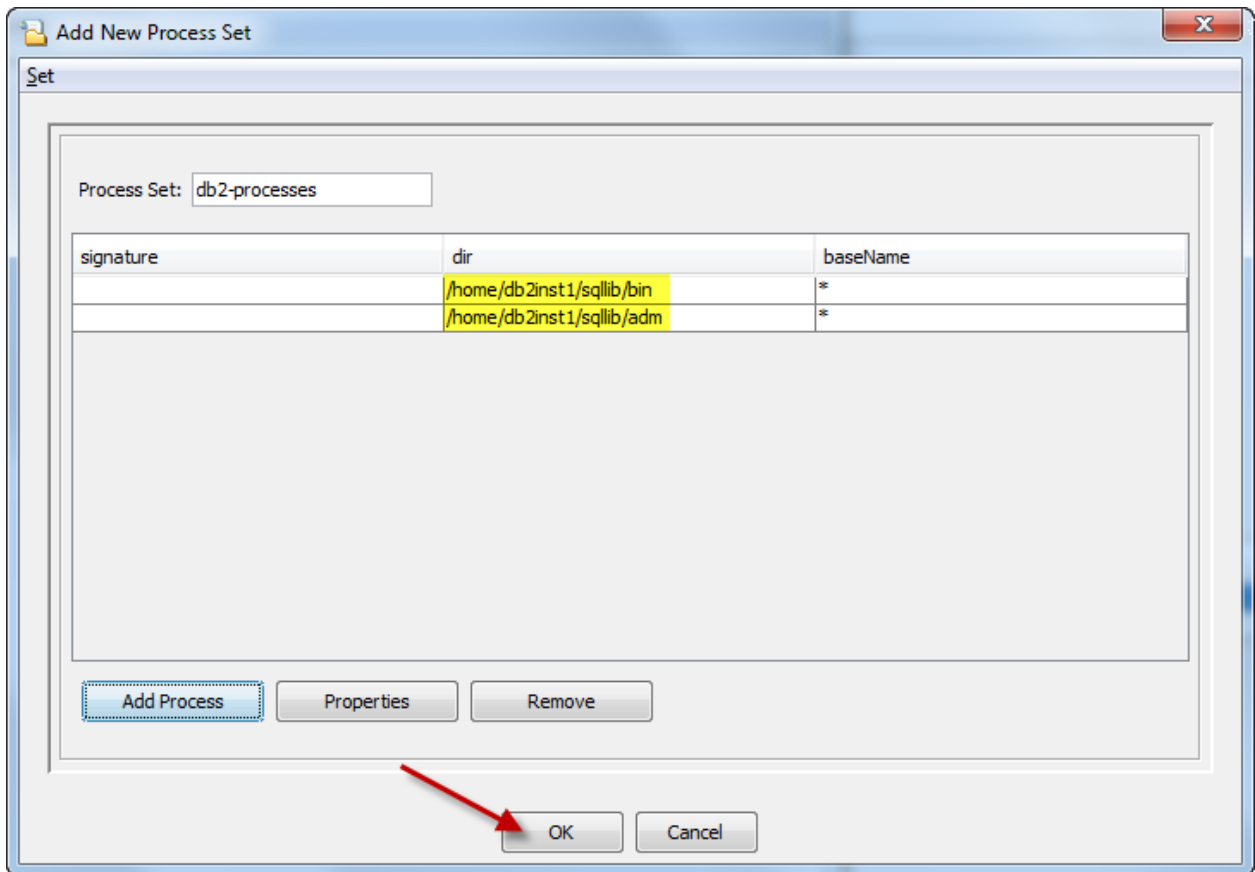
- __e. Type in the following path into the **Directory** field, leave the **BaseName** field blank, click **Add & Close** button

/home/db2inst1/sqllib/adm

The process set should look as follows:

