EXPRESSCLUSTER X Quick Start Guide  
for vSphere ESXi Host Clustering  
with iSCSI Target Clustering

Ver.2017.09.28

**Disclaimer**

The contents of this document are subject to change without notice. NEC Corporation assumes no responsibility for technical or editorial mistakes in or omissions from this document. To obtain the benefits of the product, it is the customer’s responsibility to install and use the product in accordance with this document. The copyright for the contents of this document belongs to NEC Corporation. Copying, altering, or translating this document, in full or in part, without the permission of NEC Corporation, is prohibited.

**About this Guide**

This guide provides a hands-on "Quick Start" set of instructions for the EXPRESSCLUSTER X for Linux. The guide assumes its readers to have Linux system administration knowledge and skills with experience in installation and configuration of CentOS or Red Hat Enterprise Linux operating systems, Storages, and Networks. The guide includes step-by-step instructions to install and configure EXPRESSCLUSTER X with iSCSI Target, vSphere Management Assistant (vMA) and vSphere ESXi.

**Where to go for more information**

For any further information, please visit the EXPRESSCLUSTER web-site at

<http://www.nec.com/expresscluster>

The following guides are available for instant support:

* Getting Started Guide - This guide explains general cluster concepts and overview of EXPRESSCLUSTER functionality.
* Installation Guide - This guide explains EXPRESSCLUSTER installation and configuration procedures in detail.
* Reference Guide - This is a reference of commands that can be put in EXPRESSCLUSTER scripts and maintenance commands that can be executed from the server command prompt.

The guides stated in above can be found at:

<http://www.nec.com/global/prod/expresscluster/en/support/manuals.html>

Table of Contents

[1. Overview 1](#_Toc497844332)

[1.1. Description of the solution 1](#_Toc497844333)

[2. System Requirements and Planning 1](#_Toc497844334)

[2.1. Product Versions 1](#_Toc497844335)

[2.2. Configuration example 2](#_Toc497844336)

[Network 2](#_Toc497844337)

[PC Servers spec for each vSphere ESXi / vSphere Hypervisor 3](#_Toc497844338)

[VM spec for iSCSI Target Cluster 3](#_Toc497844339)

[Hosts Parameters example 3](#_Toc497844340)

[3. Setup Procedure 5](#_Toc497844341)

[3.1. Setting up ESXi 5](#_Toc497844342)

[3.2. Setting up iSCSI Target Cluster 5](#_Toc497844343)

[Creating VMs 5](#_Toc497844344)

[Installing OS and packages 5](#_Toc497844345)

[Configuring iSCSI Target Cluster 6](#_Toc497844346)

[Adding the failover-group for controlling iSCSI Target service. 6](#_Toc497844347)

[Adding the MD resource 6](#_Toc497844348)

[Adding the execute resource for controlling target service 7](#_Toc497844349)

[Adding floating IP resource for iSCSI Target 7](#_Toc497844350)

[Adding the execute resource for automatic MD recovery 7](#_Toc497844351)

[Adding the custom monitor resource for automatic MD recovery 8](#_Toc497844352)

[Adding Monitor which make remote vMA VM and ECX keep online. 8](#_Toc497844353)

[Applying the configuration 9](#_Toc497844354)

[Configuring iSCSI Target 9](#_Toc497844355)

[3.3. Setting up ESXi - iSCSI Initiator 10](#_Toc497844356)

[3.4. Deploying UC VMs on iSCSI datastore 11](#_Toc497844357)

[3.5. Setting up vMA Cluster 11](#_Toc497844358)

[Configuring Failover Group 11](#_Toc497844359)

[Configuring Monitor resource 16](#_Toc497844360)

[Adding monitor for remote ESXi iSCSI session and ESXi inventory 16](#_Toc497844361)

[Adding Network Monitor for VMn 17](#_Toc497844362)

[Adding Monitor which make remote vMA VM and ECX keep online. 18](#_Toc497844363)

[Applying the configuration 19](#_Toc497844364)

[3.6. Setting up ESXi - VM automatic boot, Network 19](#_Toc497844365)

[4. Common Maintenance Tasks 19](#_Toc497844366)

[4.1. The graceful shutdown procedure for both ESXi 19](#_Toc497844367)

[4.2. Stopping one of vMA Cluster node 19](#_Toc497844368)

[4.3. Deleting / Adding UC VM on vMA Cluster 20](#_Toc497844369)

[Deleting VM 20](#_Toc497844370)

[Adding VM 20](#_Toc497844371)

[5. Troubleshooting 21](#_Toc497844372)

[5.1. Log Collection HOWTO 21](#_Toc497844373)

[6. The value on this solution 22](#_Toc497844374)

# Overview

The general procedure to deploy EXPRESSCLUSTER X on two ESXi server machines (Primary and Standby) for high availability of UC VMs consists of the following major steps:

1. Perform system planning to determine requirements and specify specific configuration settings prior to start of actual system installation and configuration.
2. Set up Primary and Standby ESXi.
3. Set up Primary and Standby VMs, then set up iSCSI Target Cluster on them.
4. Configure iSCSI Initiator on both ESXi and connect them to the iSCSI Target.
5. Deploy Primary and Standby vMA, then set up vMA Cluster on them.
6. Deploy UC VMs on ESXi and configure vMA Cluster.

