**\*AmberCry Kit Power on and Startup Guide\***

**Network Information:**

The kit network is 10.1.x.x/16. Each individual kit has it's own subnet, kit 1 is 10.1.6.x, kit 2 is 10.1.7.x, and kit 3 is 10.1.8.x

|  |  |  |  |
| --- | --- | --- | --- |
| **SERVICE** | **IP** | **USER** | **PASSWORD** |
| CMC | http://10.1.x.2 | root | Br111ckSquad!!! |
| iDRAC Blade 1 | http://10.1.x.3 | root | Br111ckSquad!!! |
| iDRAC Blade 2 | http://10.1.x.4 | root | Br111ckSquad!!! |
| ESXi | http://10.1.x.10 | root | Br111ckSquad!!! |
| Moloch | http://10.1.x.20:8005 | admin | admin |

**Definitions:**

* **iDRAC:** Integrated Dell Remote Access Controller. Allows users to manage a server remotely.
* **CMC:** Chassis Management Controller. Allows users to manage the chassis remotely.

**Required Components:**

- Kit x Chassis

- Kit x Blades 1 and 2

- Three RJ45 tipped ethernet cable

- One SFP 1G Ethernet adapter

- One TPLink Unmanaged Switch

- One Laptop

- All assosciated power cables and surge protectors

**Background Information**:

a) It is important to ensure that the kit blades go to the matching kit chassis, e.g. Kit 1 Blades to Kit 1 Chassis. You can tell using the serial numbers on the kit blades and chassis and referring them against the table below. They will not network correctly if plugged in wrong.

|  |  |  |  |
| --- | --- | --- | --- |
| **KIT NUMBER** | **CHASSIS SERIAL** | **BLADE1 SERIAL** | **BLADE2 SERIAL** |
| 1 | ID9K-03-01 | ID9K-06-01 | ID9K-06-02 |
| 2 | ID9K-03-02 | ID9K-06-03 | ID9K-06-04 |
| 3 | ID9K-03-03 | ID9K-06-05 | ID9K-06-06 |

b) On the Chassis, the serial number is located on the lefthand side from the front. On the Blades, the serial is located on the top of the blade, towards the front.

When installing or "plugging in" any component of this kit, if it has to be forced, it's being plugged in incorrectly. It should slide in and seat well. If not, find someone with more experience to assist.

c) On the chassis, in the top row of input ports, more on the right side of center, there is an ethernet port labelled '**GB1**' that allows a user to plug in a laptop to access the CMC. You will need to plug in one ethernet cable here, subsequently referred to as the "Chassis Management Port"

d) Below the Chassis Management Port, there are a total of twelve larger ports. These ports cannot be plugged into with just an RJ45 Tipped ethernet cable. They require an SFP to be plugged in first. Install the SFP with the serial number facing upwards, and then plug the ethernet cable into the SFP.

e) To explain the ports on the chassis, ports labelled 1-4 are wired directly into the top blade. Ports labelled 5-8 are wired directly into the bottom blade. Ports labelled 9-12 are more complicated. They network the blades together and will provide data from both blades just by plugging into one of them

f) Further explanation of the ports on the chassis, ports labelled 2, 4, 6, 8, 10, and 12 are disabled. If you plug anything into them, you will not receive data or connectivity. Furthermore, Ports labelled 9 and 11 are both able to transmit data from all of the following ports: 1,3,5 and 7. So to network the kits as simply as possible, install an SFP in port 9 to maintain connectivity to all blades and their active ports.

g) Moloch Services will not run until Elastic Search services are up and running on each node. These nodes reside on ESXi(this is a hypervisor operating system) as Virtual Machines.

**POWER ON AND STARTUP STEPS:**

1. Begin by designating where you have enough space and convenience to set up the AmberCry Kit. There needs to be a nearby powersource to plug in a surge protector.

2. Pull out the Chassis from the pelican case. Verify the serial number and place the chassis where you want to set it up. On the chassis, there are arms on the left and right sides inside the blade slots that need to be slid out before installing the blades. They slide out much like dresser drawer rails. There is an upside-down 'L' shaped tab above each arm that needs to be pushed up to slide those arms out.