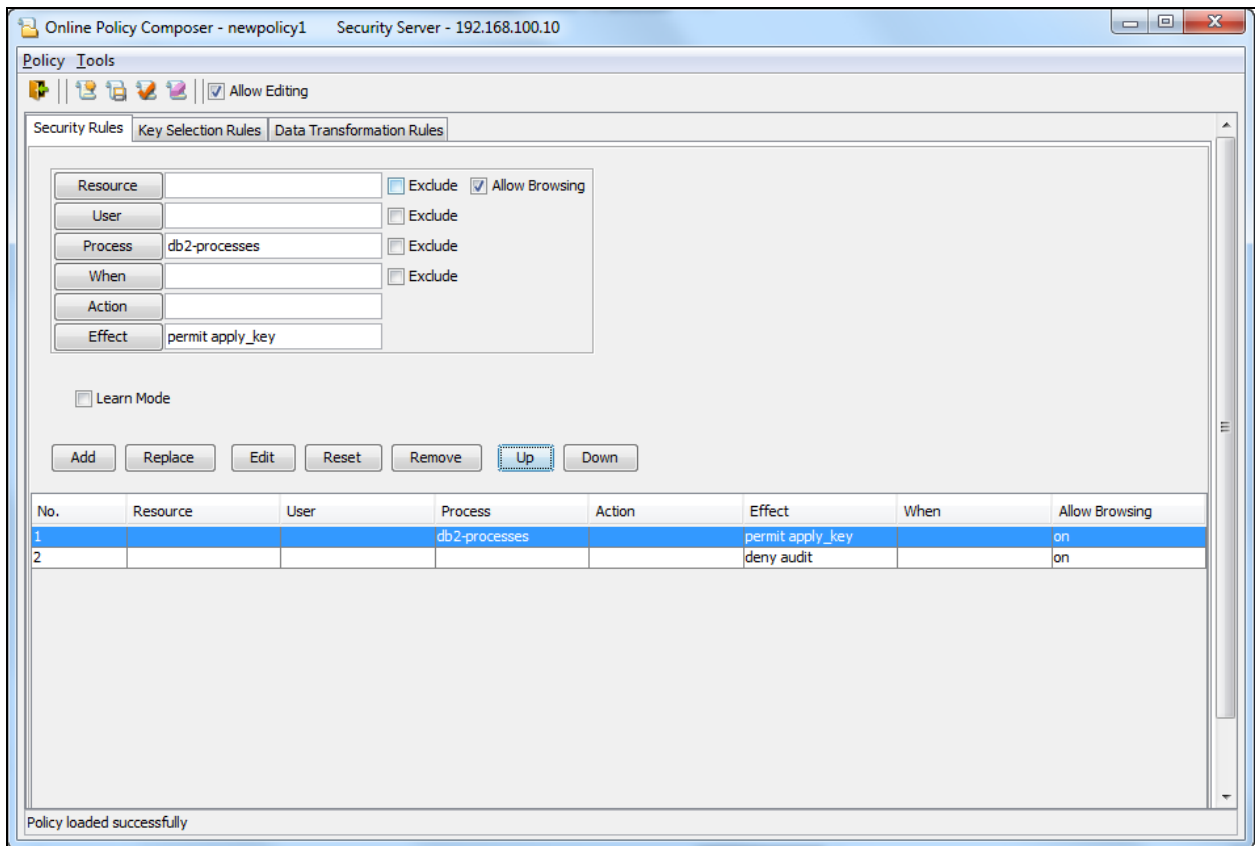
signature	dir	baseName
	/home/db2inst1/sqllib/bin	*
	/home/db2inst1/sqllib/adm	*

- __f. Add the **Process Set** name db2-processes and click the **OK** button

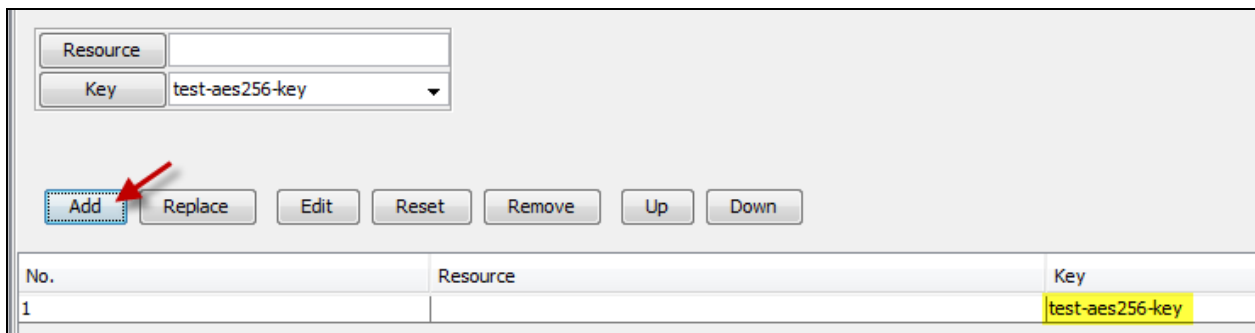



- __6. Click the **Select** button to add the db2-processes to the policy editor
- __7. Change the Effect to permit apply_key
- __8. Move the DB2 policy rule by clicking the **Up** button

