Google Rapid Response (GRR)


```
Created By: CTN3 Farr, Collin
93 Cyber Protection Team
collin.m.farr2.mil@mail.mil
```


GRR Rapid Response is an incident response framework focused on remote live forensics. It consists of a python client (agent) that is installed on target systems, and python server infrastructure that can manage and talk to clients. The goal of GRR is to support forensics and investigations in a fast, scalable manner to allow analysts to quickly triage attacks and perform analysis remotely.

Creating GRR From Install:

Installing OS (Red Hat Enterprise Linux *Version - 6.9 &* <)

1. Download the RHEL v.X.x Binary DVD From: `https://access.redhat.com/downloads/content/69/ver=/rhel--7/7.5/x86_64/product-software`

2. Create a new virtual machine (VM) template with desired virtualization software using Binary DVD.iso

- Be sure to allocate enough resources for GRR depending on size of desired deployment (i.e. if deploying to 20+ endpoint hosts be sure to make the hard drive space large enough to be able to store all hunts).

1. Once the VM is booted a few configuration changes need to be made:

   i. `Date/Time` should be set to Coordinated Universal Time (UTC).

   ii. Under the `Installation Source` section:
   Verify the media the install is coming from.

   - Be sure the media is selected before continuing.
   i. Under “Software Selection”:
   - “Minimal Install” should be selected along with the add-ons “Development Tools” and “Compatible Libraries”.

   i. Verify “Installation Location” is correct. (It should be the virtual disk from the creation of the VM.

   ii. Under “Network & Hostname” check to be sure the ethernet interface is present. These settings will be configured later.

   iii. Hit Next to start the install of the operating system.

   - Be sure to verify that the root account password is set.

Configuring Red Hat For GRR

1. Determine the name of the network interface for the VM (usually along the lines of eth0 or ens33)
   #ip addr

2. Configure the configuration file for that interface.
   #vi /etc/sysconfig/network-scripts/ifcfg-

3. The following configurations should replace what is already in the config file.
   DEVICE=
   BOOTPROTO= |none , static|
   ONBOOT=yes

PREFIX=24
IPADDR=
NETWORK=
NETMASK=<255.255.255.0>
GATEWAY=

4. Save this file and exit vi
   :wq!

5. Using ifdown and ifup restart the interface.
   #ifdown
   #ifup

6. Edit Resolv.conf file to add nameservers.
   #vi /etc/resolv.conf

7. Add the following to the configuration file
   nameserver 8.8.8.8
   nameserver 8.8.4.4

8. Check for network connectivity by pinging the default gateway and then external network

   - *NOTE* To check for external network connectivity pinging Google's DNS is always a safe option. (8.8.8.8)

9. Configure RHEL to utilize repositories.

   i. Register The RHEL Instance.
      #subscription-manager register
      User: dmss.devops
      Password:
   ii. Download and configure the Epel-repo.
      #rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
      # yum update

10. Configure the firewall to allow HTTP connections to the VM.

    i. Check to see if firewalld is running using
       #firewall-cmd --state
    ii. Once verified the firewall is running check the allowed services for "HTTP"
       #firewall-cmd --get-services | grep http
    iii. If http is not allowed add to list of services and make persistent using using:
       #firewall-cmd --add-service=http
       #firewall-cmd --runtime-to-permanent
    iv. If http is allowed continue.
    v. Add the GRR web interface ports to allowed ports list.
       # firewall-cmd --add-port=8000/tcp
       # firewall-cmd --add-port=8080/tcp
       # firewall-cmd --runtime-to-permanent

Installing GRR (using pip).

1. Using Yum install the needed dependencies:
   # yum install -y epel-release python-devel wget which libffi-devel
   openssl-devel zip git gcc gcc-c++ redhat-rpm-config

```
# yum install -y python-pip
```

2. Using pip install grr-response-server:
   # pip install grr-response-server

Configuring GRR.

1. Create the initial GRR configuration file # grr_config_updater initialize
   - The RSA Keys w ill automatically generate for GRRs configurations.
2. Choosing a(n) SQL version.
   #1
3. Configure the Datastore Location. (The default is fine but is able to be changed)
4. If using a unique hostname, enter that next.
5. Frontend and Admin UI server URL. If using DNS to reach back to the GRR Server, add that domain here otherw ise use the static ip that is set:
   http://x.x.x.x:8080/ (Front End)
   http://x.x.x.x:8000/ (Admin UI)
6. If using a mail server to receive GRR alerts correctly input that information here
7. Rekall is no longer supported, do not enable it.
   #n
8. Adding The Admin user. (Set the admin users passw ord)

