InMage Scout Standard Release Notes

Version – 8.0.1 Update 7

Table: Document History

Document Version	Document Date	Remarks
1.0	March 1, 2015	Standard version
1.1	April 7, 2015	Minor update
1.2	Nov 20 ,2015	Updated CX and vContinuum MT known issues and limitations sections.
1.3	May 2, 2017	Scout Update 5 - Updated known limitation for SLES 11 - Added steps to upgrade protected P2V Windows Cluster to Scout Update 5
14	Oct 6,2017	Updated P2V Windows cluster upgrade section as per Update 6 and future update release
15	Dec 31,2018	Added link for steps to upgrade MySQL and PHP libraries in CX and RX servers.

Contents

1 Disclaimer of Warranty

InMage Systems makes no representations or warranties, either express or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

2 About this document

The purpose of the Release Notes is to communicate major changes as well as new features in this release of the Scout. It also documents known issues and their workarounds.

The 8.0.1 GA release of Scout introduces new features, enhancements to existing features, bug fixes and support for new applications and new platforms.

3 Overview

3.1 Scout

Scout Software is a continuous data protection product that allows users to asynchronously replicate their servers (physical or virtual) over LAN and/or WAN for local and/or remote recovery with near zero data loss.

The software is used by enterprises for disaster recovery (DR) and by Managed Service Providers (MSPs) to offer DR as a service (DRaaS) to their customers.

3.2 ScoutCloud RX

ScoutCloud RX is a multi-tenant portal intended for use by MSPs and end-customers with large Scout deployments to monitor the health of protected servers in a centralized fashion.

4 What's new in this release?

- Integration with Azure billing. Scout now sends a count of the number of instances protected by Scout to Azure Site Recovery, thereby allowing your usage of Scout to be tracked against your Azure bill.
- Simplified MSCS Physical servers or VMs protection and recovery through vContinuum wizard.
- Improved Configuration Server (CS) performance by optimizing memory usage.
- Bug fixes.

5 Upgrade Path

Scout 8.0.1 is a full build. User can directly upgrade from 7.x to 8.0.1 version.

5.1 Agents

Agent upgrade is supported from Scout 7.0 GA/7.1 GA/8.0 GA to Scout 8.0.1 GA. Agent upgrade is supported irrespective of updates installed.

Table 1

Base Release	Release Update	Upgrade to 8.0.1 GA Supported?
Scout 7.0 GA	Any Update	Yes
Scout 7.1 GA	Any Update	Yes
Scout 8.0. GA	Any hotfix	Yes

5.2 RX

RX upgrade is supported from Scout 7.0 GA/7.1 GA/8.0 GA to Scout 8.0.1 GA. RX upgrade is supported irrespective of updates installed.

Table 1

Base Release	Release Update	Upgrade to 8.0.1 GA Supported?
Scout 7.0 GA	Any Update	Yes
Scout 7.1 GA	Any Update	Yes
Scout 8.0 GA	Any hotfix	Yes

5.3 CX Server

CX Server upgrade is supported from 7.0 GA /7.1 GA/8.0 GA to Scout 8.0.1 GA. CX Server upgrade is supported irrespective of updates installed.

Table 2

Base Release	Release Update	Upgrade to 8.0.1 GA Supported?
Scout 7.0 GA	Any Update	Yes
Scout 7.1 GA	Any Update	Yes
Scout 8.0 GA	Any hotfix	Yes

5.4 vContinuum

vContinuum upgrade support is available from vContinuum previous releases 4.0(7.0 GA)/4.1(7.1GA)/8.0 GA to Scout 8.0.1GA. vContinuum upgrade is supported irrespective of updates installed.

Table 3

Base Release	Release Update	Upgrade to 8.0.1 GA Supported?
vContinuum 4.0(Scout 7.0 GA)	Any Update	Yes
vContinuum 4.1 (Scout 7.1 GA)	Any Update	Yes
vContinuum 8.0 GA	Any hotfix	Yes

6 Upgrade sequence

If earlier version of Scout already present, upgrade sequence should be as below.

1. Upgrade Rx (if exists)
2. Upgrade CS +PS
3. Upgrade PS (if exists separately)
4. Upgrade unified agents on secondary servers (target side)
5. Upgrade vContinuum wizard (if exists)
6. Upgrade unified agents on primary servers (source side)

7 Installation/Upgrade Instructions

Fresh deployment: Refer to InMage_Scout_Quick_Install_Guide.pdf for instructions to deploy and configure Scout components (Configuration Server(CS), Process Server (PS), Unified Agent (UA), and vContinuum) and ScoutCloud RX.
Upgrade: Refer to the upgrade section in Scout User guide.

8 Supported Platforms

Refer to Scout_Compatibility_Matrix.pdf for information on the operating system platforms on which Scout and ScoutCloud RX software can be deployed.

9 Issues Addressed

9.1 Scout vContinuum

1. For P2V scenario, when source server disk order gets changed due to reboot, for that protected server DR-Drill or Recovery operation will fail.
2. Retention logs are not getting removed when “remove VM” operation is used.
3. Change of IP fails in recovered VM when protected VM has VMXNet3.
4. vContinuum discovery takes more time in large ESX environment where lots of guest OS and ESX Clusters are present.

5. For P2V scenario, when hardware based services are present (HP services), recovered VM takes longer time to come up. It needed manual intervention to make the service start type as manual
6. On recovered Linux VM, configuration files permissions are not preserved for files like /etc/hosts, /etc/nsswitch.conf..etc
7. If source Linux server has virtual IPs, then in recovered VM, virtual IPs are not set properly.
8. Sometime in P2V scenario, recovered VM is failing to boot with the kernel panic error because vContinuum was cleaning the root data.
9. Resume protection fails in case of Windows server having EFI partition.
10. vCenter discovery fails for non-English language.
11. Remove and Recovery operation fails when vCenter credential get changed.

9.2 CX Server

1. For DR-Drill or Recovery operation of P2V, Fx job fails on copy and cause recovery to stuck at powering ON the recovered VM.
2. When one of the servers in the plan is decommissioned then it removes consistency jobs for all other servers protected in the same plan.
3. vContinuum wizard fails to show the plan details as it is unable to load the page.
4. In case of 1 to N, deletion of one pair sometimes causing Out of order for differential files.
5. Policy violation events table filling up without pruning and causes to out of memory.
6. Fx traps are not functioning as expected
7. CX does not retain the value of "Use process server NATIP address" check box.
8. Duplicate volsync processes are causing out of order differential files.
9. Addressed the Poodle Vulnerability(tagged as CVE-2014-3566 in the NVD) in Configuration Server.
10. When more than twenty replication pairs are assigned to same PS, then values of health report and bandwidth are not getting updated on Linux CS.

9.3 VX Agent

1. Data inconsistent issue on SUSE non-root volume.
2. In P2V case, recovered RHEL6UP5 64bit VM fails to boot after recovery.
3. MSCS Cluster storage validation tests fail when UA is installed on cluster nodes
4. On MSCS node sometime vxagent get crashed while booting the server.
5. When secure mode is enabled from source to PS, after sometime, replication pairs stop progressing and vxagent heartbeats will not get updated in CX.
6. When involflt driver is loaded after vxagent service starts, replication will not progress.

9.4 RX

1. Added fix to display authorized info for the respective customer.
2. Fixed XSS security issue.
3. Addressed the Poodle Vulnerability(tagged as CVE-2014-3566 in the NVD) in RX.