## Description of the solution

* This solution supports failover of application VMs over LAN (same subnet) and does not support WAN (different subnet).
* With this solution, VM failover can be performed regardless of the guest OS type or the application type running on it.

## Deliverables for installation and maintenance

* This document
* Scripts in the attached *iSCSI-Cluster-scripts* and *vMA-Cluster-scripts* folder.

## Strong point of the solution

* 2 boxes configuration : *vSAN* requires 3 boxes at least
* Synchronous replication : impossible by *vSphere Replication*
* Does not require running *vCenter*.

Linux VM #1

**EC**

storage

iSCSI Target

ESXi

VM

vMA

EC

Linux VM #2

**EC**

iSCSI Target

storage

ESXi

vMA

**EC**

VM

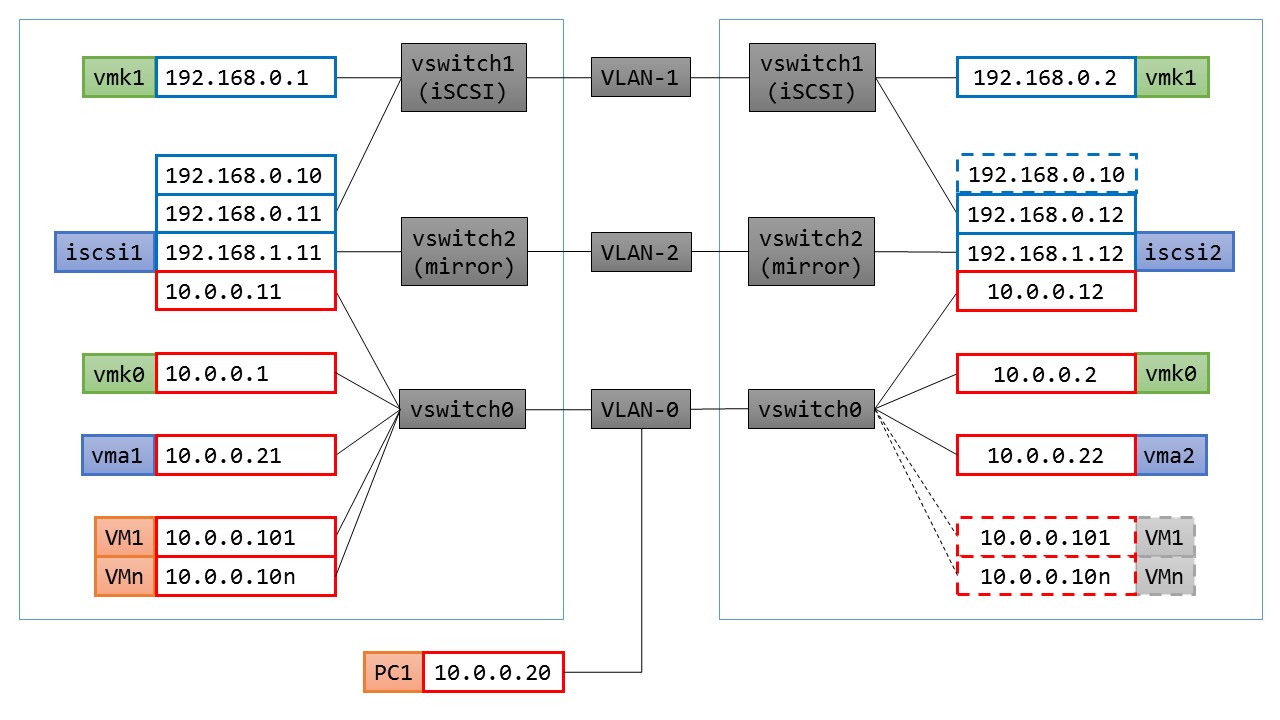
# System Requirements and Planning

## Product Versions

* VMware vSphere Hypervisor 6.0 (VMware ESXi 6.0)
* vSphere Management Assistant 6.0
* Red Hat Enterprise Linux 7.2 x86\_64 (or Cent OS 7.2)
* EXPRESSCLUSTER X for Linux 3.3.3-1

## Configuration example

### Network



IP addresses in RED depend on the user system and in BLUE is independent from the user system. And so, IP address in BLUE can be used in the actual system as it is.