9. Dow nload Client Templates.
   #Y
10. Repack the Client Templates.
    #Y

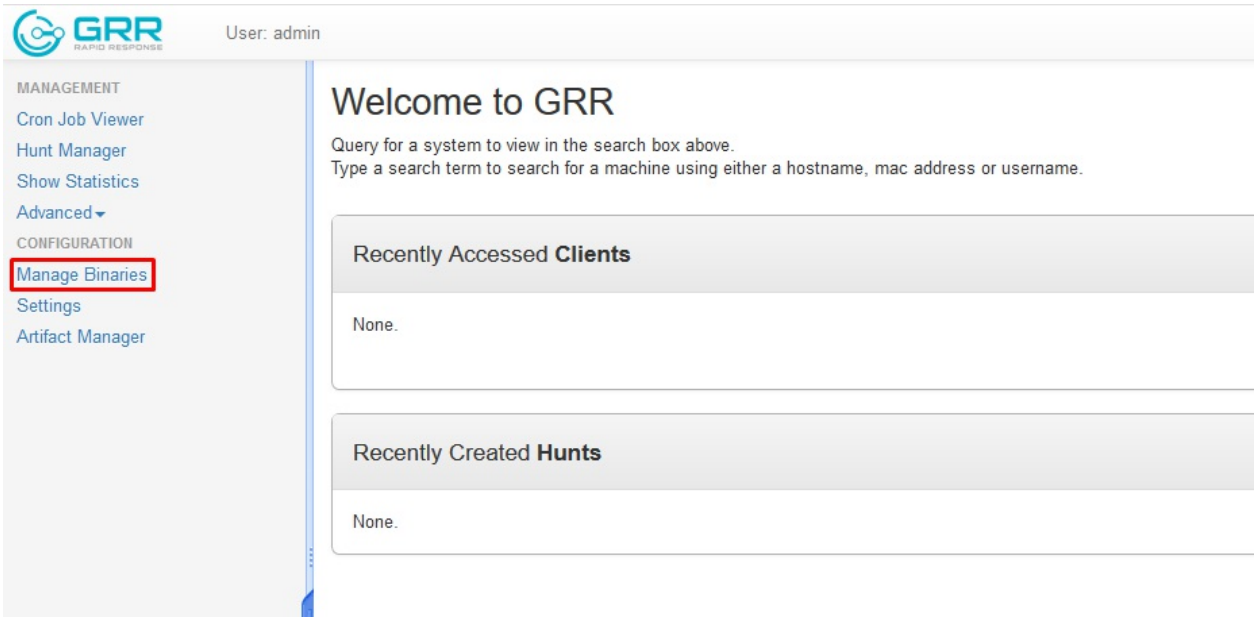
Starting GRR to a Running State.

1. Using the commands added by GRR deploy the individual services.
   - Using the '&' w ill run the command in the background
     #grr_admin_ui &
     #grr_w orker &
     #grr_frontend &
2. Attempt to connect to the UI from a host w ithin the netw ork using the set addresses in the configuration file. If Attempted connection fails:
   i. Attempt to Ping the GRR server to verify traffic gets to the destination.
   ii. Double check the IP address of the Server against w hat is in the configuration.
   iii. Attempt to Ping from the GRR Server out into the host team internal netw ork.
   iv. Double check that all firew alld rules and implementations have been set correctly.

Deploying GRR Agents.

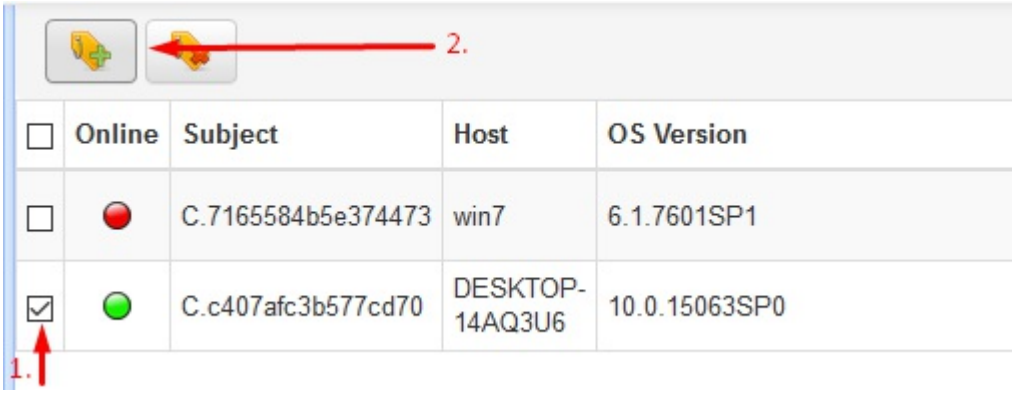
```
For Windows Operating systems (Psexec):
```

1. Determine w hether the hosts are 32 or 64 bit operating systems
2. Dow nload the respective agent from the w eb ui.
   i. Under the configuration section select 'Manage Binaries'



2. Select the agent which fits your operating system

3. Create an IP list containing all the hosts you wish to deploy the GRR agent to.
4. Using psexec deploy the agents #psexec @ -u -p -c -f -s
   - NOTE: For an install without feedback from the agent use the '-d' flag.
   - When using psexec, if the executable is not within the Command line environmental path an absolute path or browsing to the containing directory will be required.
   - A successful install will return an exit code of 0.
5. After successful deployment, be sure to add label to active hosts with a description of what they are.
   - Users, Services, SCADA, Etc.