9.5 FX Agent

1. Fx copies non modified file to target server. With the fix Fx now copy only those files that are modified or failed to copy since last fx job run.

10 Known Issues and Limitations

10.1 CX

1. A replication pair cannot be moved from one protection plan to another.
2. On detecting a resize of a protected volume, CX sets the volume replication pair's *Resync Required* flag to *Yes* and pauses replication for that volume. This is to allow the Scout administrator to also resize the corresponding target volume. However, CX allows the administrator to resume replication without validating the target volume size. If replication is resumed without resizing the target volume appropriately, it would encounter disk write errors when attempting to write to unavailable blocks on that volume.
3. If force unregister is used on the Configuration Server, the unregister operation will be triggered but will not be validated for successful completion by the Configuration Server. If for some reason the action should fail to effect the unregister operation with Azure Site Recovery, stale registrations may continue to exist in the Azure Site Recovery vault. The user will need to contact support in order to delete the stale entries that may continue to persist in Azure Site Recovery.
4. Restore of the CS to a different server from CS backup requires to copy the certificates of the original CS server to new CS server.
5. After upgrading CX, the "Auto Refresh" check box is getting unchecked for "Protection Health", "CS/PS Health" and "Alerts and Notifications" dock of CX Dashboard. User need to set the dashboard preferences freshly.
6. "Reboot required" option is in disabled state while doing the push upgrade. User need to manually reboot the upgraded machines.
7. Standby CX is not supported on Windows CX.
8. CS and PS IP should be static. Change in CS/PS IP will break the communication between agent and CS/PS and replication pair will not progress.
9. Process Servers are not listed on Network traffic page.

10.2 Agent

1. After installing agents on all the nodes of the Microsoft cluster nodes, , if a new cluster disk is added to the nodes all the cluster nodes need reboot before protecting the disk. Without reboot, replication will be marked for "resync" on subsequent failover/failback of the newly added disk. The resync notification will be indicated on CX-UI. In this case, restart resync after rebooting all the cluster nodes.
2. Protection for dynamic disks on MSCS cluster (with Symantec Storage Foundation) is not supported.
3. When source system time jumps from point A to future time B and back to a point between A&B then, until the time on production system reaches the time > B, all recovery points will show same timestamp B. Recovery using timestamp is not supported till this event. However, you can perform recovery using bookmarks.

4. Caution is required during uninstallation of EMC PowerPath or InMage Linux agent, when both are installed on the server. The uninstallation of these should happen exactly in the reverse order in which they are loaded to avoid undesired issues.
5. Recovery ranges shown based on source machine's local time on CX UI do not have daylight saving time (DST) consideration.
6. For Windows, while replication on basic volume is in progress, converting source disk storage type from basic to dynamic would mark volume replication for resync on next reboot.
7. For Windows, while replication is in progress, format of source volume may lead to resync.
8. Source device protection of disk devices that are renamed using Linux udev rules is not supported.
9. Scout does not support protection of a volume that has character '$' in its name.
10. Mount point stale entries of recycle bin protection causes the replication progress stuck.
11. S2 process crashed when protecting more than one name to the same device.
12. Scout does not support protection of "cryptsetup" encrypted devices.
13. Protection of dev-mapper logical volumes created from disks/partitions on Linux using dmsetup is not supported.
14. System level protection for SuSE 10 & 11 requires resynchronization (restart resync) after a system reboot.
15. When protected source volume is formatted then Resync flag will be set to yes for the protection.
16. Consistency job starts failing after deletion of some of the replication pairs when Scout filter driver still tracks the changes for the deleted pairs.
17. For MSCS, if a volume is active on node 1 with drive letter say 'D', then on node 2, a newly added local disk volume takes up drive letter as 'D' causing Resync required set to yes as Scout expects 'D' to be offline on node 2.
    Workaround: Always choose unused shared drive letter for local volume.
18. For MSCS, say volume D and E are shared volumes online on node 1 and 'F' is newly added shared volume from cluster node 1. If all the volumes are failedover to node 2, the volume 'F' for some seconds comes up with drive letter 'D' on node 2. This causes Resync required set to Yes.

10.3 Fx

1. When a new Fx job is created and run immediately while any other Fx job is running on the target then newly created job may fail until existing job completes. This happens only when Fx job is set for two different machines. If source and target machines are same then issue will not occur.
2. Only Push mode is supported.
3. Fx replication between 8.0.1 agent and earlier version(<8.0) is not supported. Both source and target host should have either 8.0.1 agent or both should have earlier version of agent.

   For example Fx job between source(8.0.1 agent) and target (7.1 agent) is not supported.

10.4 Scout vContinuum MT

1. If the device order on the protected Linux virtual machine changes either due to reboot or due to reconfiguration, replication will not progress. Workaround: Remove the VM from protection and re-protect the VM.
2. Unselect "Microsoft VHD disks" while protecting Physical Machines. Protection will fail if VHD disks are selected.
3. Reverting to a VMware snapshot will require resync operation.
4. Recently added NICs shows only after 15 minutes in vContinuum wizard.
   Workaround: User can restart "Svagent(InMage Vx repliction)" service on production server.
5. At times, Windows 2008 recovered VM's RAID 5 and Mirror volumes show up as "Failed redundancy". However, data on the volume is accessible and applications will continue to start & function.

   Workaround:

   a) Open disk management, select one of the dynamic disks, right click and click on "reactivate disk".

   (or)

   b) Right-click on volume which is showing "Failed redundancy" and reactivate volume.
6. In case of cloning protected virtual machines and bringing up cloned virtual machines on same production network, replication will not progress and replication pairs will be marked for *Resync Required* to "YES".
7. Protection will fail if VM's disks are located at 0:0, 1:0, 2:0, 3:0 with same size. This would result into scsi-id mismatch issue as OS level and Host level disk comparison fails.
8. In case of Linux, if system partitions are spread across multiple disks then all disks need to be protected with a fresh protection plan. Add disk feature for system disks or having system partition is not applicable.

   Workaround: Fresh protection needs to be setup considering all system devices.
9. Linux physical-virtual or virtual-virtual workflow does not support security policies with automation.

   a) SELinux workaround: Target machine boots into maintenance mode. After passing selinux=0 in kernel boot parameters, system comes up fine. Similar change needs to be done in /boot/grub/menu.lst file for permanently fixing the problem after system boots up.

   (b) Active AppArmor security policy is not supported
10. Linux virtual to virtual workflow does not support device name schemes (i) /dev/disk/by-path (ii) /dev/disk/by-id in /etc/fstab & /boot/grub/menu.lst.
    a. If system disk uses above naming scheme, system fails to boot. Workaround: Root device should be made as /dev/sdaX in GRUB kernel entry depending on the order on source machine, where X is corresponding partition number
    b. User disk or partition in /etc/fstab with above naming scheme drops system boot process into maintenance if filesystem is auto mounted. Above device name scheme needs to be changed to appropriate device name in recovered virtual machine

    Physical to virtual does not have this limitation.
11. In Linux P2V scenario, if system disk is in LV without VG, then the system disk will not be reported to CX and vContinuum cannot protect that disk.
12. Cluster node IP's are not updated for second physical NIC in the failback recovery with error "Object already Exists".

    Workaround: Set the IP address manually.
13. With EISA partition on production, dynamic mirror volumes will be converted to simple volumes on secondary site. However, it will not have any issues for accessing the drive and all

applications will continue to work.
Workaround: Re-create mirror before trying for failback operation.