The policy should look as follows:



- ___9. Click the Key Selection Rules tab
- ___10. Change the key to the **test-aes256-key** and click **Add**



- ___11. Click the  icon to save the policy
- ___12. When prompted to save the policy click **Yes**
- ___13. Change the policy name to **db2-policy** and click the **OK** button

6.2 Apply the db2-policy to a DB2 database

A DB2 sample database has already been created on /data. To encrypt a new DB2 database would simply mean applying the db2-policy to empty directories (guard points) and then creating the database on the guard points. There are two methods to encrypt an existing DB2 database, 1) using DB2 backup and restore or 2) using a data transformation utility. For the purpose of this exercise, backup and restore will be used.

6.2.1 Backup the existing DB2 database

- __1. As root, make a directory for the DB2 backup and make it read and writable

```
mkdir /backup
```

```
chmod 777 /backup
```

- __2. Apply the DB2 policy to /backup

As the DB2 backup file is created it will be encrypted by the file system encryptor

- __a. Click the **Hosts** tab
- __b. Click the **rh5-u3-x64-agent** host
- __c. Click the **Guard FS** tab
- __d. Click the **Guard** button
- __e. Add **/backup** to the **Path**, ensure that **db2-policy** is selected and click the **Ok** button

The Guard Points should look as follows:

Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Status
<input type="checkbox"/>	test-policy		/vipdata/		Directory (Auto Guard)	testdom	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	db2-policy		/backup/		Directory (Auto Guard)	testdom	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Guard Unguard Enable Disable Refresh

Page 1 of 1

- __3. su to the instance owner ID

```
su - db2inst1
```

- __4. Start DB2

```
db2start
```

__5. Run the DB2 backup command

```
db2 backup db sample to /backup
```

6.2.2 Demonstrate data access to the sample data

The strings command prints the displayable characters and is a easy way to see if a file is encrypted.

__1. Use the strings command to show data from the DB2 database

```
strings /data/db2inst1/NODE0000/SAMPLE/T0000002/C0000000.LRG |more
```

```
db2inst1@rh5-u3-x64-agent/data/db2inst1/NODE0000/SAMPLE/T0000002
SAMPLE
db2inst1
/home/db2inst1/db2inst1/NODE0000/SQL00001/
044:HD
778:RES
543:CWM
553:MJA
042:BF
J22"
BRANCH OFFICE J2
I22"
BRANCH OFFICE I2
H22"
BRANCH OFFICE H2
G22"
BRANCH OFFICE G2
F22"
BRANCH OFFICE F2
E21"
000100
SOFTWARE SUPPORT
E11"
[db2inst1@rh5-u3-x64-agent T0000002]$
```

Some of the data from the Department table is displayed.

__2. Display the same table from an SQL statement

```
db2 connect to sample
```

```
db2 "select * from department"
```

```

db2inst1@rh5-u3-x64-agent/data/db2inst1/NODE0000/SAMPLE/T0000002
48 record(s) selected.

[db2inst1@rh5-u3-x64-agent T0000002]$ db2 "select * from department"

DEPTNO DEPTNAME                                MGRNO  ADMRDEPT  LOCATION
-----
A00    SPIFFY COMPUTER SERVICE DIV.                000010  A00       -
B01    PLANNING                                     000020  A00       -
C01    INFORMATION CENTER                          000030  A00       -
D01    DEVELOPMENT CENTER                           -       A00       -
D11    MANUFACTURING SYSTEMS                       000060  D01       -
D21    ADMINISTRATION SYSTEMS                      000070  D01       -
E01    SUPPORT SERVICES                            000050  A00       -
E11    OPERATIONS                                   000090  E01       -
E21    SOFTWARE SUPPORT                             000100  E01       -
F22    BRANCH OFFICE F2                            -       E01       -
G22    BRANCH OFFICE G2                            -       E01       -
H22    BRANCH OFFICE H2                            -       E01       -
I22    BRANCH OFFICE I2                            -       E01       -
J22    BRANCH OFFICE J2                            -       E01       -

14 record(s) selected.

[db2inst1@rh5-u3-x64-agent T0000002]$ █

```

__3. Terminate the connection

```
db2 terminate
```

6.2.3 Encrypt the sample database

To start a guard point the agent needs exclusive access to the guard point directory. Applying a policy to a directory does not encrypt the contents of the directory. In the case of DB2 a database restore will write out the entire database encrypting the database during the restore.