### PC Servers spec for each vSphere ESXi / vSphere Hypervisor

|  |  |
| --- | --- |
| CPU cores | (2 cores for ESXi) + (2 cores for iSCSI) + (1 core for vMA)  + (Cores for UC VMs) |
| Memory | (2GB for ESXi) + (2GB for iSCSI) + (600MB for vMA)  + (required amount for UC VMs) |
| LAN Ports | 3 or more ports (iSCSI, ECX data-mirroring, Management) |
| HDD | (8GB for ESXi) + (16GB for iSCSI) + (3GB for vMA)  + (required amount for UC VMs) |

### VM spec for iSCSI Target Cluster

|  |  |
| --- | --- |
| vCPU | 2 or more |
| Network | 3 ports |
| Memory | 2GB or more |
| vHDD | 16GB for system + required amount for UC VMs (recommendation is 500GB or less) |

### Hosts Parameters example

| **ESXi** | **Primary** | **Secondary** |
| --- | --- | --- |
| Hostname | esxi1 | esxi2 |
| root password | passwd | passwd |
|  |  |  |
| IP Address for Management | 10.0.0.1 | 10.0.0.2 |
| IP address for VMkernel1(\*) | 192.168.0.1 | 192.168.0.2 |
| iSCSI Initiator WWN | iqn.1998-01.com.vmware:1 | iqn.1998-01.com.vmware:2 |
|  |  |  |
| **iSCSI Target Cluster** | **Primary** | **Secondary** |
| Hostname | iscsi1 | iscsi2 |
| root password | passwd | passwd |
|  |  |  |
| IP Address for Public (iSCSI) | 192.168.0.11/24 | 192.168.0.12/24 |
| FIP for iSCSI Target | 192.168.0.10 | 192.168.0.10 |
| IP Address for Mirroring | 192.168.1.11/24 | 192.168.1.12/24 |
| IP Address for Management | 10.0.0.11/24 | 10.0.0.12/24 |
|  |  |  |
| MD - Cluster Partition | /dev/sdb1 | <-- |
| MD - Data Partition | /dev/sdb2 | <-- |
| WWN of iSCSI Target | iqn.2016-10.com.ec:1 | <-- |
|  |  |  |
| **vMA Cluster** | **Primary** | **Secondary** |
| Hostname | vma1 | vma2 |
| vi-admin password | passwd | passwd |
|  |  |  |
| IP Address | 10.0.0.21 | 10.0.0.22 |

(\*) for iSCSI Initiator

# Setup Procedure

## Setting up ESXi

* Install vSphere Hypervisor.
* Set up hostname and IP address.

|  | **Primary** | **Secondary** |
| --- | --- | --- |
| Hostname | esxi1 | esxi2 |
| Management IP | 10.0.0.1 | 10.0.0.2 |

* Configure ssh service to start automatically when ESXi start.
  + On both vSphere Client for esxi1 and esxi2
  + Click ESXi host icon in left pane.
  + Select [Configuration] tab > [Security Profile] > [Properties] of Services
  + Check [Start and stop with host] > push [Start] button and make "ssh" running.

## Setting up iSCSI Target Cluster

### Creating VMs

On each ESXi, set up a VM to have

| **Virtual HW** | **Number, Amount** |
| --- | --- |
| vCPU | 2 or more |
| Memory | 2GB or more |
| Network | 3 ports |
| vHDD | 16GB for OS + required amount for UC VMs (recommendation is 500GB or less) |

### Installing OS and packages

On both iSCSI Target VMs,

* Install RHEL or CentOS 7.2 and configure
  + hostname (e.g. iscsi1, iscsi2)
  + IP address (e.g. 10.0.0.11, 192.168.0.11, 192.168.1.11 for iscsi1)
  + block device for MD resoruce ( /dev/sdb1 for Cluster Partition and /dev/sdb2 for Data Partition).
* Install packages and ECX licenses

# yum install targetcli targetd

# rpm -ivh expresscls.\*.rpm

# clplcnsc -i [base-license-file] -p BASE33

# clplcnsc -i [replicator-license-file] -p REPL33

# reboot

### Configuring iSCSI Target Cluster

On the client PC,

* Open Cluster Manager ( <http://10.0.0.11:29003/> )
* Change to [Operation Mode] from [Config Mode]
* Configure the cluster iSCSI-Cluster which have no failover-group.
  + Configure two Heartbeat I/F
    - 192.168.0.11 , 192.168.O.12 for primary interconnect
    - 192.168.1.11 , 192.168.1.12 for secondary interconnect and mirror connect