14. Resume protection failed after datastore vMotion for DR-VM as datastore vMotion caused vmdk paths and vm folder to change.
15. Import dynamic disk(s) manually if any disk(s) is/are in foreign state on recovered VM/DR-Drill VM.
16. During recovery, if recovery point is selected with specific time option from Scout vContinuum wizard and if the specified time matches with the exact tag time, recovery will happen to earlier tag.
17. Linux MT name should not contain "." else readiness check will fail while performing recovery though RX.
18. After PS failover, replication pairs will not progress in resume scenario if first process server is down.
    Workaround: If replication pairs don't progress because of PS server unavailability, user need to click on each pair-->click on settings-->choose new progress server.
19. For V2V scenario, protection of Linux VM will fail when it has LSI logic SAS controller having more than six disks.
20. Unprotected MSCS node can't be added to the existing protected cluster plan. To protect new cluster node to the existing cluster, user need to remove the existing protection and re-protect the complete cluster.
    For example one node is protected out of two node MSCS cluster and then adding second node to protection will fail. Workaround is to remove the existing protection and protect both the nodes at the same time.
21. For MSCS, after upgrading to 8.0.1, it is recommended to remove existing protection plan and create new protection plan to make avail of all the new features added in Scout 8.0.1 for MSCS. For existing MSCS protection plan after upgrading agent to 8.0.1 the limitation remain the same as that on earlier version like volume resize and add disk will have the same limitation until MSCS nodes are freshly protected.
22. Delete disk and remove volume will not be allowed for local disk/volumes of protected MSCS node.
23. Resume operation for MSCS servers may fail when recovered MSCS VMs are in the same network as that of CS.
    Workaround: Ensure recovered MSCS cluster nodes are in powered off state.
    On all source cluster nodes:
    1. Stop VX Agent service
    2. Delete these keys if they are present
    HKEY_LOCAL_MACHINE\SOFTWARE\SV Systems\ClusterTracking
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SV Systems\ClusterTracking
    3. Start VX Agent service
24. For MSCS cluster, disk deletion operation may not remove replication pairs of the volume of the disk. Workaround: Perform "Remove volume" operation from vContinuum wizard for the volumes whose pairs were not removed as part of remove disk operation.
25. When two different plans are recovered from two different MTs at the same time then it is possible that one of the plan may not be listed for resume operation.
26. Re-sizing of local disks is not supported in MSCS cluster protected machines in vContinuum.

Limitations:

1. Recovery will fail if vContinuum is installed on the same server where CX is installed. Do not install vContinuum on the server where CX is installed.

2. Hostname of the Master Target cannot exceed 15 characters.
3. Master Target should not be under a vApp pool.
4. If vContinuum wizard shows incorrect free space of datastore, close the wizard, refresh datastore from vSphere client and launch vContinuum wizard again.
5. vContinuum does not support protecting iSCSI disks directly exported to source VMs. The protection of these disks would require manual steps using Scout CS UI. However iSCSI disks directly exported to physical servers can be protected using vContinuum with P2V model.
6. vContinuum does not support protecting VMs configured to use pass-through devices (like RAW devices, tapes, etc.).
7. Target vSphere version should be either same or higher than the source vSphere server. If it is lower, it should at least support source VM OS version.
   Example: - Primary vSphere 5.1 should be protected to either version 5.1 or above
8. Windows 2012 virtual/physical machine can only be protected to ESX 5.0U1,ESX5.1 or later versions (due to VMware limitation).
9. Remote install/uninstall of InMage Scout Unified Agent on primary servers and Master Target using vContinuum is not supported for Linux.
10. For RHEL 5U3/CentOS5.3 and earlier versions, IP address on recovered VMs must be assigned manually
11. In case of 1-N protection, local backup to same production vSphere ESX is not supported.
12. InMage Offline sync folder should be in a single datastore. Offline sync folder on multiple datastores is not supported.
13. McAfee anti-virus version 8.8 should not be installed on Master Target. However, other versions of McAfee anti-virus can be installed on Master target.
14. EFI with dynamic disks cannot be protected using vContinuum.
15. DR-Drill with array based snapshot works only with storage arrays having Virtual LUN Copy feature. Check with your vendor whether your storage system supports this feature or not.
16. At times, change in network configuration for Windows server may fail in recovery. User needs to manually set network configuration (IP, subnet, DNS).
17. Linux workflow does not support UEFI disk partitioning layout.
18. At times, P2V of Linux shows "Operating system not found".
    Work around: Swap the disks to boot properly at vSphere level by using "Edit settings" option on vSphere Client UI.
19. When source is Windows 2012 R2 then MT should be Windows 2012 R2. If MT is running on windows 2012, it has incompatibility issue with loading system registry hive to make configuration changes on MT machine and recovery will fail with "error loading registry hive".
    Workaround: Manually change the IP of recovered VM.
20. In case of local backup (Both production and DR VM) on same ESX server, failback is not supported.
21. A partition without a driver letter or mount point cannot be protected using vContinuum.
22. For Linux V2V, recovered VM can potentially run into maintenance mode if all source disks are not protected.
23. When protected dynamic disk volume (example G: volume) is removed and new dynamic disk from the same machine is added for protection then vContinuum again protects G: volume.
    Workaround: After pair creation, perform remove volume(G: volume).
24. When CX, vContinuum and MT are upgraded to 8.0.1 and if source side agent is not upgraded, then addition of disk and volume resize operations will fail. Workaround: upgrade agent as well to 8.0.1.
25. DR-Drill operation will fail when source and MT VMs have the same disk signatures and it generally happens when both the VMs are prepared from the VM template.

Workaround: Change the disk signature of MT local disks.

26. MSCS cluster IP change is not supported by vContinuum wizard. User need to manually update cluster network setting on recovered VMs.
27. During recovery, newly assigned IP may not be set to one of the NIC of recovered MSCS VM. In this case user has to manually assign the IP to the NIC.
28. Array based snapshot DR-Drill is not supported at ESX level when ESX is connected to vCenter.
29. ASR Scout does not support non-English OS.
30. VMware VM with Paravirtual scsi controller is not supported.
31. Enabling of UUIDs is a pre-requisite for enabling V2V protection. UUID property created inside the VM should be enabled from vSphere/vCenter.
32. At the time of MSCS Cluster recovery, all the cluster nodes need to be selected for recovery. Partial recovery of cluster nodes is not supported.
33. When new disk is added to a MSCS Cluster, then ensure that drive letter assigned to it is not present in any of the cluster nodes. Otherwise, volume re-size will be triggered by vContinuum as the newly assigned drive letter matches with the existing protected volumes but with different volume size.

10.5 ScoutCloud RX

1. The protection status information at RX may vary with that of CX because of periodic data synchronization.
2. When the vContinuum setup is having multiple IPs, the recovery readiness check might fail if the vContinuum IP address is provided instead of hostname. Hostname can be provided to resolve this.
3. The information in the RPO/Data change graphs is limited to last 7 days.
4. The RPO graph for a protected server will be empty on the first day of the protection
5. Shared folders are not being shown in shared documents tab and only the files are getting listed.
6. Only three health factors "RPO Health", "Retention Health" and “Resync Health” are considered while showing the Protection status at RX. Other health factors are not considered.
7. After upgrade, if CX synchronization mode is changed from PULL to PUSH, synchronization may not happen. Workaround: unregister and register CX back with Rx.
8. When only RX is upgraded to 8.0.1 but CX is not upgraded, bandwidth report value shows as zero. Workaround: Upgrade CX to 8.0.1
9. When RX is upgraded and CX and MT are not upgraded then recovery through RX will fail. Workaround: upgrade CX and MT to 8.0.1
10. Specify tag option is not available in RX while doing recovery. User has to use vContinuum wizard for this option.
11. If force unregister is used on Scout Cloud RX Server, the unregister operation will be triggered but will not be validated for successful completion by the RX Server. If for some reason the action should fail to affect the unregister operation with Azure Site Recovery, stale registrations may continue to exist in the Azure Site Recovery vault. The user will need to contact support in order to delete the stale entries that may continue to persist in Azure Site Recovery.
12. Protection and recovery plan should not contain any space. If space is present, recovery through RX will fail.