__1. Drop the sample database

```
db2 drop db sample
```

The reason the drop is necessary is DB2 attempts to read the local database directory during a database restore if the database currently exists. Once we apply the policy db2-processes to the /data directory the local database directory will get mangled during this initial read. The local database directory is still clear text but when DB2 attempts to read the directory the db2-processes policy will apply the encryption key mangling the clear text data read. By dropping the DB2 database, this read is not attempted.

- __2. Apply the db2-policy policy to the /data directory
 - __a. Click the **Hosts** tab
 - __b. Click the **rh5-u3-x64-agent** host
 - __c. Click the **Guard FS** tab
 - __d. Click the **Guard** button
 - __e. Add **/data** to the **Path**, ensure that **db2-policy** is selected and click the **Ok** button

The Guard Points should look as follows:

Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Status
<input type="checkbox"/>	test-policy		/vipdata/		Directory (Auto Guard)	testdom	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	db2-policy		/backup/		Directory (Auto Guard)	testdom	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	db2-policy		/data/		Directory (Auto Guard)	testdom	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

- __3. Perform the database restore

```
db2 restore db sample from /backup
```

The database is now encrypted. And no access is allowed to the DB2 data files unless they are the DB2 processes

6.2.4 Attempt to circumvent the policy

- __1. Use strings to access the department data

```
strings /data/db2inst1/NODE0000/SAMPLE/T0000002/C0000000.LRG |more
```

Data access is denied and therefore string does not return any data. Cat and VI could also be attempted.

- __2. Display the table from an SQL statement

```
db2 connect to sample
```

```
db2 "select * from department"
```

Lab 7 Encrypting DB2 backups

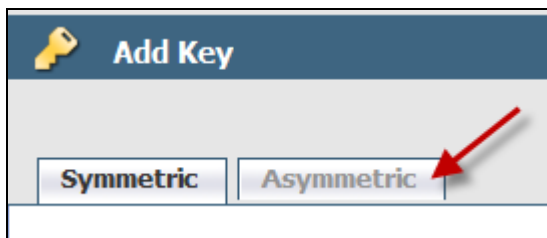
There are two ways to encrypt DB2 backups. One is to use the file system encryptor as performed in a previous lab exercise. The backup file can then be copied off to tape or other media without unencrypting the backup file. To restore the backup would require copying the file back to an encrypted file system that uses the same key of the encrypted file. The restore could be performed without any other options.

The second method to create an encrypted backup is to use the DB2 encryption backup/offline agent. The output of this method is a backup file that contains an encrypted copy of the database.

7.1.1 Create a backup key pair

The DB2 backup is encrypted with a symmetric key that is generated uniquely for each invocation of the backup. This symmetric key is protected by a public/private key pair. The key and public key is transmitted to the agent using the certificate encryption already in place. At the host the backup file is created using the symmetric key the symmetric key is then encrypted with the public key and placed in the header of the backup file as well as the public key. The symmetric key is then discarded and the only copy that remains is the encrypted version within the header. The only way to restore that key and therefore the backup is with the private key that retained at the EE Server.

- __1. Click the **Keys** tab
- __2. Click the **Add** button
- __3. Click the **Asymmetric** tab



__4. Change the **Name** and **Description** as follows and the **Ok** button:

Name = db2-backup

Description = DB2 RSA1024 backup

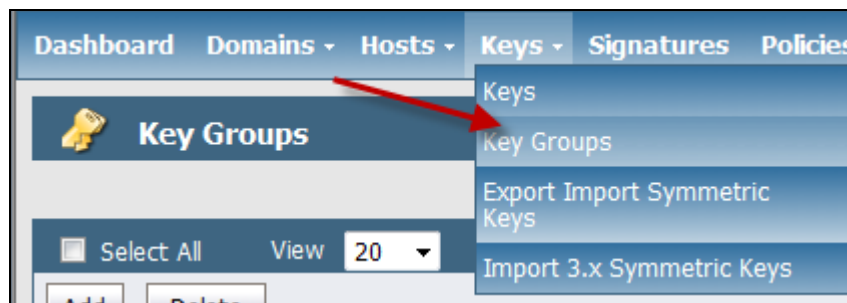
The screenshot shows a dialog box with two tabs: 'Symmetric' and 'Asymmetric'. The 'Asymmetric' tab is selected. The fields are as follows:

- *Name: db2-backup
- Description: DB2 RSA1024 backup
- Key Type: Key Pair
- Algorithm: RSA1024