### Adding the failover-group for controlling iSCSI Target service.

* Right click [Groups] in left pane > [Add Group]
* Set [Name] as [failover-iscsi] > [Next]
* [Next]
* [Next]
* [Finish]

### Adding the MD resource

* Right click [iSCSI-Cluster] in left pane > [Properties]
* [Interconnect] tab > set [mdc1] for [MDC] and 10.0.0.0/24 network > [OK]
* Right click [failover-iscsi] in left pane > [Add Resource]
* Select [Type] as [mirror disk resource], set [Name] as [md1] then click [Next]
* [Next]
* [Next]
* Set
  + [Mount Point] as [/mnt]
  + [Data Partition Device Name] as [ /dev/sdb2 ]
  + [Cluster Partition Device Name] as [ /dev/sdb1 ]
* [Finish]

### Adding the execute resource for controlling target service

* Right click [failover-iscsi] in left pane > [Add Resource]
* Select [Type] as [execute resource] then click [Next]
* [Next]
* [Next]
* Select start.sh then click [Edit]. Add below lines.

#!/bin/bash

echo "Starting iSCSI Target"

systemctl start target

echo "Started iSCSI Target"

* Select stop.sh then click [Edit]. Add below lines.

#!/bin/bash

echo "Stopping iSCSI Target"

systemctl stop target

echo "Stopped iSCSI Target"

* [Finish]

### Adding floating IP resource for iSCSI Target

* Right click [failover-iscsi] in left pane > [Add Resource]
* Select [Type] as [floating IP resource] then click [Next]
* [Next]
* [Next]
* Set floating IP address as [ 192.168.0.10 ]
* Click [Finish]

### Adding the execute resource for automatic MD recovery

This resource is enabling more automated MD recovery by supposing the node which the failover group trying to start has latest data than the other node.

* Right click [failover-iscsi] in left pane > [Add Resource]
* Select [Type] as [execute resource], set [Name] as [exec-md-recovery] then click [Next]
* Uncheck [Follow the default dependency] > [Next]
* [Next]
* Select start.sh then click [Replace]
* Select [exec-md-recovery.pl]
* [Finish]

### Adding the custom monitor resource for automatic MD recovery

* on Cluster Manager
  + change to [Operation Mode] from [Config Mode]
  + right click [Monitors] > [Add Monitor Resource]
  + [Info] section
    - select [custom monitor] as [type] > input genw-md > [Next]
  + [Monitor (common)] section
    - input 60 as [Wait Time to Start Monitoring]
    - select [Active] as [Monitor Timing]
    - [Browse] button
      * select [md1] > [OK]
    - [Next]
  + [Monitor (special)] section
    - [Replace]
      * select genw-md.pl > [Open] > [Yes]
    - input /opt/nec/clusterpro/log/genw-md.log as [Log Output Path] > check [Rotate Log]
    - [Next]
  + [Recovery Action] section
    - select [Execute only the final action] as [Recovery Action]
    - [Browse]
      * [LocalServer] > [OK]
    - select [No operation] as [Final Action]
    - [Finish]

### Adding Monitor which make remote vMA VM and ECX keep online.

* on Cluster Manager
  + change to [Operation Mode] from [Config Mode]
  + right click [Monitors] > [Add Monitor Resource]
  + [Info] section
    - select [custom monitor] as [type] > input genw-remote-node > [Next]
  + [Monitor (common)] section
    - select [Always] as [Monitor Timing]
    - [Next]
  + [Monitor (special)] section
    - [Replace]
      * select genw-remote-node.pl > [Open] > [Yes]
    - [Edit]
      * write $VMNAME1 as VM name iscsi1 in the esxi1 inventory
      * write $VMNAME2 as VM name iscsi2 in the esxi2 inventory
      * write $VMIP1 as IP address for iscsi1
      * write $VMIP2 as IP address for iscsi2
      * write $VMK1 as IP address for esxi1 which accessible from iscsi1
      * write $VMK2 as IP address for esxi2 which accessible from iscsi2
    - input /opt/nec/clusterpro/log/genw-remote-node.log as [Log Output Path] > check [Rotate Log]
    - [Next]
  + [Recovery Action] section
    - select [Execute only the final action] as [Recovery Action]
    - [Browse]
      * [LocalServer] > [OK]
    - select [No operation] as [Final Action]
    - [Finish]

### Applying the configuration

* Click [File] > [Apply Configuration]
* Reboot iscsi1, iscsi2 and wait for the completion of starting of the cluster failover-iscsi

### Configuring iSCSI Target

On iscsi1, create fileio backstore and configure it as backstore for the iSCSI Target.

* Login to the console of iscsi1.
* Start (iSCSI) target configuration tool

# targetcli

* Unset automatic save of the configuration for safe.