11 Sizing guideline for CS/PS/MT

The recommended system requirements for CS, PS and MT VMs vary depending on several factors including the rate of data change rates of primary server, bandwidth, retention requirement, hardware make and model, etc. Refer to section 7 'Sizing Guideline' of ASR Scout Quick Install Guide to learn more about the CS, PS, MT VM size**.**

12 Upgrade protected P2V Windows Cluster to Scout Update5 or above

Manual steps required for upgrading Windows Cluster protected in P2V mode using Scout 8.0.1 Update 4 or earlier version to Scout 8.0.1 Update5 or above version.

Since all the updates installer are cumulative, it contains all the previous update fixes. This upgrade steps for P2V Windows Cluster is applicable if you are upgrading your source from Scout Update4 or earlier to Update5 or above. For example, latest Scout update version is Update6. The below steps are still applied when you upgrade your servers from Scout Update4 or earlier version to Scout Update6. If you have protected your physical Windows Cluster with Scout update 5 then you don't need these upgrade steps.

In Scout 8.0.1 Update5, the disk names format is changed for P2V clusters. Because of this the P2V Cluster protections that are already enabled using Scout 8.0.1 Update 4 or earlier version should follow the following sequence of steps to avail the cluster fixes that are added in Scout Update5 or above.

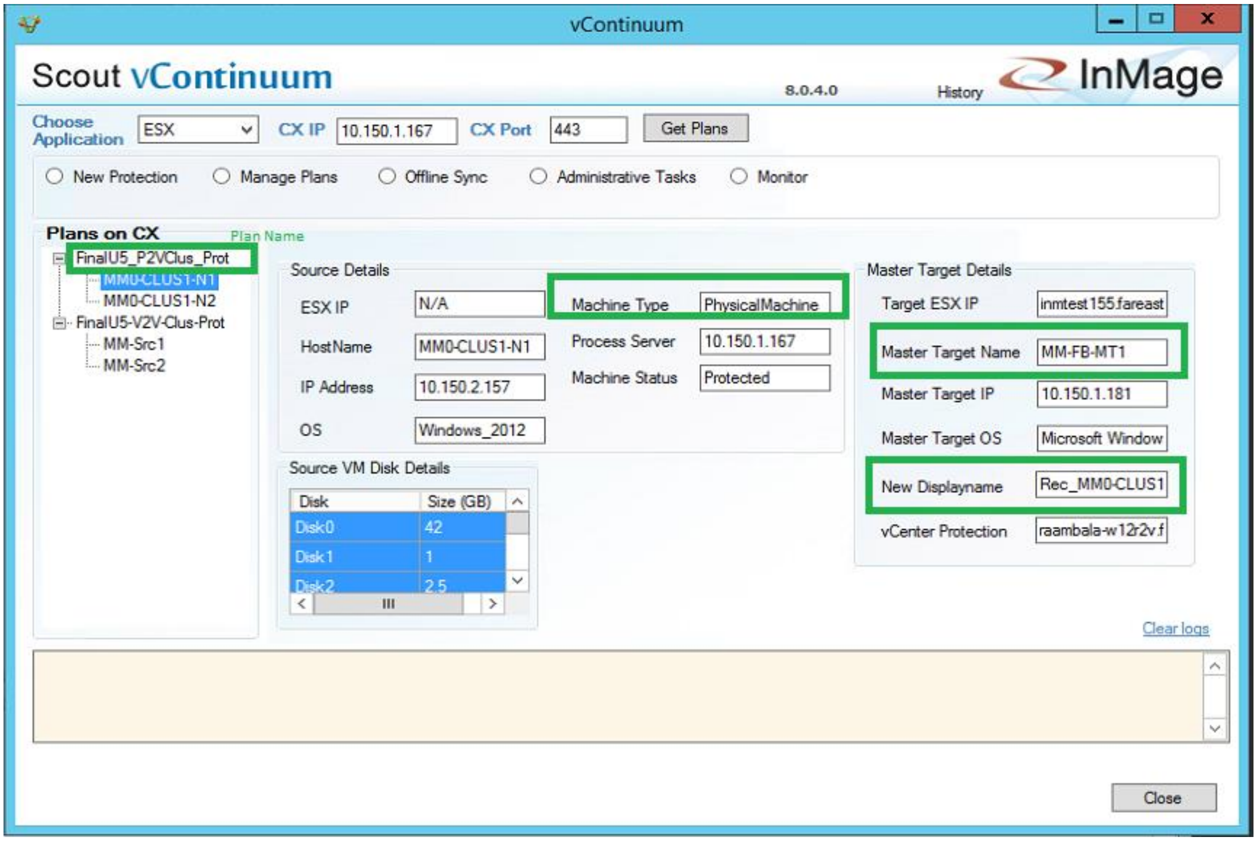
12.1 When do you need to use these manual steps?

If any of the following is true, you need to perform the manual steps before upgrading to Update5.

a) If you want to re-protect physical cluster and want to re-use the existing target disk.
b) If you want to add new cluster disk to the existing protection (protected in P2V mode)
c) If you plan to remove a protected disk from the plan

12.2 Manual Steps

1. From the vContinuum user interface, note the plan names which have protected MSCS clusters in P2V mode. You will know that a plan is protected in P2V mode if the "Machine Type" is "Physical Machine". Also, note the Master Target Name from the "Master Target Name" field as shown in the below figure.



vContinuum

Scout vContinuum 8.0.4.0 History InMage

Choose Application: ESX   CX IP: 10.150.1.167   CX Port: 443   Get Plans

○ New Protection   ○ Manage Plans   ○ Offline Sync   ○ Administrative Tasks   ○ Monitor

Plans on CX   Plan Name

- FinalU5_P2VClus_Prot
  - MM0-CLUS1-N1
  - MM0-CLUS1-N2
- FinalU5-V2V-Clus-Prot
  - MM-Src1
  - MM-Src2

Source Details

ESX IP: N/A
HostName: MM0-CLUS1-N1
IP Address: 10.150.2.157
OS: Windows_2012
Machine Type: PhysicalMachine
Process Server: 10.150.1.167
Machine Status: Protected