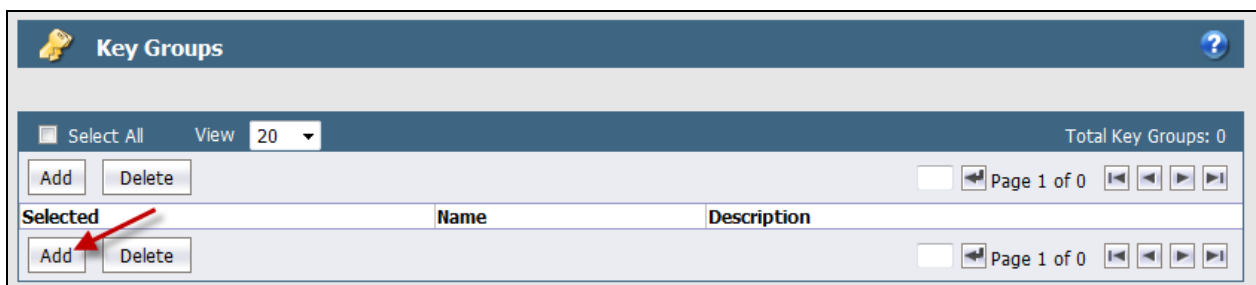
At the bottom right, there are 'Ok' and 'Cancel' buttons. A red arrow points to the 'Ok' button.

__5. Add a Key Group

__a. Click **Keys > Key Groups** tab



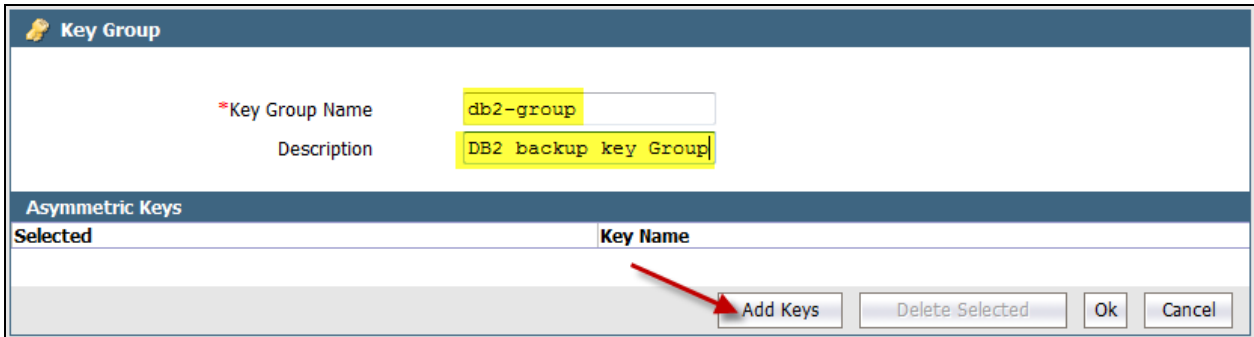
__b. Click the **Add** button



- __c. Change the **Key Group Name** and **Description** as follows and click the **Add Keys** button

Key Group Name = db2-group

Description = DB2 backup key group



- __d. Check the **db2-backup** key and click **Add Selected Keys to Group**



- __e. Click the **Ok** button to commit changes

7.1.2 Create a backup/offline policy

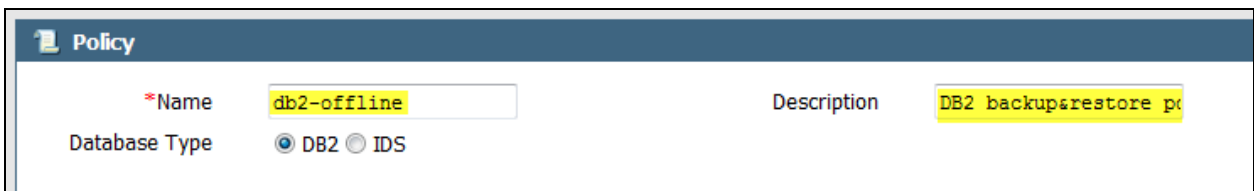
- __1. Click the **Policies** tab
- __2. Click the **Add Offline Policy** button

An offline policy governs the backup and restore of encrypted database backups.