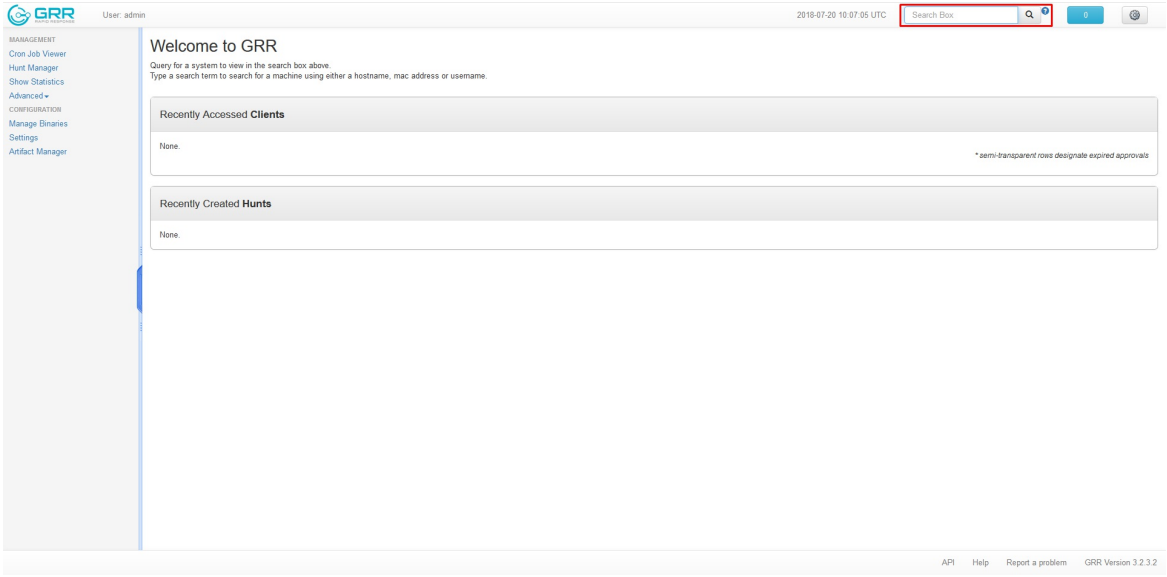
Online	Subject	Host	OS Version	MAC	Usernames	First Seen	Client version	Labels
	C.7165584b5e374473	win7	6.1.7601SP1	00:0c:29:be:76:fd 00:0c:29:be:76:f3	user	2018-07-20 10:19:37 UTC	3232	
	C.c407afc3b577cd70	DESKTOP-14AQ3U6	10.0.15063SP0	00:0c:29:4b:a8:a1 4c:bb:58:ee:e1:39	xadmin	2018-07-22 00:43:40 UTC	3232	Users

`For Linux Operating Systems`

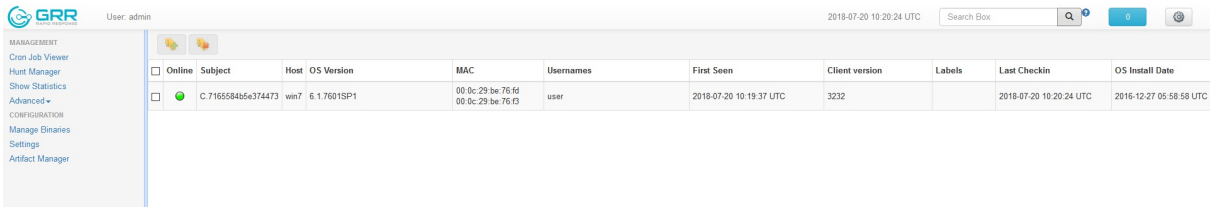
COMING SOON

Verify Agent communication with Server.

1. Using the GRR web ui, use the search bar at the top of the page.
   i. Leave search bar blank

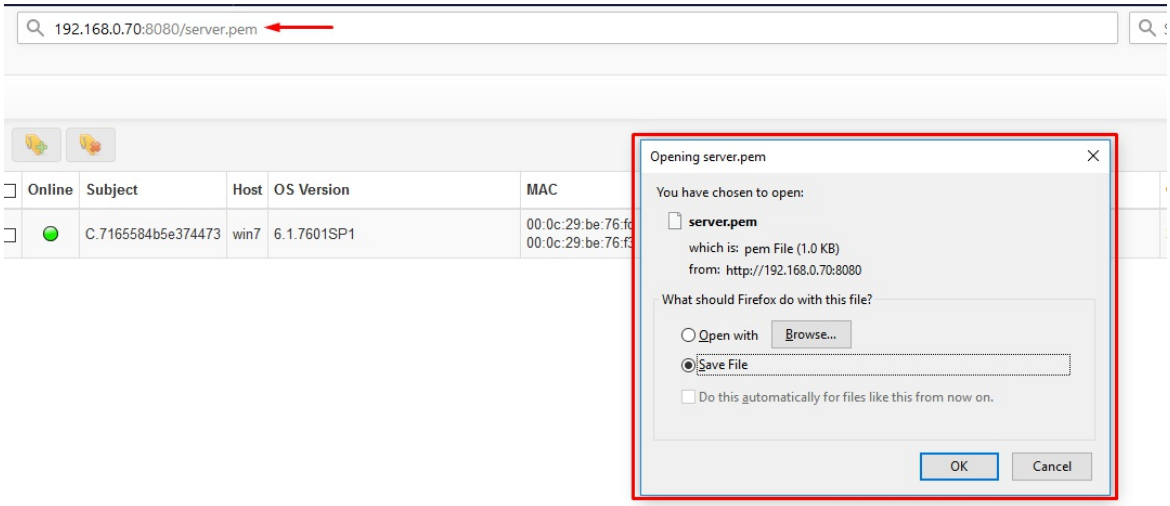


   ii. Press Enter
2. The Hosts communicating with the GRR server will be displayed in a list on this page.