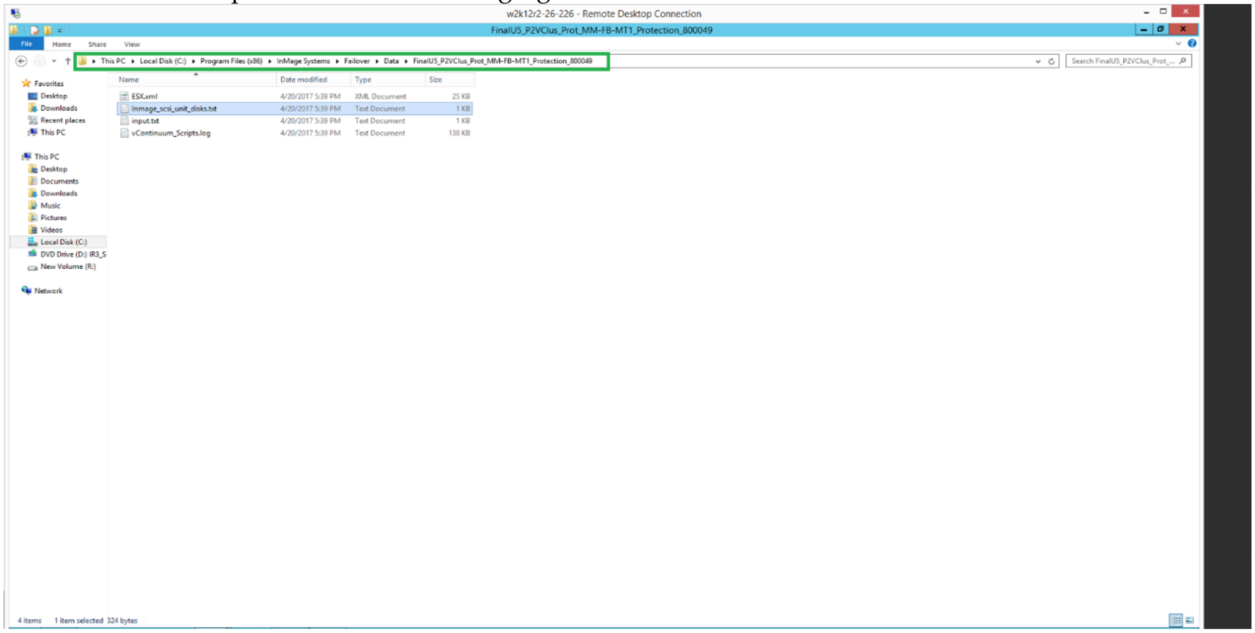
Master Target Details

Target ESX IP: inmtest155.fareast
Master Target Name: MM-FB-MT1
Master Target IP: 10.150.1.181
Master Target OS: Microsoft Window
New Displayname: Rec_MM0-CLUS1
vCenter Protection: raambala-w12r2v.f

Source VM Disk Details

Disk	Size (GB)
Disk0	42
Disk1	1
Disk2	2.5

2. For each MSCS Cluster that is protected in P2V mode, note the plan names as stated in above step and create a folder called U5\<plan_name> under <Inmage Installation Folder>\vContinuum folder.
   See the Plan Name path from the following figure.



w2k12r2-26-226 - Remote Desktop Connection

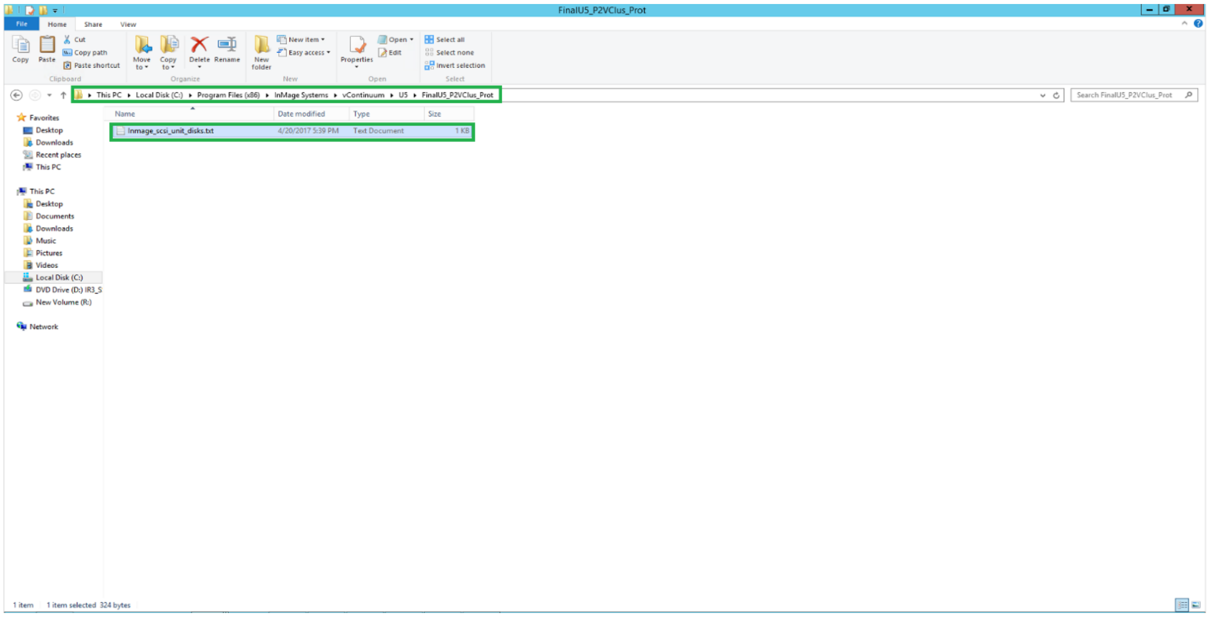
FinalU5_P2VClus_Prot_MM-FB-MT1_Protection_800049

This PC ▸ Local Disk (C:) ▸ Program Files (x86) ▸ InMage Systems ▸ Failover ▸ Data ▸ FinalU5_P2VClus_Prot_MM-FB-MT1_Protection_800049

Name	Date modified	Type	Size
ESX.xml	4/20/2017 5:39 PM	XML Document	25 KB
Inmage_scsi_unit_disks.txt	4/20/2017 5:39 PM	Text Document	1 KB
input.txt	4/20/2017 5:39 PM	Text Document	1 KB
vContinuum_Scripts.log	4/20/2017 5:39 PM	Text Document	138 KB

4 items   1 item selected 324 bytes

3. Now copy the <InMage Installation Folder>\Failover\Data\<plan_name_folder>\Inmage_scsi_unit_disks.txt file to <InMage Installation Folder>\vContinuum\U5\<plan_name_folder> as show in the figure below.