- __3. Change the Policy **Name** and **Description**:

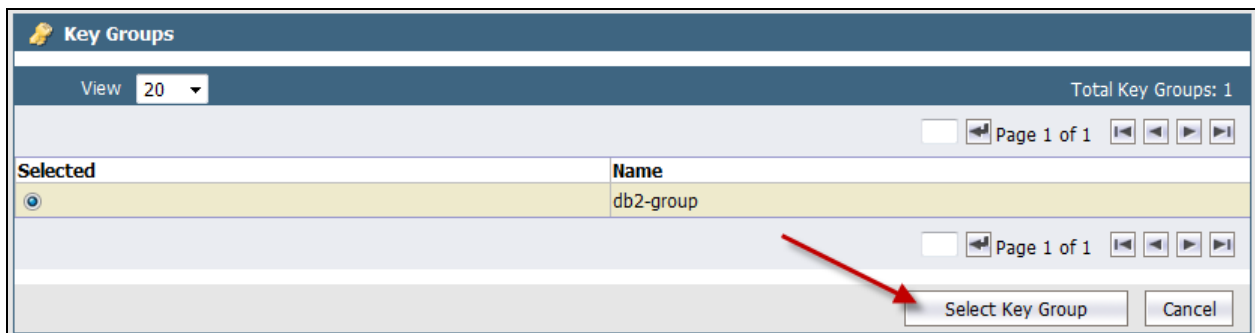
Name = db2-offline

Description = DB2 backup&restore policy

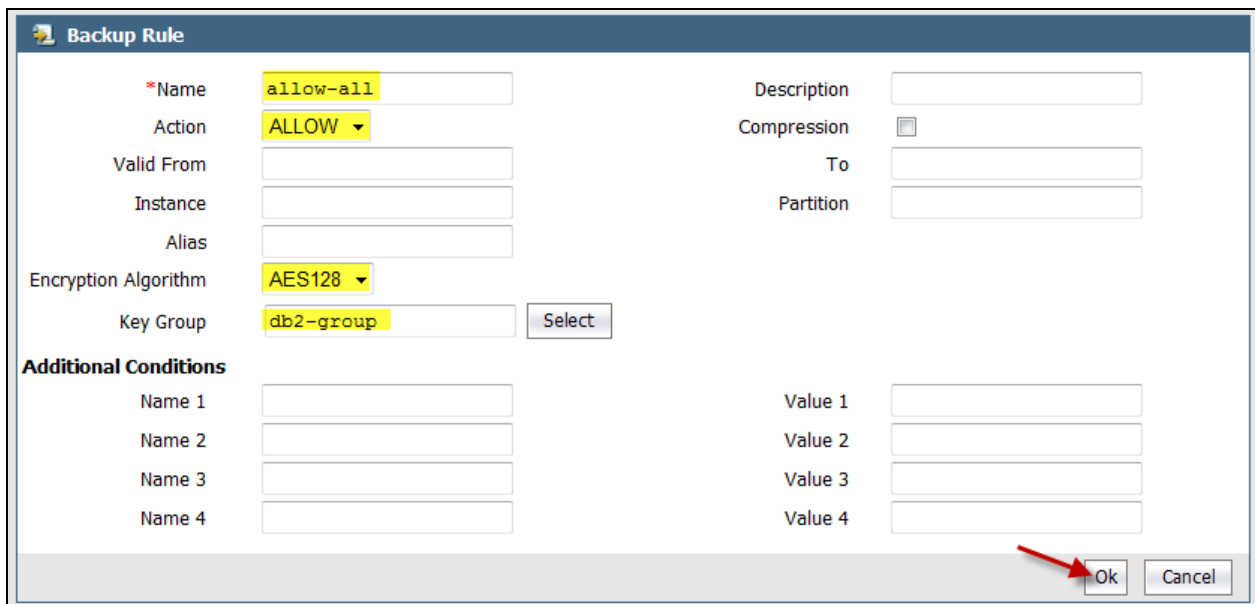


- __4. Add backup rule

- __a. Click the **Add** button in the **Backup Rules** section
- __b. Change the **Name** to **allow-all**
- __c. Change the **Action** to **Allow**
- __d. Change the Encryption Algorithm to **AES128**
- __e. Click the **Select** button
- __f. Mark the **db2-group** radio button and click the **Select Key Group** button



- __g. Click the **Ok** butt to complete the definition of the backup rule



- __5. Add restore rule
 - __a. Click the **Add** button in the **Restore Rules** section
 - __b. Change the **Name** to **allow-restore**
 - __c. Change the **Action** to **Allow**

__d. Click the **Ok** button to create the restore rule

Restore Rule

*Name: allow-restore Description:

Action: ALLOW

Valid From: To:

Instance: Partition:

Alias:

Ok Cancel

__6. Complete the definition of the offline policy by clicking the **Ok** button

Policy

*Name: db2-offline Description: DB2 backup&restore po

Database Type: DB2 IDS

Backup Rules

Select All View: 20 Total: 1

Add Delete Up Down Page 1 of 1

Selected	Name	Compression	Encryption	From	To	Action	Description
<input type="checkbox"/>	allow-all	<input type="checkbox"/>	AES128			ALLOW	

Page 1 of 1

Restore Rules

Select All View: 10 Total: 1

Add Delete Up Down Page 1 of 1

Selected	Name	From	To	Action	Description
<input type="checkbox"/>	allow-restore			ALLOW	

Page 1 of 1

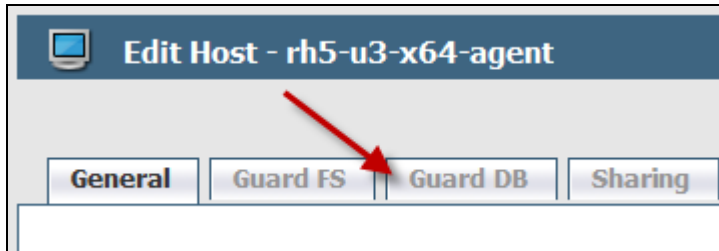
Ok Cancel

7.1.3 Apply the offline policy to rh5-u3-x64-agent

Once the offline policy is defined it needs to be applied to a host so that backup requests can be governed by the policy.

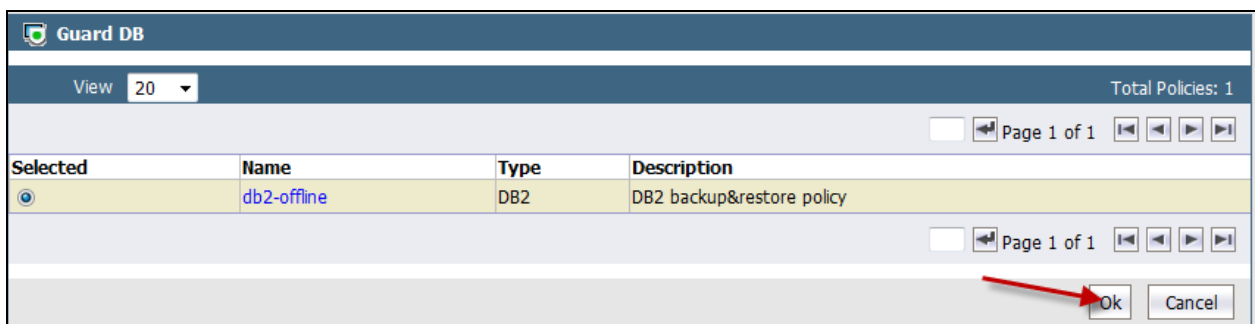
- __1. Click the **Hosts** tab
- __2. Click the **rh5-u3-x64-agent** host

- __3. Click the **Guard DB** tab



- __4. Click the **Guard** button

- __5. Mark the **db2-offline** radio button and click the **Ok** button



7.1.4 Perform and encrypted backup

To create an encrypted backup is simply at matter of including some extra options on the backup command to load and use the backup encryption agent. The agent will do all the work of obtaining the key and encrypting the backup as it is created. To load the agent the "compress complib" is overloaded to use the encryption agent rather than a separate compression library.

- __1. As root, make a directory to hold the database backup

```
mkdir /db2back
```