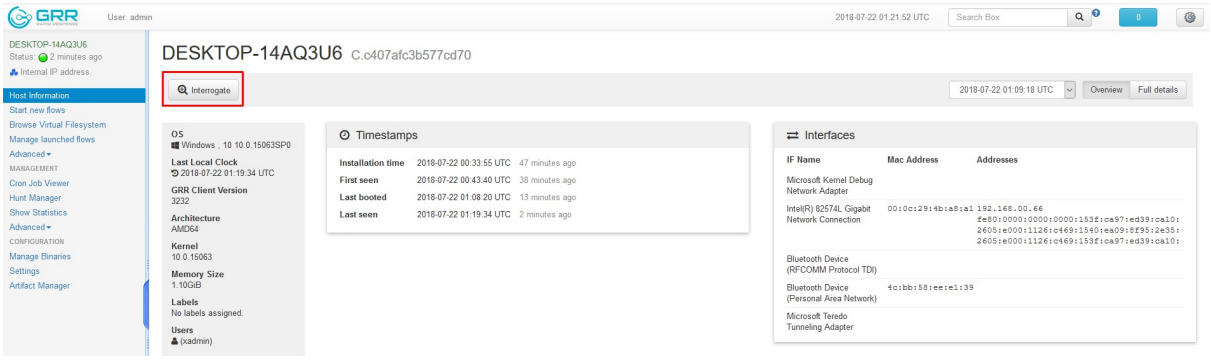
3. If a host is not communicating as expected, use ping to determine if the host is active or not.

   - Determine point of failure if host is active but not calling back to the GRR server.
     - verify the GRRservice.exe is running in `tasklist` or `task manager`.
   - Can the host communicate with the frontend interface of grr using `http://x.x.x.x:8080/server.pem`

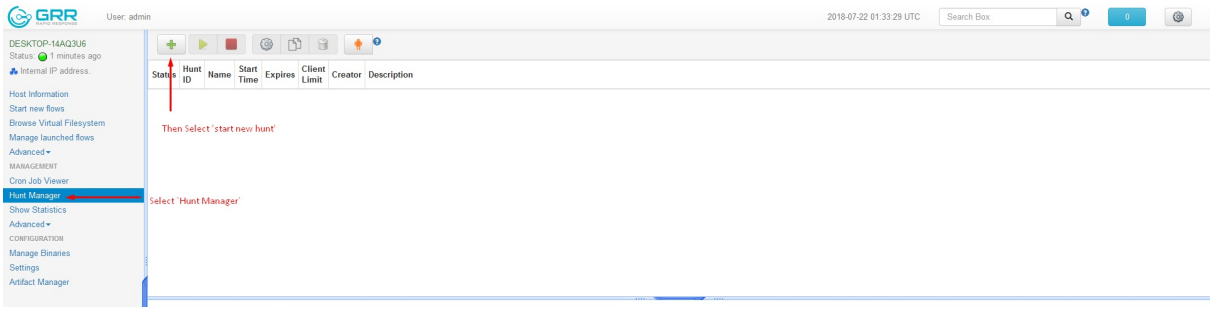


Conducting Analysis Using GRR.

- When starting analysis on one individual host, the analyst should start by interrogating the host for information. This w ill populate all of the unknow n metadata about the host.



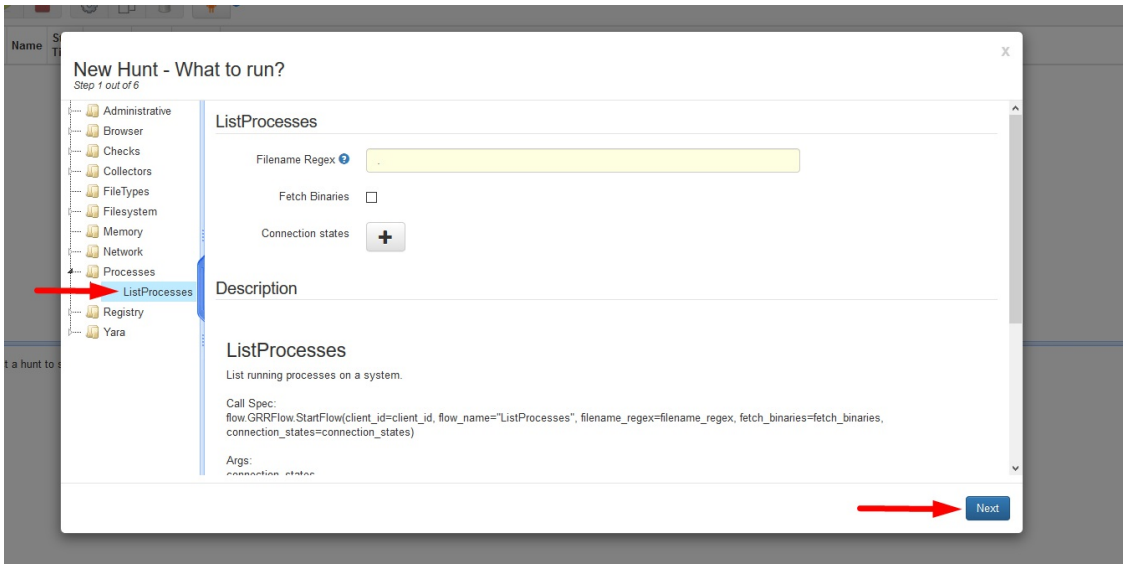
- Going forw ard, Hunts can be performed against the hosts. (for example: Task lists and Netstats)