> set global auto\_save\_on\_exit=false

* Create fileio backstore (idisk) which have required size on mount point of the mirror disk

> cd /backstores/fileio

> create idisk /mnt/idisk.img 500G

* Creating IQN

> cd /iscsi

> create iqn.2016-10.com.ec:1

* Assigning LUN to IQN

> cd /iscsi/iqn.2016-10.com.ec:1/tpg1/luns

> create /backstores/fileio/idisk

* Allow machine (IQN of iSCSI Initiator) to scan the iSCSI target.

> cd /iscsi/iqn.2016-10.com.ec:1/tpg1/acls

> create iqn.1998-01.com.vmware:1

> create iqn.1998-01.com.vmware:2

* Save config and exit.

> saveconfig

> exit

* Copy the saved target configuration to the other node.

# scp /etc/target/saveconfig.json iscsi2:/etc/target/

## Setting up ESXi - iSCSI Initiator

* Open [vSphere Client] and connect to esxi1
* Click ESXi host icon at the top of left pane.
* Select [Configuration] tab in right pane.
* Select [Storage Adapter] > [Add]
* Configure [iSCSI Software Adapter]
  + set WWN [iqn.1998-01.com.vmware:1] for the adapter
  + set IP address [192.168.0.10 ] for the iSCSI Target
* Select [Storage] > [Add Storage]
* Create [iSCSI] as datastore in the iSCSI Target

Do the same for esxi2. Use [iqn.1998-01.com.vmware:2] as WWN for its adapter.

## Deploying UC VMs on iSCSI datastore

* Setup a VM (to be protected by ECX) on esxi1 and name it VM1 for example. The VM should be saved on the shared storage.

## Setting up vMA Cluster

### Configuring Failover Group

* On ESXi-1 and ESXi-2
  + Deploy vMA OVF template on both ESXi and boot them.
  + Configure the network for ESXi and vMA to make communicable between vMA and VMkernel port.
    - ESXi Example:

|  | **Primary** | **Secondary** |
| --- | --- | --- |
| Hostname | esxi1 | esxi2 |
| root password | passwd1 | passwd2 |
| Management IP | 10.0.0.1 | 10.0.0.2 |

* + - vMA Example:

|  | **Primary** | **Secondary** | **Note** |
| --- | --- | --- | --- |
| 3) Hostname | vma1 | vma2 | need to be independent hostname ( "localhost" is inappropriate ) |
| 6) IP Address | 10.0.0.21 | 10.0.0.22 | need to be independent and static IP Address |

* + The IP address of vma1 and vma2 should be possible to communicate with Management IP of both ESXi and UC VM(s) to be protected.
    - Example UC VM to be protected:

| **Hostname** | **IP address** |
| --- | --- |
| vm1 | 10.0.0.101 |

* On vma1 and vma2
  + Put ECX rpm file and its license file by using scp command and so on.
  + Install ECX

> sudo bash

# rpm -ivh expresscls-3.3.3-1.x86\_64.rpm

# clplcnsc -I [license file] -P BASE33

# reboot

* Configure ECX On Cluster Manager
  + Access <http://10.0.0.21:29003/> with web browser to open Cluster Manager
  + on Cluster Manager
    - change to [Config Mode] from [Operation Mode]
    - [File] > [Cluster Generation Wizard]
    - [Start Cluster Generation Wizard for standard edition]
    - Input vMA-cluster as Cluster Name, [English] as Language > [Next]
    - [Add] > input [IP Address of secondary server] > [OK] > [Next]
    - [Next]
    - [Next]
    - [Add]
    - input failover-VMn as [Name] > [Next]
    - [Next]
    - [Next]
    - [Add]
    - Select [execute resource] as [Type] > input exec-VMn as [Name] > [Next]
    - [Next]
    - Select [Stop the cluster service and regoot OS] as [Final Action] in [Recovery Operation at Deactivation Failure Detection] > [Next]
    - Select [start.sh] > [Replace] > Select vm-start.pl >
    - [Edit] > followings need to be specified in the script.
      * the path to the VM configuration file (.vmx) as @cfg\_paths.  
        it can be obtained at vMA console as below.