3. Pull out the first blade from the pelican case. Verify the serial number to ensure it is being installed in the correct chassis. Blade 1 goes in the top bay and Blade 2 goes in the bottom bay. On the front of the blade, there is a small locking handle with a blue tab on it. Release the handle by pulling the blue tab and swing that handle out before installing the blades. Slide the blade into the slot gently until it will not go further, then close the locking handle to lock it in place. You should hear an audible 'click'.

4. After installing the blades, place the unmanaged switch on top of the chassis and plug in ethernet cables into any port. It does not matter which ports because it is an unmanaged switch.

5. Plug one ethernet cable into the analyst laptop and plug the other end into the switch. Plug one ethernet cable into the Chassis Managment Port and plug the other end into the switch.

6. Install an SFP into port 9 on the Chassis with the label up, and plug one ethernet cable into that SFP.

**\*\* BEFORE POWERING ON THE KIT, ENSURE ALL ETHERNET CABLES ARE PLUGGED IN WHERE THEY NEED TO BE. IF NOTHING IS PLUGGED IN WHEN THEKIT IS POWERED ON, ALL PORTS WILL BE DISABLED\*\***

7. Plug the power cables into the surge protector, the chassis, and the switch. Verify the Surge Protector is turned on. The chassis will have the power ports on the right-hand side on the front of the chassis. Once power is connected, the fan blades will spin quickly for a short period of time. This is normal.

8. It may take a few minutes before the blue 'heartbeat' light located on the left-hand side of the front of the chassis and next to the power button is lit, but once the blue 'heartbeat' light turns on, press the chassis power button. It will light up green if it is beginning to power on. The fans will spin again and stay on this time. This is normal.

9. Wait a few moments, then log into the laptop with the password **'Br111ckSquad!!!**'. Open a Google Chrome Browser and type in the kit's CMC IP(specified above)

10. Log into the CMC using the user of 'root' and password '**Br111ckSquad!!!**'. When logged in, on the left side of the browser window you will see a section titled 'Server Overview'. You will see that there are four items beneath that, but only two are available, these would be 1 and 3. This is normal. The 1st selection goes to Blade 1 and the 3rd selection(or only other available option) goes to Blade 2.

11. Select the 1st server from the list to manage Blade 1. Near the top, you will see three tabs in the black bar. Select the one that says 'Power', then ensure the tab underneath it says 'Control'. When the power control options load, ensure 'Power On' radio button is selected, then click the blue "Apply" button near the bottom. You will be asked if you want to execute the server control action. Select yes. Repeat for Blade 2. To verify they are powered on, look for lights on the front end of the blade. If none are lit, the blade is not powered on.

12. Navigate to the Blade 1 iDRAC IP(specified above). Log in with the user of 'root' and the password '**Br111ckSquad!!!**'.

13. Scroll to the bottom of the page once logged in. On the right side of the web page will be a thumbnail underneath a title that says "Virtual Console". Click on the thumbnail.

14. A new window will open that will show a boot process. This is going to be the Boot up process for ESXi and it may take a few minutes to complete. Do not press any options, let it boot to the preset defaults. You will know that the boot process is complete when you see a menu that says something to the effect of "Navigate to http://10.1.x.10 to manage this device"

15. Open up a Google Chrome Browser from the laptop and navigate to the ESXi IP(specified above). Log in using the user of 'root' and password '**Br111ckSquad**!!!'.

16. On the left-hand side of the webpage will be a short list. Click on the item that says "Virtual Machines". When they load, select the top checkbox above the list to select all the virtual machines and select the "Power On" option.

17. Click on the VM titled "node1 -.11", then click the thumbnail to enter the virtual machine.

18. Log in under the default user(should be named "gucci") with the password '**Br111ckSquad!!!**'.

19. Right-click on the desktop of the VM and select "open terminal". Type in the command "systemctl status elasticsearch" and press enter to verify that the output says "Active" and/or "Running"

20. In the same terminal session, type in "systemctl status kibana" and press enter to verify the output says "Active" and/or "Running". If both are running, close out of the Virtual Machine and continue. If not, contact someone with an infrastructure JQR for help.