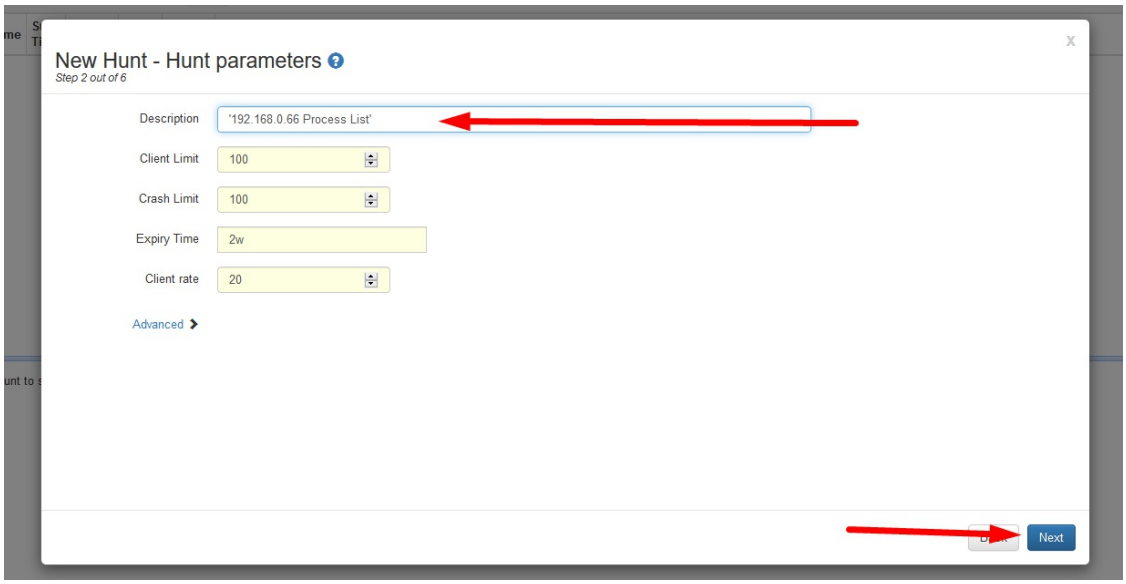
  i. Running Netstats or Process List against hosts.
    a. Choose the 'Hunt Manager' tab and select the green + or 'Start new Hunt'

b. Select either Netw ork for `netstat` or Processes for `tasklist`
   - For this demonstration w e w ill be running a tasklist but the process is relatively the same for any other hunts.

c. Select the ListProcesses option then select Next.

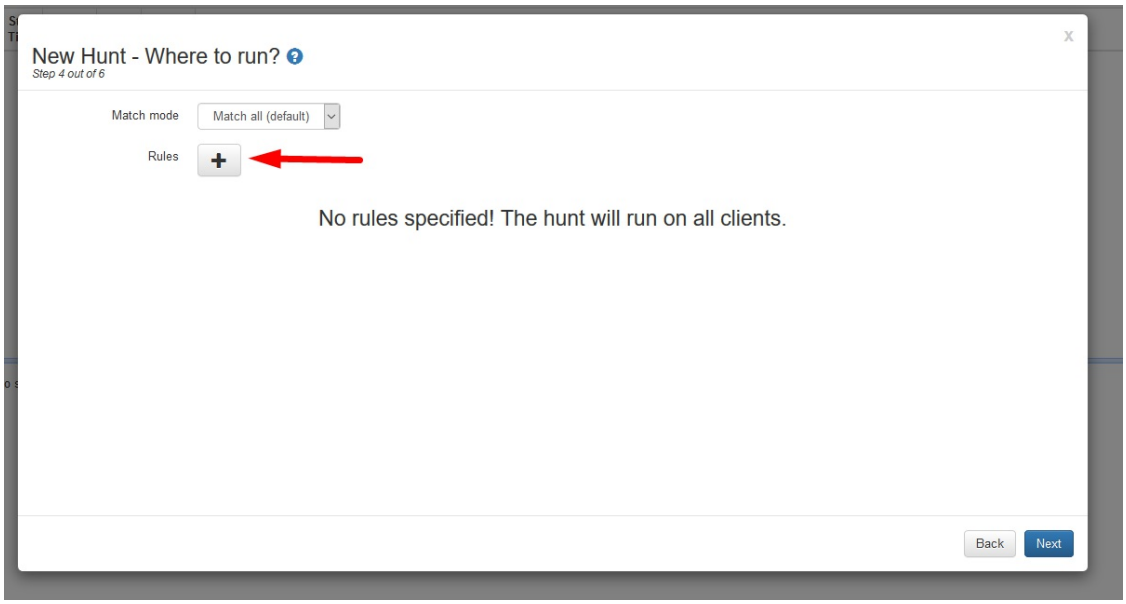


d. Enter a description for the Hunt for it to be distinguished in the future then select 'Next'.