$ sudo bash

# vmware-cmd --server 10.0.0.1 -U root -l

/vmfs/volumes/588b1739-87411a6f-618f-002421a9b4be/vm1/vm1.vmx

* + - * Datastore name as $datastore which the VM to be protected is stored.
      * IP addresses for VMkernel Port for both ESXi as $vmk1 and $vmk2 which is accessible from the vMA Cluster nodes.
      * IP addresses for the Cluster nodes as $vma1 and $vma2 which is used for accessing to VMkernel Port.
    - Select [stop.sh] > [Replace] > Select vm-stop.pl >
    - [Edit] > the same with start.sh need to be specified.
    - [Tuning] > [Maintenance] tab > Input /opt/nec/clusterpro/log/exec-VMn.log as [Log Output Path] > Check [Rotate Log] > [OK] > [Finish]
    - [Finish]
    - [Next]
    - [Add] > select [custom monitor] as [Type] > input genw-VMn as [Name] > [Next]
    - select [Active] as [Monitoring Timing] > [Browse] >  
      select [exec-VMn] > [OK] > [Next]
    - [Replace] > select genw-vm.pl >
    - [Edit] > Parameters in the bellows need to be specified in the script.  
      (these parameters are the same as start.sh and stop.sh of exec-VMn)
      * The path to the VM configuration file (.vmx) as @cfg\_paths.
      * IP addresses for VMkernel Port for both ESXi as $vmk1 and $vmk2 which is accessible from the vMA Cluster nodes.
      * IP addresses for the Cluster nodes as $vma1 and $vma2 which is used for accessing to VMkernel Port.
    - input /opt/nec/clusterpro/log/genw-VMn.log as [Log Output Path] >  
      Check [Rotate Log] > [Next]
    - select [Executing failover to the recovery target] > [Browse] >  
      select [failvoer-VMn] > [OK] >  
      [Finish]
    - [Finish] > [Yes]
    - [File] menu > [Apply the Configuration File]
    - **OPTIONAL**: Do the followings if iSCSI Target Cluster and vMA Cluster need to be failed over simultaneously.
      * Right click [failover-VMn] in left pane > [Add Resource]
      * Select [Type] as [execute resource] > Input [exec-VMn-datastore] as [Name] > [Next]
      * [Next]
      * [Next]
      * Select [start.sh] > [Replace] > Select [exec-vm-datastore.sh]
      * [Edit] > followings need to be specified in the start.sh.
        + the name of the failover group in iSCSI Target Cluster (e.g. failover-iscsi) as GRP.
        + GRP="failover-iscsi"
        + IP address for primary node of iSCSI Target Cluster as IP1, and for secondary node as IP2. These IP addresses should be accessible from vMA Cluster nodes.
        + IP1="10.0.0.11"
        + IP2="10.0.0.12"
      * [Tuning] > [Maintenance] tab > Input [/opt/nec/clusterpro/log/exec-VMn-datastore.log] as [Log Output Path] > Check [Rotate Log] > [OK]
      * [Finish]
      * Right click [exec-VMn] in right pane > [Properties]
      * [Dependency] tab > Uncheck [Follow the default dependency] > Click [Add] for exec-datastore > [OK]
      * [File] menu > [Apply the Configuration File]
  + on the console of both node (vma1, vma2),  
    Register root password of both ESXi to enable vmware-cmd and esxcli command accessing ESXi without password.  
    NOTE: Enclose the password with ' (single quotation). This is because if the password includes meta character for perl script such as $ (dollar mark), credstore\_admin.pl doesl not work as expected.

> sudo bash

# /usr/lib/vmware-vcli/apps/general/credstore\_admin.pl add -s 10.0.0.1 -u root -p 'passwd1'

New entry added successfully

# /usr/lib/vmware-vcli/apps/general/credstore\_admin.pl add -s 10.0.0.2 -u root -p 'passwd2'

New entry added successfully

# /usr/lib/vmware-vcli/apps/general/credstore\_admin.pl list

Server user Name

10.0.0.1 root

10.0.0.2 root

Server Thumbprint

# exit

>

* + on vma1 console, register ESXi thumbprint to use esxcli command

> sudo bash

# esxcli -s 10.0.0.1 -u root vm process list

Connect to 10.0.0.1 failed. Server SHA-1 thumbprint: AD:5C:1E:DF:E6:39:18:B8:F9:65:EE:09:5A:7C:B4:E6:90:45:DB:DC (not trusted).

# /usr/lib/vmware-vcli/apps/general/credstore\_admin.pl add -s 10.0.0.1 -t AD:5C:1E:DF:E6:39:18:B8:F9:65:EE:09:5A:7C:B4:E6:90:45:DB:DC

New entry added successfully

# exit

>

* + on vma2 console, register ESXi thumbprint to use esxcli command

> sudo bash

# esxcli -s 10.0.0.2 -u root vm process list

Connect to 10.0.0.2 failed. Server SHA-1 thumbprint: AD:5C:1E:DF:E6:39:18:B8:F9:65:EE:09:5A:7C:B4:E6:90:45:DB:DC (not trusted).