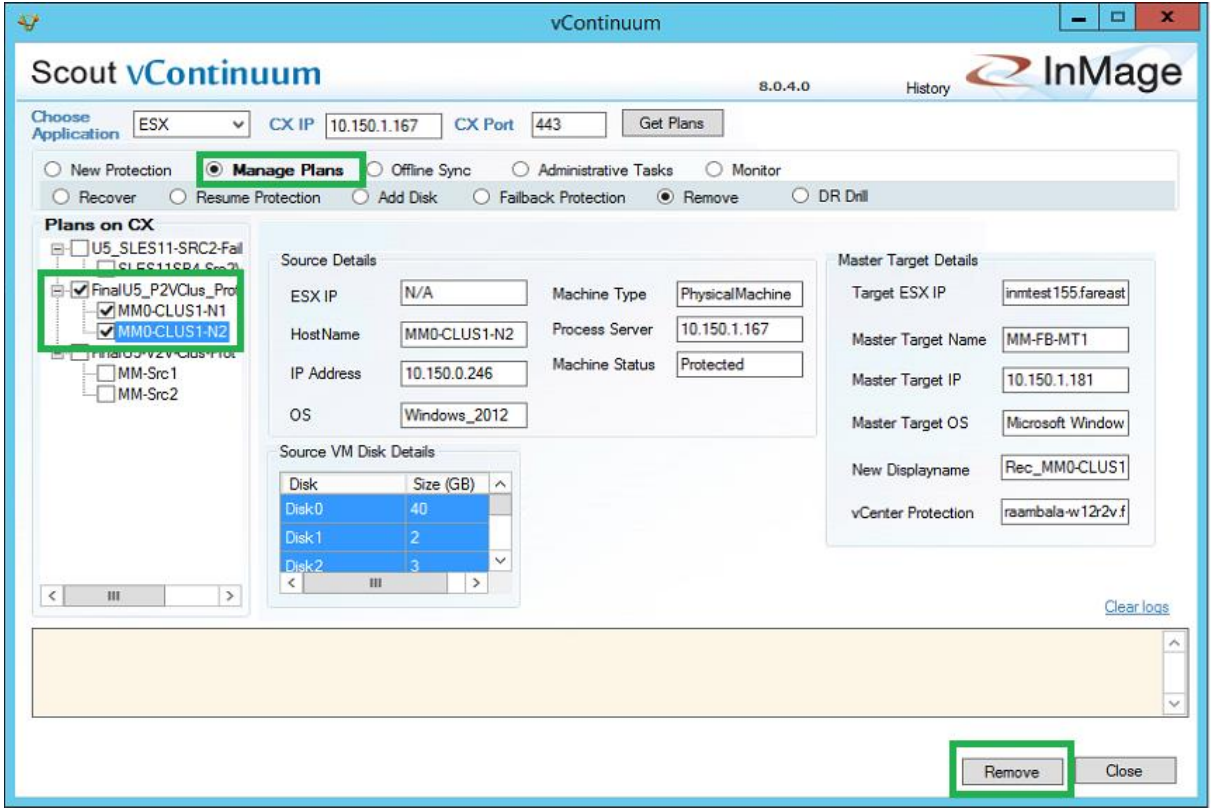


This PC ▸ Local Disk (C:) ▸ Program Files (x86) ▸ InMage Systems ▸ vContinuum ▸ U5 ▸ FinalU5_P2VClus_Prot

Name	Date modified	Type	Size
Inmage_scsi_unit_disks.txt	4/20/2017 5:39 PM	Text Document	1 KB

1 item 1 item selected 324 bytes

4. Remove protection of this plan from vContinuum UI as shown below.



Choose Application: ESX CX IP: 10.150.1.167 CX Port: 443

○ New Protection ● Manage Plans ○ Offline Sync ○ Administrative Tasks ○ Monitor

○ Recover ○ Resume Protection ○ Add Disk ○ Failback Protection ● Remove ○ DR Drill

Plans on CX
- □ U5_SLES11-SRC2-Fail
  - □ SLES11SP4-Src2\
- ☑ FinalU5_P2VClus_Prot
  - ☑ MM0-CLUS1-N1
  - ☑ MM0-CLUS1-N2
- □ FinalU5-V2V-Clus-Prot
  - □ MM-Src1
  - □ MM-Src2

Source Details

ESX IP	N/A	Machine Type	PhysicalMachine
HostName	MM0-CLUS1-N2	Process Server	10.150.1.167
IP Address	10.150.0.246	Machine Status	Protected
OS	Windows_2012		

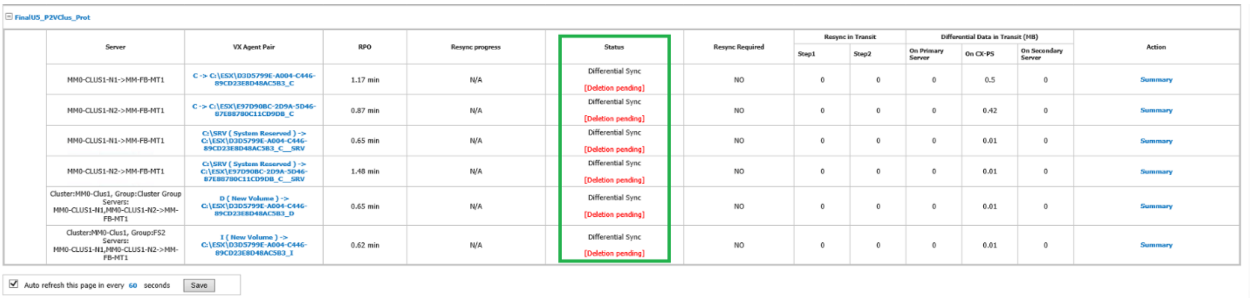
Source VM Disk Details

Disk	Size (GB)
Disk0	40
Disk1	2
Disk2	3

Master Target Details

Target ESX IP	inmtest155.fareast
Master Target Name	MM-FB-MT1
Master Target IP	10.150.1.181
Master Target OS	Microsoft Window
New Displayname	Rec_MM0-CLUS1
vCenter Protection	raambala-w12r2v.f

