hauc

HAUC Quick Start Guide

This document descrives detailed procedure for setting up HAUC on vSphere ESXi.

Preparing 64bit Windows PC

Download **hauc-master.zip** and extract.

- Edit cf/hauc.conf so that match to your environment.

Download **ECX**

- Extract it and copy *expresscls-4.1.1-1.x86_64.rpm* in it to the subfolder *cf*.

Put the (trial) license files of ECX to the subfolder *cf*.

- ECX4.x-lin1.key
- ECX4.x-Rep-lin1.key
- ECX4.x-Rep-lin2.key

Download putty, plink, pscp to the subfolder *cf*.

Download and install Strawberry Perl.

Configure the Windows PC to have IP address such as 172.31.255.100/24 so that becomes IP reachable to **172.31.255.0/24** network where the ESXi hosts exists.

Download CentOS 7.6 (CentOS-7-x86_64-DVD-1810.iso) and put it **/vmfs/volumes /datastore1/iso/** on ESXi#1 and ESXi#2. (The directory “iso” needs to be created under /vmfs/volumes/datastore1/.)

Setting up ESXi - Network

Install vSphere ESXi then set up IP address as following.

	Primary ESXi	Secondary ESXi

	Primary ESXi	Secondary ESXi
Management IP	172.31.255.2	172.31.255.3

Start ssh service and configure it to start automatically.

- Open vSphere Host Client for ESXi#1 (http://172.31.255.2/) and ESXi#2 (http://172.31.255.3/)
    - [Manage] in [Navigator] pane > [Services] tab
        - [TSM-SSH] > [Actions] > [Start]
        - [TSM-SSH] > [Actions] > [Polilcy] > [Start and stop with host]

Install the licenses

- Obtain the license keys for both ESXi.
- On vSphere Host Client for both ESXi,
    - [Manage] in {Navigator] pane > [Licensing] tab > [Actions] > [Assign license]
    - enter the license key > [Check license] > [Assign license]

Setup NTP servers

- On vSphere Host Client for both ESXi,
    - [Manage] in [Navigator] pane > [System] tab
    - [Time and date] > [Edit settings]
    - Select [Use Network Time Protocol (enable NTP client)] > Select [Start and stop with host] as [NTP service startup policy] > input IP address of NTP server for the configuring environment as [NTP servers]

Configure vSwitch, Physical NICs, Port groups, VMkernel NIC for iSCSI Initiator

- Run *cf-esxi-phase1.pl* in subfolder *cf*.
    - When you see the message like following, answer “y”.

```
2019/12/10 23:44:49 [D] | WARNING - POTENTIAL SECURITY BREACH!
2019/12/10 23:44:49 [D] | The server's host key does not match the one PuTTY has
2019/12/10 23:44:49 [D] | cached in the registry. This means that either the
2019/12/10 23:44:49 [D] | server administrator has changed the host key, or you
2019/12/10 23:44:49 [D] | have actually connected to another computer pretending
2019/12/10 23:44:49 [D] | to be the server.
2019/12/10 23:44:49 [D] | The new rsa2 key fingerprint is:
2019/12/10 23:44:49 [D] | ssh-rsa 2048 2f:7a:f6:f7:85:d5:fc:f4:f0:c5:9b:a2:59:19:4
2019/12/10 23:44:49 [D] | If you were expecting this change and trust the new key,
2019/12/10 23:44:49 [D] | enter "y" to update PuTTY's cache and continue connectin
```

```
2019/12/10 23:44:49 [D] | If you want to carry on connecting but without updating
2019/12/10 23:44:49 [D] | the cache, enter "n".
2019/12/10 23:44:49 [D] | If you want to abandon the connection completely, press
2019/12/10 23:44:49 [D] | Return to cancel. Pressing Return is the ONLY guaranteed
2019/12/10 23:44:49 [D] | safe choice.
2019/12/10 23:44:57 [D] | Update cached key? (y/n, Return cancels connection) Conn
```

Setting up ESXi - Datastore

If a storage (HDD) dedicated for UC VMs is prepared on each ESXi, set up the storage as **datastore2**.

- On vSphere Host Client for ESXi#1 and ESXi#2,
    - [Storage] in [Navigator] pane > [Datastores] tab > [New datastore]
        - Select [Create new VMFS datastore] > [Next] > input [datastore2] as [name] > Select the storege device for UC VMs.
- Edit the lines of @iscsi_ds in *hauc.conf* in subfolder *cf* as

```
our @iscsi_ds   = ('datastore2', 'datastore2');
```

Creating VMs for iSCSI Cluster and vMA Cluster

Specify the size of volume or HDD which vMA and iSCSI VMs are stored.