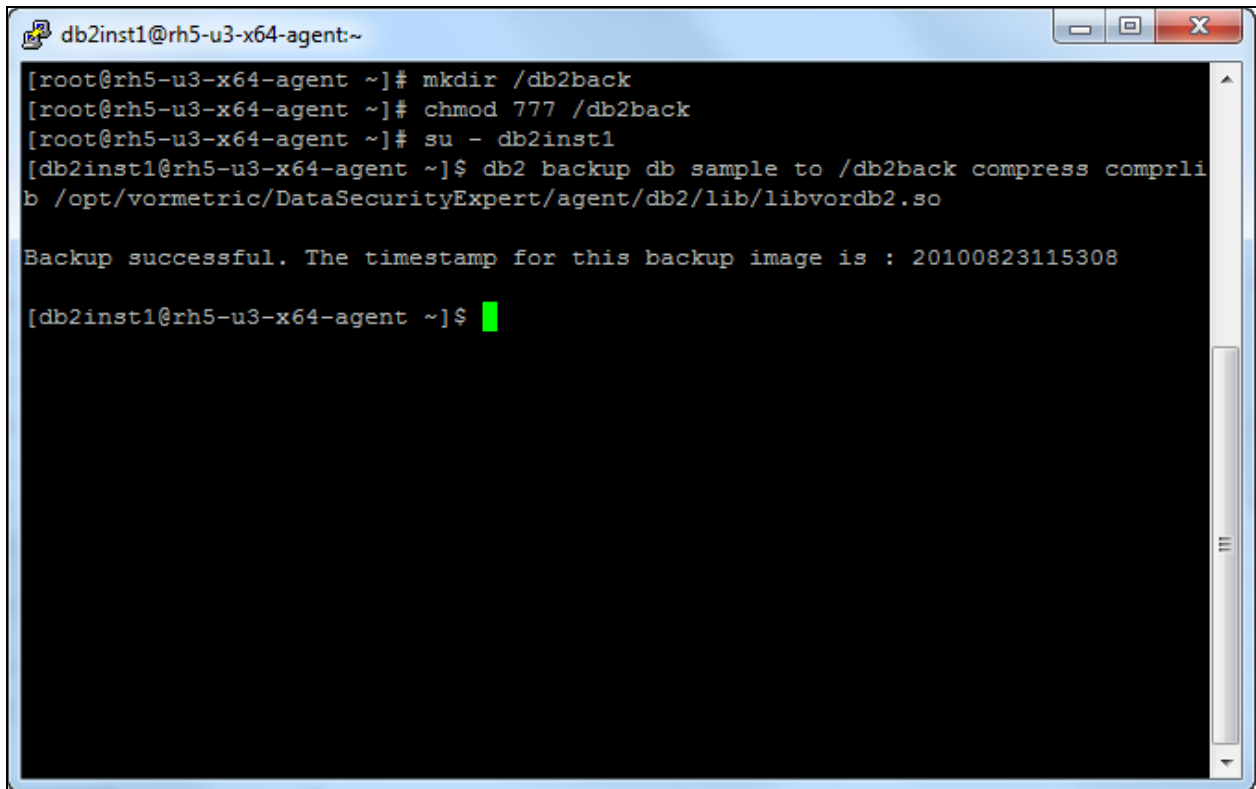
- __2. Ensure the directory is read and writable to DB2

```
chmod 777 /db2back
```

- __3. As db2inst1, encrypt a backup of the sample database

```
su - db2inst1
```

```
db2 backup db sample to /db2back compress comprlib  
/opt/vormetric/DataSecurityExpert/agent/db2/lib/libvordb2.so
```

A terminal window titled "db2inst1@rh5-u3-x64-agent:~" with standard window controls (minimize, maximize, close) in the top right. The terminal shows a sequence of commands: "mkdir /db2back", "chmod 777 /db2back", and "su - db2inst1". The main command is "db2 backup db sample to /db2back compress comprlib /opt/vormetric/DataSecurityExpert/agent/db2/lib/libvordb2.so". The output is "Backup successful. The timestamp for this backup image is : 20100823115308". The prompt returns to "db2inst1@rh5-u3-x64-agent ~]\$".

```
db2inst1@rh5-u3-x64-agent:~  
[root@rh5-u3-x64-agent ~]# mkdir /db2back  
[root@rh5-u3-x64-agent ~]# chmod 777 /db2back  
[root@rh5-u3-x64-agent ~]# su - db2inst1  
[db2inst1@rh5-u3-x64-agent ~]$ db2 backup db sample to /db2back compress comprlib  
/opt/vormetric/DataSecurityExpert/agent/db2/lib/libvordb2.so  
  
Backup successful. The timestamp for this backup image is : 20100823115308  
  
[db2inst1@rh5-u3-x64-agent ~]$
```

Appendix A. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have

been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental. All references to fictitious companies or individuals are used for illustration purposes only.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Appendix B. Trademarks and copyrights

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	AIX	CICS	ClearCase	ClearQuest	Cloudscape
Cube Views	DB2	developerWorks	DRDA	IMS	IMS/ESA
Informix	Lotus	Lotus Workflow	MQSeries	OmniFind	
Rational	Redbooks	Red Brick	RequisitePro	System i	
System z	Tivoli	WebSphere	Workplace	System p	

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. See Java Guidelines

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

ITIL is a registered trademark and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Other company, product and service names may be trademarks or service marks of others.



© Copyright IBM Corporation 2010.

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Other company, product and service names may be trademarks or service marks of others.



Please Recycle