5. Observe that the protections of disks under this plan are being removed from the CX UI.

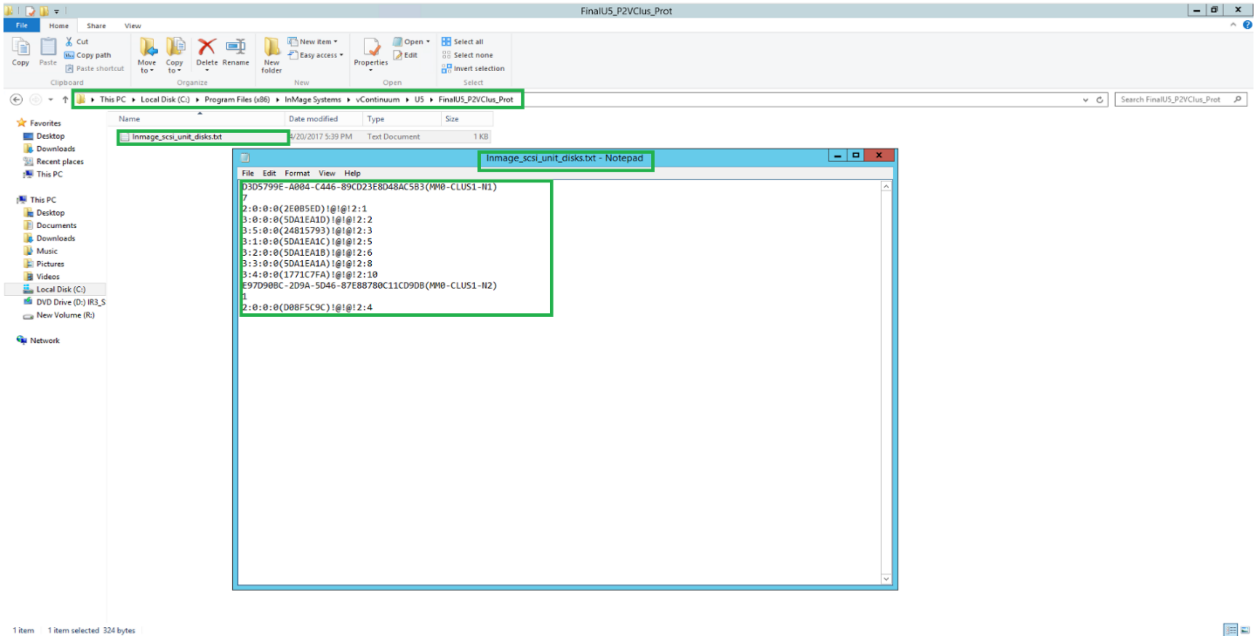


FinalU5_P2VClus_Prot

Server	VX Agent Pair	RPO	Resync progress	Status	Resync Required	Resync in Transit		Differential Data in Transit (MB)			Action
						Step1	Step2	On Primary Server	On CX-PS	On Secondary Server	
MM0-CLUS1-N1->MM-FB-MT1	C -> C:\ESX\D3D5799E-A004-C446-89CD23E8D48AC5B3_C	1.17 min	N/A	Differential Sync [Deletion pending]	NO	0	0	0	0.5	0	Summary
MM0-CLUS1-N2->MM-FB-MT1	C -> C:\ESX\E97D90BC-2D9A-5D46-87E88780C11CD9DB_C	0.87 min	N/A	Differential Sync [Deletion pending]	NO	0	0	0	0.42	0	Summary
MM0-CLUS1-N1->MM-FB-MT1	C:\SRV (System Reserved) -> C:\ESX\D3D5799E-A004-C446-89CD23E8D48AC5B3_C__SRV	0.65 min	N/A	Differential Sync [Deletion pending]	NO	0	0	0	0.01	0	Summary
MM0-CLUS1-N2->MM-FB-MT1	C:\SRV (System Reserved) -> C:\ESX\E97D90BC-2D9A-5D46-87E88780C11CD9DB_C__SRV	1.48 min	N/A	Differential Sync [Deletion pending]	NO	0	0	0	0.01	0	Summary
Cluster:MM0-Clus1, Group:Cluster Group Servers: MM0-CLUS1-N1,MM0-CLUS1-N2->MM-FB-MT1	D (New Volume) -> C:\ESX\D3D5799E-A004-C446-89CD23E8D48AC5B3_D	0.65 min	N/A	Differential Sync [Deletion pending]	NO	0	0	0	0.01	0	Summary
Cluster:MM0-Clus1, Group:FS2 Servers: MM0-CLUS1-N1,MM0-CLUS1-N2->MM-FB-MT1	I (New Volume) -> C:\ESX\D3D5799E-A004-C446-89CD23E8D48AC5B3_I	0.62 min	N/A	Differential Sync [Deletion pending]	NO	0	0	0	0.01	0	Summary

☑ Auto refresh this page in every 60 seconds Save

6. Open the Inmage_scsi_unit_disks.txt file from the new folder created in step 3 above.



This PC ▸ Local Disk (C:) ▸ Program Files (x86) ▸ InMage Systems ▸ vContinuum ▸ U5 ▸ FinalU5_P2VClus_Prot

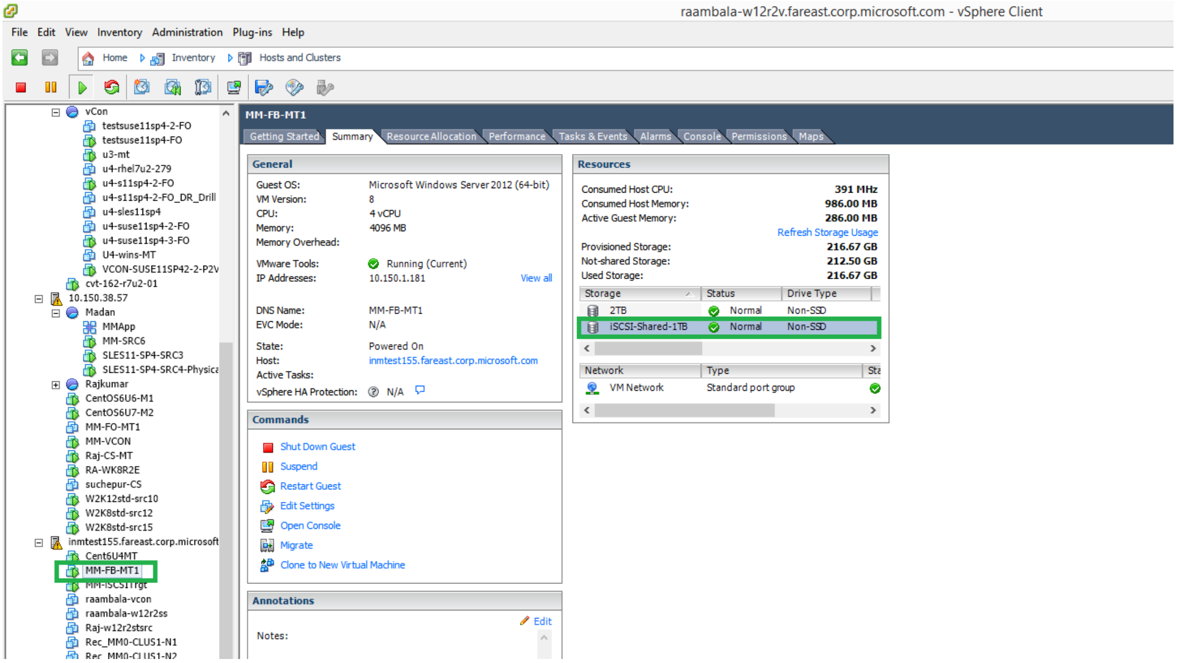
Name	Date modified	Type	Size
Inmage_scsi_unit_disks.txt	4/20/2017 5:39 PM	Text Document	1 KB

Inmage_scsi_unit_disks.txt - Notepad

```
D3D5799E-A004-C446-89CD23E8D48AC5B3(MM0-CLUS1-N1)
7
2:0:0:0(2E0B5ED)!@!@!2:1
3:0:0:0(5DA1EA1D)!@!@!2:2
3:5:0:0(24815793)!@!@!2:3
3:1:0:0(5DA1EA1C)!@!@!2:5
3:2:0:0(5DA1EA1B)!@!@!2:6
3:3:0:0(5DA1EA1A)!@!@!2:8
3:4:0:0(1771C7FA)!@!@!2:10
E97D90BC-2D9A-5D46-87E88780C11CD9DB(MM0-CLUS1-N2)
1
2:0:0:0(D08F5C9C)!@!@!2:4
```

1 item 1 item selected 324 bytes

7. Go to the target vCenter where the Master Target is present and identify the datastore where the Master Target's disks are protected.



raambala-w12r2v.fareast.corp.microsoft.com - vSphere Client

MM-FB-MT1

General

Guest OS: Microsoft Windows Server 2012 (64-bit)
VM Version: 8
CPU: 4 vCPU
Memory: 4096 MB
Memory Overhead:
VMware Tools: Running (Current)
IP Addresses: 10.150.1.181
DNS Name: MM-FB-MT1
EVC Mode: N/A
State: Powered On
Host: inmtest155.fareast.corp.microsoft.com
Active Tasks:
vSphere HA Protection: N/A