- Edit *hauc.conf* in the subfolder *cf*

    ```
    our $advertised_hdd_size = 1200;
    ```

    This is the Advertised HDD Size (in GB) of a single HDD/SSD or an array on which datastore2 resides. (i.e. 1200 for an advertised capacity of 1.2 TB)

    ```
    our $managed_vmdk_size = 635;
    ```

    This is the Total Size (in GB) of all of your Managed Thick-Provisioned VMs, including intended disk allocations and memory allocations for each VM. (i.e. 635, which will just fit into a 1.2TB HDD, allowing for 33% free space)

    NOTE

    - The size should be not Gibibyte but Gigabyte.
    - Just supply the interger value. (Do not speciy a unit symbol “G”)
    - The actual size of the *iSCSI1 Datastore* will be calculated from these two input values

Create VMs of iSCSI1, iSCSI2, vMA1, vMA2.

- Run *cf-esxi-phase2-create-vm.pl* in subfolder *cf*,

  NOTE

    - This takes a long time for making vmdk eager zeroed thick.
    - If you run *cf-esxi-phase2-create-vm.pl* again, **delete** the VMs (iscsi1, iscsi2, vma1, vma2) before that by using vSphere Host Client, and confirm the ESXi datastore does not have the folders the VMs.

Boot all the VMs and install CentOS.

- All you need to do during the installation is select *sda* as *INSTALLATION DESTINATION* and set *ROOT PASSWORD*. No need to worry about other things like *TIME ZONE* or *TIME OF DAY*.

Configure the first network of the VMs.

- Open two ESXi Host Client (https://172.31.255.2 and https://172.31.255.3), open the console of iSCSI and vMA VMs and login to them as root user, then run the below command to set IP address so that Windows client can access to the VMs.

    - on iSCSI1 console:

      ```
      nmcli c m ens192 ipv4.method manual ipv4.addresses 172.31.255.11/24 connection.aut
      ```

    - on iSCSI2 console:

      ```
      nmcli c m ens192 ipv4.method manual ipv4.addresses 172.31.255.12/24 connection.aut
      ```

    - on vMA1 console:

      ```
      nmcli c m ens160 ipv4.method manual ipv4.addresses 172.31.255.6/24 connection.autc
      ```

    - on vMA2 console:

```
nmcli c m ens160 ipv4.method manual ipv4.addresses 172.31.255.7/24 connection.autc
```

Confirm accessibility to the following six IP addresses from Windows PC by using putty. **Do not omit this process**. The procedure hereafter assumes that SSH Hostkey entries of these IP addresses are made on Windows registry by this process.

- 172.31.255.2 (ESXi#1)
- 172.31.255.3 (ESXi#2)
- 172.31.255.6 (vMA1)
- 172.31.255.7 (vMA2)
- 172.31.255.11 (iSCSI1)
- 172.31.255.12 (iSCSI2)

Setting up iSCSI Cluster

Configure iSCSI VMs to fill prerequisite conditions for creating iSCSI Cluster.

- Run *cf-iscsi-phase1.pl* in the subfolder *cf*.
  On the completion, both VMs are rebooted. Wait the completion of the reboot.

Create iSCSI Cluster.

- Run *cf-iscsi-phase2.pl* in the subfolder *cf*.
  On the completion, both VMs are rebooted.

- Open ECX WebUI (http://172.31.255.11:29003) and wait the cluster starts the failover group "*failover-iscsi*", and wait the completion of synchronizing the mirror disk resource.

  NOTE

  - While the synchronizing, the following error message is displayed and can be ignored.

    Detected an error in monitoring mdw1. (65 : Both local and remote mirror disks are abnormal.(md1))

Setting up ESXi - iSCSI Initiator

- Run *cf-esxi-phase3.pl* in subfolder *cf*.

After running the script, confirm that the newly created *iSCSI1* datastore can be accessed by browsing Storage in both of the ESXi hosts.

Deploying UC VMs on iSCSI datastore

Issue *mirror break* so that prevent automatic mirror-recovery during the deployment.

- On iSCSI Cluster WebUI (http://172.31.255.11:29003)
  [Mirror disks] tab > click [md1] > [Mirror break] icon under [iscsi2] > [Execute]

Deploy the following UCE VMs (for which failover protection must be provided by ECX) on your choice of *esxi1* or *esxi2*. These VMs must be deployed on the *iSCSI1* datastore.

- SV9500
- UCE
- MGSIP
- GNAV
- CMM
- UM8700 (or UM4730)
- VS32

Issue *mirror recovery*.

- On iSCSI Cluster WebUI
  [Difference copy] icon under [iscsi1] > [Execute]

Setting up vMA Cluster

Configure vMA VMs to fill prerequisite conditions for creating vMA Cluster.

- Run *cf-vma-phase2.pl* in the subfolder *cf*.

  After the completion, both VMs are rebooted. Wait the completion of the reboot.

Create vMA Cluster

- Run *cf-vma-phase3.pl* in the subfolder *cf*.

  After the completion, open vMA Cluster WebUI (http://172.31.255.6:29003) and wait for the cluster to be started.

2020.01.06 Miyamoto Kazuyuki kazuyuki@nec.com