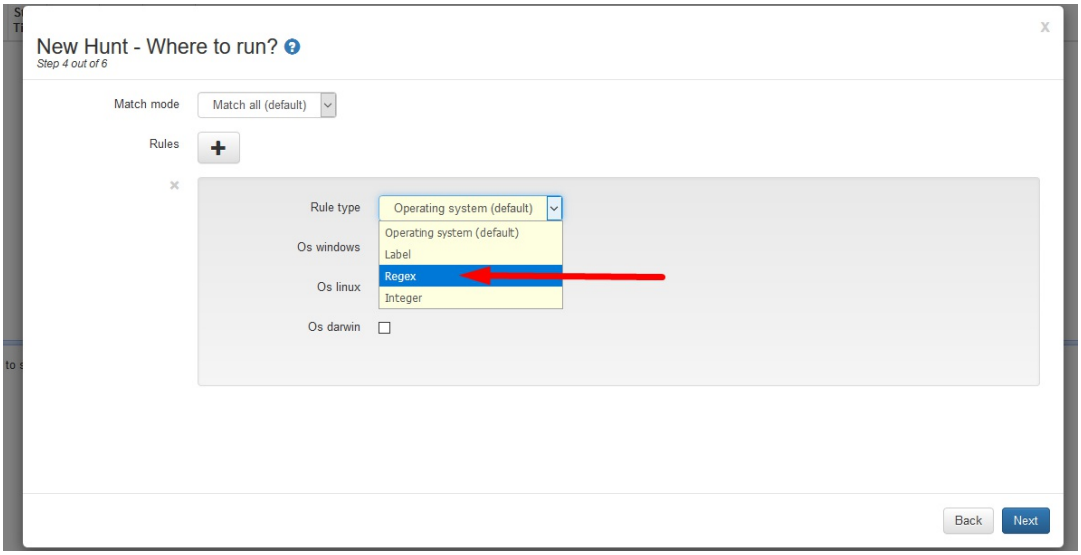
e. Unless you have implemented Output plugins, select next.

f. This next screen is the 'Match Mode' screen this is the where the Grr server will know which hosts you would like to run the hunt against. Select the '+' to add a new match case.

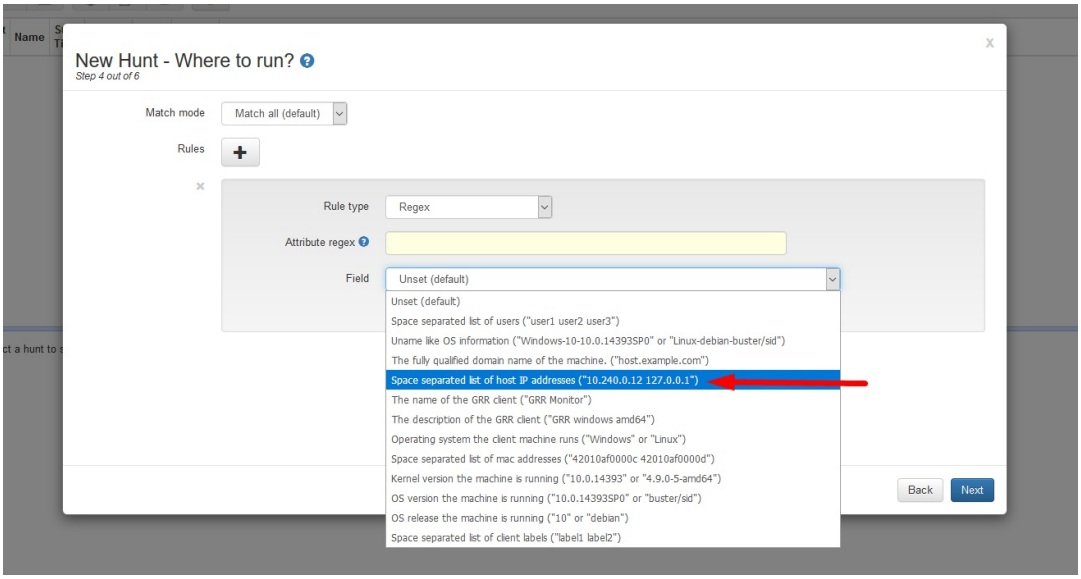


a. There are multiple ways to set up the 'Match Cases'
- By Operating Systems
- By Labels made for the hosts
- Or By 'Regex' which consists of multiple Cases.