21. Navigate the the Blade 2 iDRAC IP(specified above). Log in with the user of 'root' and the password '**Br111ckSquad!!!**'.

22. Scroll to the bottom of the page once logged in. On the right side of the web page will be a thumbnail underneath a title that says "Virtual Console". Click on the thumbnail, even if it says "No Signal".

23. The boot process for Blade 2 should be complete by now. If not, wait for it to complete. When it is complete, there will be a login prompt for the user "gucci", or a blue screen with the time on it. Log in with the password '**Br111ckSquad!!!**'. If the blue screen is what you see, click and drag upwards to get to the login prompt. If the screen is green and says "No Input", try to wake the server be clicking on the screen. If it doesn't work, contact someone with an Infrastructure JQR for help.

24. Right click on the Blade 2 desktop after logging in, and select "open terminal"

25. Verify the Elastic Cluster is up and running by running the command "sudo curl -XGET 'http://10.1.x.11:9200/\_cluster/health?pretty'" and press enter. (There is an underscore before the "cluster" in the command) The output should have the word "green" next to the status. If not, contact someone with an infrastructure JQR for help. When using the "sudo" command, use the password '**Br111ckSquad!!!**' when prompted.

26. After verifying the cluster is up, type in "sudo systemctl start molochcapture" and press enter, then type in "sudo systemctl start molochviewer" and press enter.

27. Verify both services are running by typing "systemctl status molochcapture" andpress enter, then type in "systemctl status molochviewer" and press enter. Verify the output says "Active" and/or "Running". If both are running, close out of the iDRAC console window. If not, contact someone with an infrastructure JQR for help.

28. To verify Moloch is working, type into a Google Chrome Browser "**http://10.1.x.20:8005**". Ensure you type in the port "8005" to reach the viewer. Even if you don't see data, if you have a web page, you have completed the Power on and Startup. Default credentials are "**admin**" for **both username and password**.

**\*\*ONLY FOR KIT 2, THE MOLOCH MASTER KIT\*\***

It is necessary to run the following commands to ensure that Moloch can work together with the other kits.

29. Repeat steps 23 and 24 to log back into the Blade 2 Desktop and open a terminal.

30. Type in "cd /data/moloch/viewer" and press enter

31. Type in "sudo /data/moloch/bin/node multies.js -n multi-viewer" and press enter to let that run. As before, use the password **'Br111ckSquad!!!**' when prompted.

32. Right click on the desktop and open a new terminal session. Then type in "cd /data/moloch/viewer" and press enter.

33. Type in "sudo /data/moloch/bin/node viewer.js -n multi-viewer" and press enter. As before, use the password **'Br111ckSquad!!!**' when prompted. Leave both terminal sessions open.

34. To verify that the Multi-Viewer service is working, close out of the Blade 2 Desktop and type into a Google Chrome Browser "**http://10.1.7.20:8009**". If you connect and see data, everything is working correctly. Default credentials are "**admin**" for **both username and password**.

**POWER OFF STEPS:**

1. Navigate and log into ESXi the same as steps 15 and 16. Select all of the VM's as if you were to power them on, but this time, select "Power Off Virtual Machines". When the dialogue box pops up, click the "reload" button.

2. Wait for that to complete, then log into the CMC by navigating back the CMC IP(specified above), and select the server for Blade 1 as if you were to power it on.

3. Go to power, then select control, then select the radio button next to "Power Off", then click apply. Select "yes" when asked if you want to execute a server control action.

4. Repeat step 3. for Blade 2.

5. Select "Chassis Overview" at the top of the page, then select "Power" and select "Control". Then select the radio button next to "Power Off", then click apply. Select "yes" when asked if you want to execute a server control action.

6. When fans stop spinning loudly, the kit is powered off. Unplug all cabling and store the Chassis and Blades in their corresponding pelican cases.