# /usr/lib/vmware-vcli/apps/general/credstore\_admin.pl add -s 10.0.0.2 -t AD:5C:1E:DF:E6:39:18:B8:F9:65:EE:09:5A:7C:B4:E6:90:45:DB:DC

New entry added successfully

# exit

>

* + on Cluster Manager
    - change to [Operation Mode] from [Config Mode]
    - [Service] menu > [Start Cluster]

### Configuring Monitor resource

* Copying public key of root user onto ESXi to enable execution of ssh command without password. ssh command is used in some scripts for the configuration.
* On vma1 console
  + copy public key of root user to esxi2

> sudo bash

# scp ~/.ssh/id\_rsa.pub 10.0.0.2:/etc/ssh/keys-root/

* + remote login to esxi2 as root user and configure ssh for remote execution from vma1.

# ssh 10.0.0.2

Password:

# cd /etc/ssh/keys-root

# cat id\_rsa.pub >> authorized\_keys

# exit

# exit

> exit

* On vma2 console (do the same for esxi1 (10.0.0.1))
  + copy public key of root user to esxi1
  + remote login to esxi1 as root user and configure ssh for remote execution from vma2.

### Adding monitor for remote ESXi iSCSI session and ESXi inventory

* on Cluster Manager
  + change to [Operation Mode] from [Config Mode]
  + right click [Monitors] > [Add Monitor Resource]
  + [Info] section
    - select [custom monitor] as [type] > input genw-remote-esxi > [Next]
  + [Monitor (common)] section
    - input 180 as [Interval]
    - input 60 as [Wait Time to Start Monitoring]
    - select [Active] as [Monitor Timing]
    - [Browse] button
      * [exec-VMn] > [OK]
    - [Server]
      * select [Select] > [Add] (adding vma1) > [OK]
    - [Next]
  + [Monitor (special)] section
    - [Replace]
      * select genw-remote-esxi.pl > [Open] > [Yes]
    - [Edit]
      * write $DatastoreName as iSCSI datastore
      * write $vmk1 as IP address for esxi1
      * write $vmk2 as IP address for esxi2
      * write $vma1 as IP address for vma1
      * write $vma2 as IP address for vma2
      * write $vmhba1 as the name of iSCSI Software Adapter on esxi1
      * write $vmhba2 as the name of iSCSI Software Adapter on esxi2
    - input /opt/nec/clusterpro/log/genw-esxi.log as [Log Output Path] > check [Rotate Log]
    - [Next]
  + [Recovery Action] section
    - select [Execute only the final action] as [Recovery Action]
    - [Browse]
      * [LocalServer] > [OK]
    - select [No operation] as [Final Action]
    - [Finish]

### Adding Network Monitor for VMn

* on Cluster Manager
  + right click [Monitors] > [Add Monitor Resource]
  + [Info] section
    - select [ip monitor] as [type] > input ipw-VMn > [Next]
  + [Monitor (common)] section
    - input 600 as [Wait Time to Start Monitoring]
    - select [Active] as [Monitor Timing]
    - [Browse] button
      * [exec-VMn] > [OK]
    - [Next]
  + [Monitor (special)] section
    - [Add]
      * input IP address of VMn (e.g. 10.0.0.101)  
        **[ Note ]** Adding NIC on vma1 and vma2 is required if the VMn belongs to the different network than vma1 and vma2. Configure the IP address for the additional NIC to have the same network address with VMn.  
        /etc/sysconfig/networking/devices/ifcfg-eth1  
        and symbolic link file  
        /etc/sysconfig/network/ifcfg-eth1  
        should be configured.
      * [OK]
    - [Next]
  + [Recovery Action] section
    - select [Executing failover to the recovery target] as [Recovery Action]
    - [Browse]
      * select [failover-VMn] > [OK]
    - [Finish]

### Adding Monitor which make remote vMA VM and ECX keep online.

* on Cluster Manager
  + change to [Operation Mode] from [Config Mode]
  + right click [Monitors] > [Add Monitor Resource]
  + [Info] section
    - select [custom monitor] as [type] > input genw-remote-node > [Next]
  + [Monitor (common)] section
    - select [Always] as [Monitor Timing]
    - [Next]
  + [Monitor (special)] section
    - [Replace]
      * select genw-remote-node.pl > [Open] > [Yes]
    - [Edit]
      * write $VMNAME1 as VM name of vma1 in the esx01 inventory
      * write $VMNAME2 as VM name of vma2 in the esx02 inventory
      * write $VMIP1 as IP address for vma1
      * write $VMIP2 as IP address for vma2
      * write $VMK1 as IP address for esxi1
      * write $VMK2 as IP address for esxi2
    - input /opt/nec/clusterpro/log/genw-remote-node.log as [Log Output Path] > check [Rotate Log]
    - [Next]
  + [Recovery Action] section
    - select [Execute only the final action] as [Recovery Action]
    - [Browse]
      * [LocalServer] > [OK]
    - select [No operation] as [Final Action]
    - [Finish]

### Applying the configuration

- [File] menu > [Apply the Configuration File]

## Setting up ESXi - VM automatic boot, Network

* Configure both ESXi to automatically boot all the nodes in vMA Cluster (vma1, vma2) and iSCSI Target Cluster (iscsi1, iscsi2) when ESXi starts.
* The network for iSCSI and Data Mirroring should use physically independent network if possible. Configure logically independent at least.
* Try to invalidate TSO, LRO and Jumbo Frame if iSCSI performance is not enough.