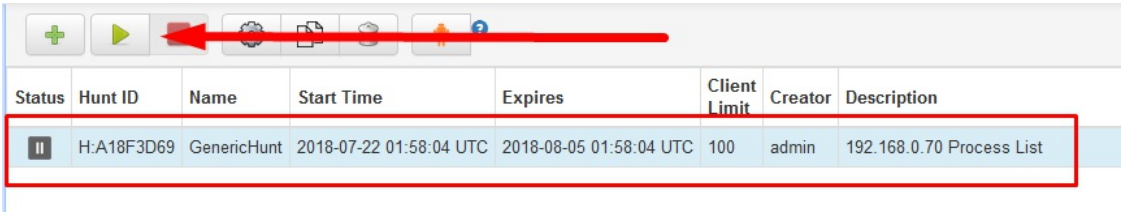
a. Choose the Regex option to run against specific IP addresses.



b. Under field select `Space seperated list of host IP addresses`, and enter the IP address in the `Attribute Regex` field then select Next.

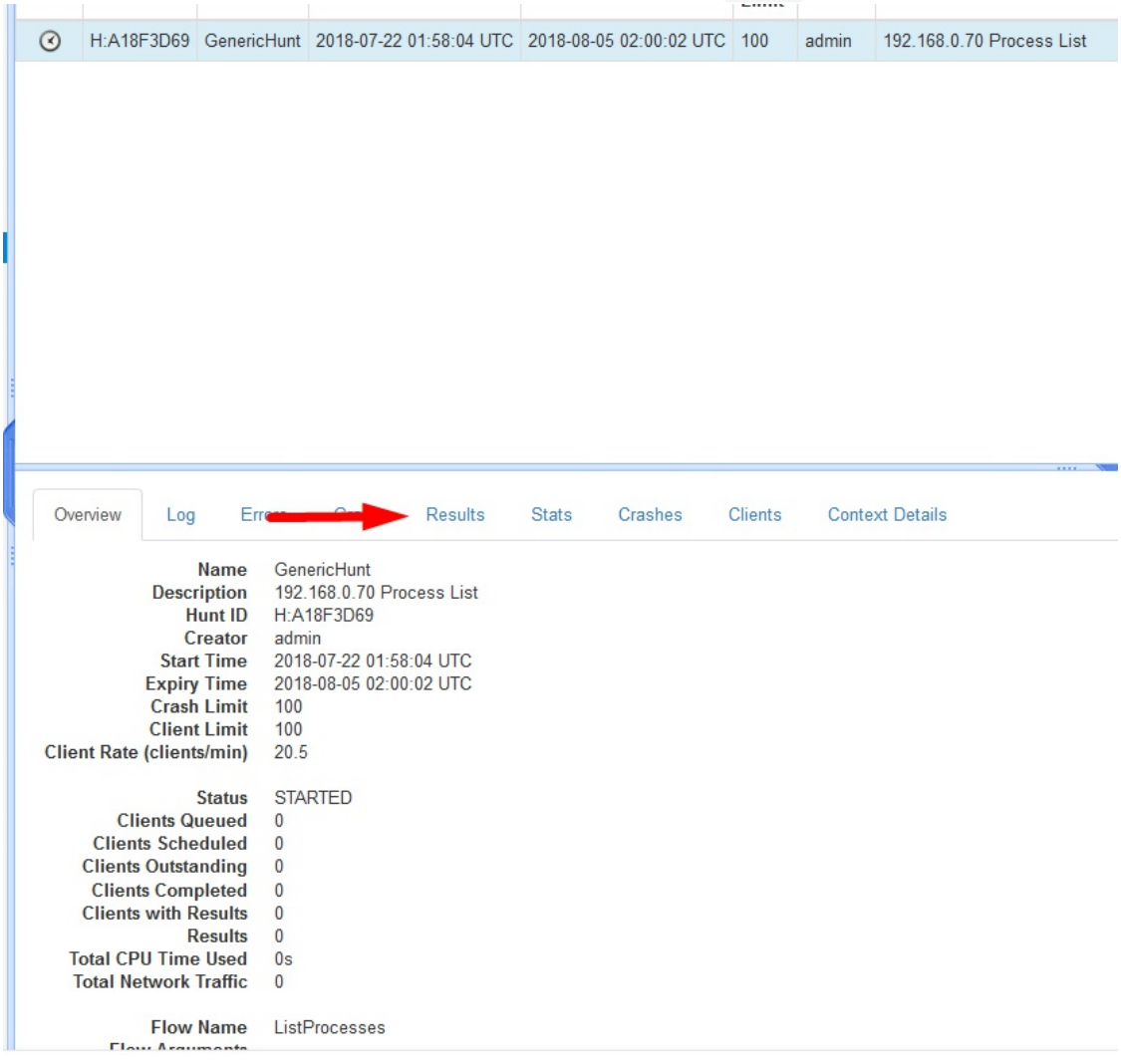


g. After selecting 'Create Hunt', Select the Hunt and click start.