# Common Maintenance Tasks

## The graceful shutdown procedure for both ESXi

1. Issue cluster shutdown for the vMA Cluster.  
   Then all the UC VMs and vMA VMs are shutted down.
2. Issue cluster shutdown for the iSCSI Cluster.  
   Then both iSCSI Target VMs are shutted down.
3. Issue shutdown for both the ESXi.

## Stopping one of vMA Cluster node

* genw-remote-node in vMA Cluster periodically executes "power on" for another vMA VM. And so, "suspend" the genw-remote-node before when intentionally shutdown the vMA VM
* genw-remote-node in vMA Cluster periodically executes "starting cluster service" for another vMA VM. And so, "suspend" the genw-remote-node before when intentionally stop the cluster service.

## Deleting / Adding UC VM on vMA Cluster

Operation flow of "Deleting UC VM" then "Adding UC VM" can be used for version up operation for UC VM.

### Deleting VM

* Open Cluster Manager for vMA Cluster ( <http://10.0.0.21:29003/> )
* Change to [Config Mode] from [Operation Mode]
* In left pane, click [failover-VMn] to be deleted
* In right pane, right click [exec-VMn] > [Remove Resource] > [Yes]
* In left pane, right click [failover-VMn] > [Remove Group] > [Yes]
* [File] menu > [Apply the Configuration File]

### Adding VM

* Open Cluster Manager for vMA Cluster ( <http://10.0.0.21:29003/> )
* Change to [Config Mode] from [Operation Mode]
* Right click [Groups] in left pane > [Add Group]
* Basic Settings : Set [Name] as [failover-VMn] > [Next]
* Startup Servers : [Next]
* Group Attributes : [Next]
* Group Resources : [Add]
  + Info : Select [execute resource] as [Type] > input exec-VMn as [Name] > [Next]
  + Dependency : [Next]
  + Recovery Operation : Select [Stop the cluster service and regoot OS] as [Final Action] in [Recovery Operation at Deactivation Failure Detection] > [Next]
  + Details : Select [start.sh] > [Replace] > Select vm-start.pl >
    - [Edit] > followings need to be specified in the script.
      * the path to the VM configuration file (.vmx) as @cfg\_paths.  
        it can be obtaind at vMA console like below.

$ sudo bash

# vmware-cmd --server 10.0.0.1 -U root -l

/vmfs/volumes/588b1739-87411a6f-618f-002421a9b4be/vm1/vm1.vmx

* + - * Datastore name as $datastore which the VM to be protected is stored.
      * IP addresses for VMkernel Port for both ESXi as $vmk1 and $vmk2 which is accessible from the vMA Cluster nodes.
      * IP addresses for the Cluster nodes as $vma1 and $vma2 which is used for accessing to VMkernel Port.
  + Select [stop.sh] > [Replace] > Select vm-stop.pl >
    - [Edit] > the same with start.sh need to be specified.
    - [Tuning] > [Maintenance] tab > Input /opt/nec/clusterpro/log/exec-VMn.log as [Log Output Path] > Check [Rotate Log] > [OK]
  + [Finish]
* [Finish]
* [File] menu > [Apply the Configuration File]

# Troubleshooting

## Log Collection HOWTO

* ECX logs of vMA Cluster and iSCSI Cluster
  + Open *Cluster Manager* for iSCSI Cluster by IE

http://10.0.0.11:29003/

* + [Tool] menu > [Collect Cluster Logs] > [OK]
    - In Save dialog, input *iscsi-log.tar.gz* as File Name
  + [Save] > [Close]
  + Open *Cluster Manager* for vMA Cluster by IE

http://10.0.0.21:29003/

* + [Tool] menu > [Collect Cluster Logs] > [OK]
    - In Save dialog, input *vma-log.tar.gz* as File Name
  + [Save] > [Close]
* ESXi logs of both nodes
  + Open *vSphere Client* for esxi1 and esxi2
  + Click [Home] > [System Log] > [Export System Log]
  + [Next] > [Next] > [Finish]

# The value on this solution

* Can be built with 2 physical hosts. vSAN requires 3 or more physical hosts.
* Can be built without vSphere vCenter.
* Can be built without SAN shared storage.
* Synchronous and asynchronous replication is possible and ZERO RPO is guaranteed by synchronous replication.