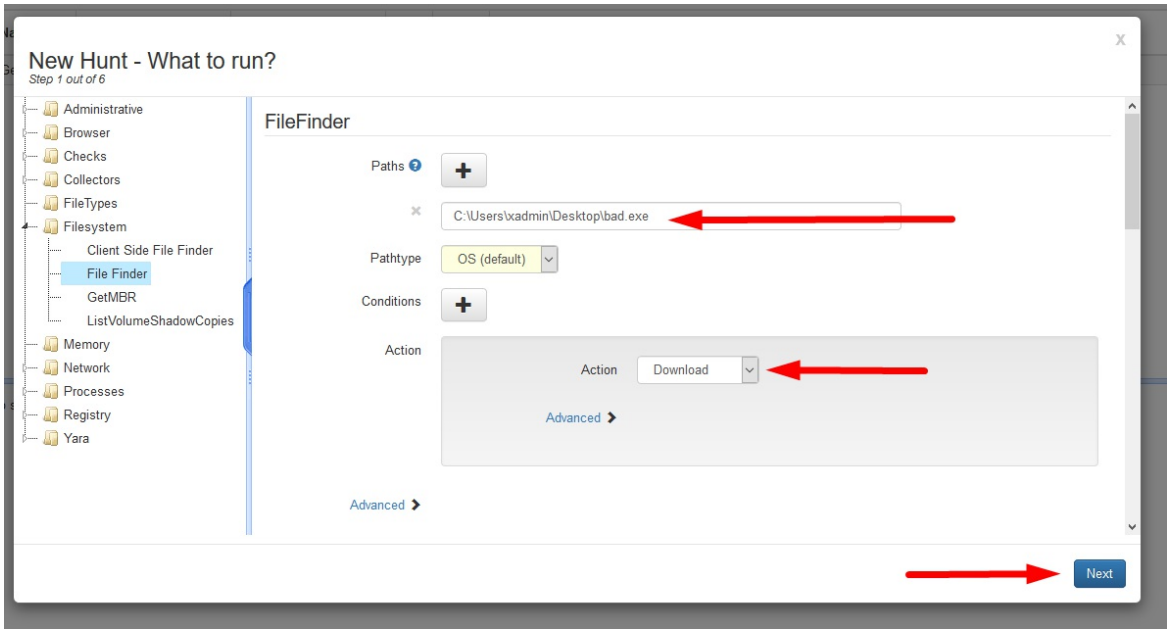
Status	Hunt ID	Name	Start Time	Expires	Client Limit	Creator	Description
⏸	H:A18F3D69	GenericHunt	2018-07-22 01:58:04 UTC	2018-08-05 01:58:04 UTC	100	admin	192.168.0.70 Process List

h. After the Hunt has completed, Select the hunt again and at the bottom click `Results`

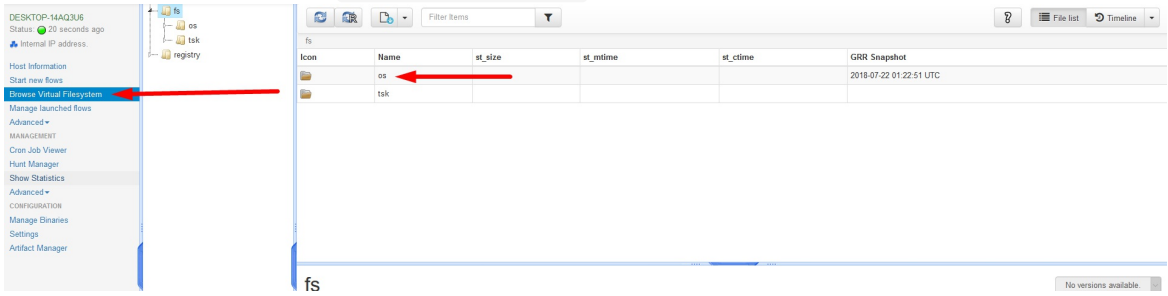


⏲	H:A18F3D69	GenericHunt	2018-07-22 01:58:04 UTC	2018-08-05 02:00:02 UTC	100	admin	192.168.0.70 Process List

ii. Finding a File on a host.
iii. Choose the 'Hunt Manager' tab and select the green + or 'Start new Hunt'
iv. Select the `Filesystem` option, then `File Finder`.
v. Enter the file path, and the action taken against this file then select Next.



vi. Enter a description for the Hunt for it to be distinguished in the future then select 'Next'.
vii. Unless you have implemented Output plugins, select next.
viii. This next screen is the 'Match Mode' screen this is the where the Grr server will know which hosts you would like to run the hunt against. Select the '+' to add a new match case.
ix. Choose the Regex option to run against specific IP addresses.
x. Under field select `Space seperated list of host IP addresses`, and enter the IP address in the `Attribute Regex` field then select Next.
xi. After selecting 'Create Hunt', Select the Hunt and click start.
xii. After the Hunt has completed, Select the hunt again and at the bottom click `Results`
xiii. Browsing the Filesystem of a host.
xiv. After Selecting desired host, Click `Browse Virual Filesystem`. Then Select 'Os'



xv. This will go directly to the main directory where all drives installed on the device will be seen.
    - Note the listing will have to be refreshed to populate the folders and files within the drive.