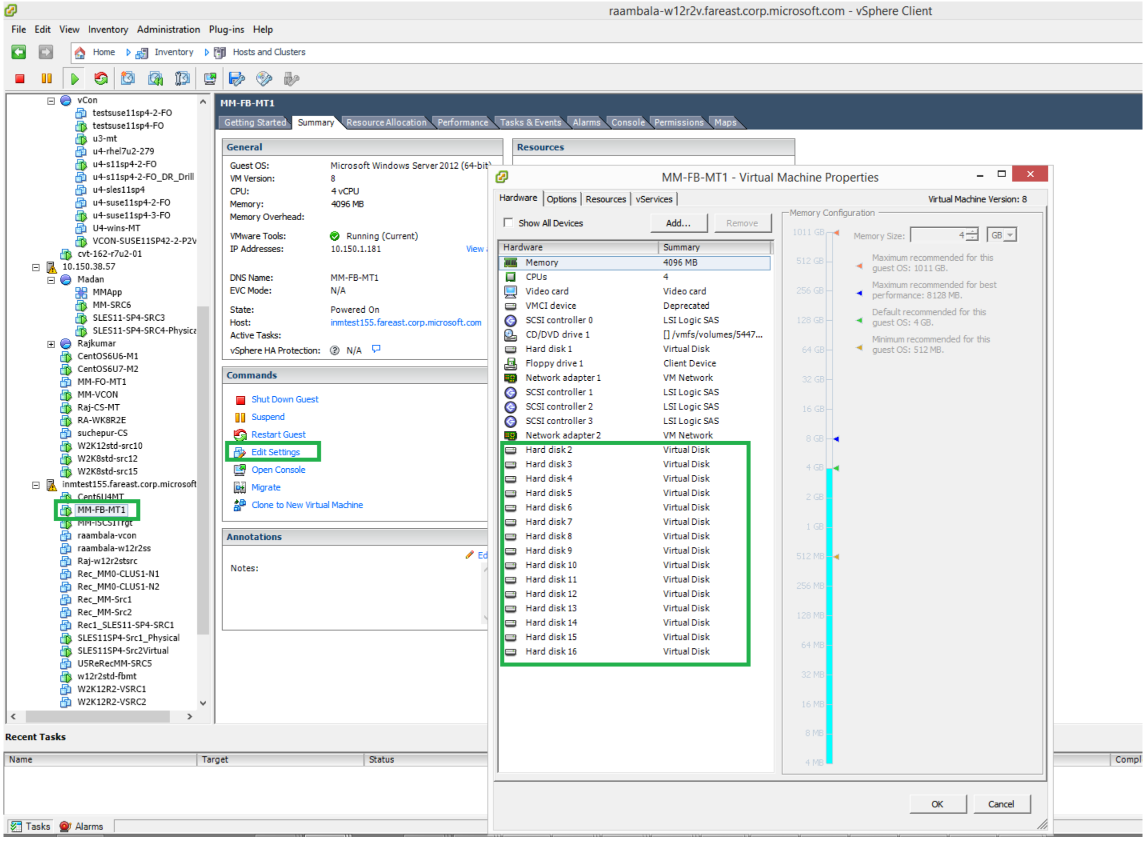
Resources

Consumed Host CPU: 391 MHz
Consumed Host Memory: 986.00 MB
Active Guest Memory: 286.00 MB
Provisioned Storage: 216.67 GB
Not-shared Storage: 212.50 GB
Used Storage: 216.67 GB

Storage	Status	Drive Type
2TB	Normal	Non-SSD
iSCSI-Shared-1TB	Normal	Non-SSD

Network	Type
VM Network	Standard port group

8. Note the Master Target's disks in the target vCenter.


raambala-w12r2v.fareast.corp.microsoft.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
MM-FB-MT1
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps
Commands
Shut Down Guest
Suspend
Restart Guest
Edit Settings
Open Console
Migrate
Clone to New Virtual Machine
Annotations
Notes:
Recent Tasks
Name Target Status
Tasks Alarms
MM-FB-MT1 - Virtual Machine Properties
Hardware Options Resources vServices
Show All Devices
Add...
Remove
OK
Cancel

General

Guest OS: Microsoft Windows Server 2012 (64-bit)
VM Version: 8
CPU: 4 vCPU
Memory: 4096 MB
Memory Overhead:
VMware Tools: Running (Current)
IP Addresses: 10.150.1.181
DNS Name: MM-FB-MT1
EVC Mode: N/A
State: Powered On
Host: inmtest155.fareast.corp.microsoft.com
Active Tasks:
vSphere HA Protection: N/A

Virtual Machine Version: 8

Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
CD/DVD drive 1	[] /vmfs/volumes/5447...
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VM Network
SCSI controller 1	LSI Logic SAS
SCSI controller 2	LSI Logic SAS
SCSI controller 3	LSI Logic SAS
Network adapter 2	VM Network
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Hard disk 5	Virtual Disk
Hard disk 6	Virtual Disk
Hard disk 7	Virtual Disk
Hard disk 8	Virtual Disk
Hard disk 9	Virtual Disk
Hard disk 10	Virtual Disk
Hard disk 11	Virtual Disk
Hard disk 12	Virtual Disk
Hard disk 13	Virtual Disk
Hard disk 14	Virtual Disk
Hard disk 15	Virtual Disk
Hard disk 16	Virtual Disk

Memory Configuration

Memory Size: 4 GB

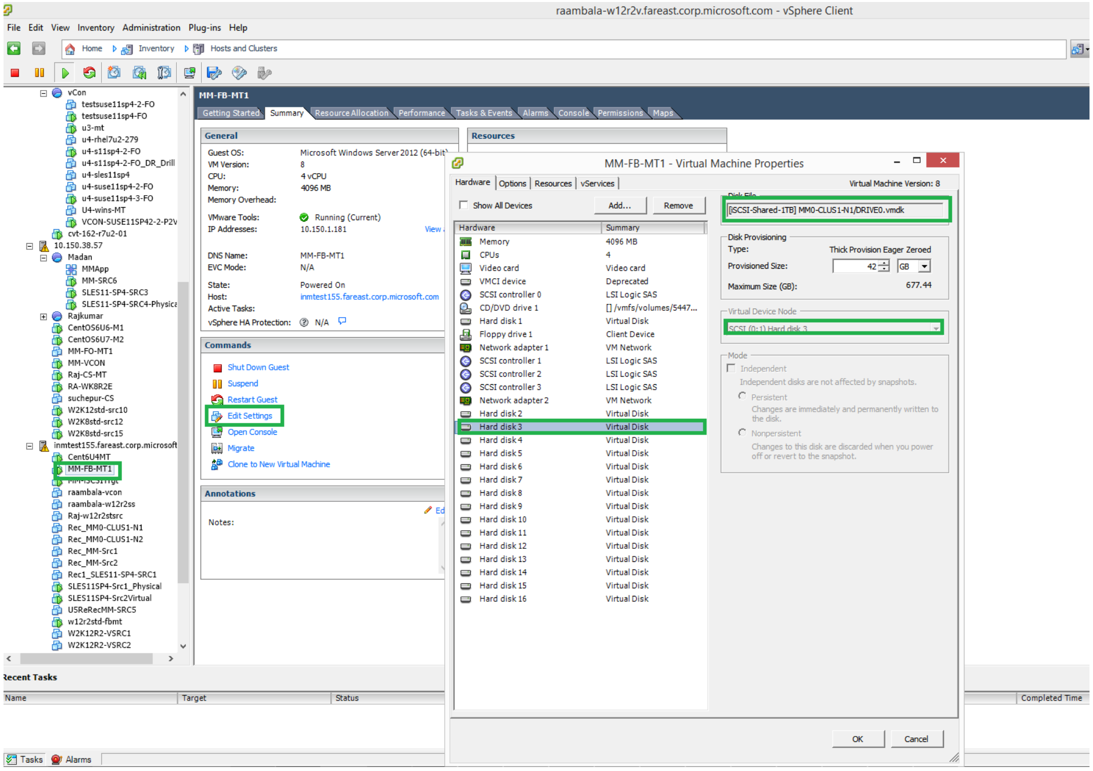
Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 8128 MB.

Default recommended for this guest OS: 4 GB.

Minimum recommended for this guest OS: 512 MB.

9. Note the path of the disks that are protected under MT as shown below.


raambala-w12r2v.fareast.corp.microsoft.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
MM-FB-MT1
Edit Settings
MM-FB-MT1 - Virtual Machine Properties
Hardware Options Resources vServices
Show All Devices
Add...
Remove
OK
Cancel

Hard disk 3 — Virtual Disk

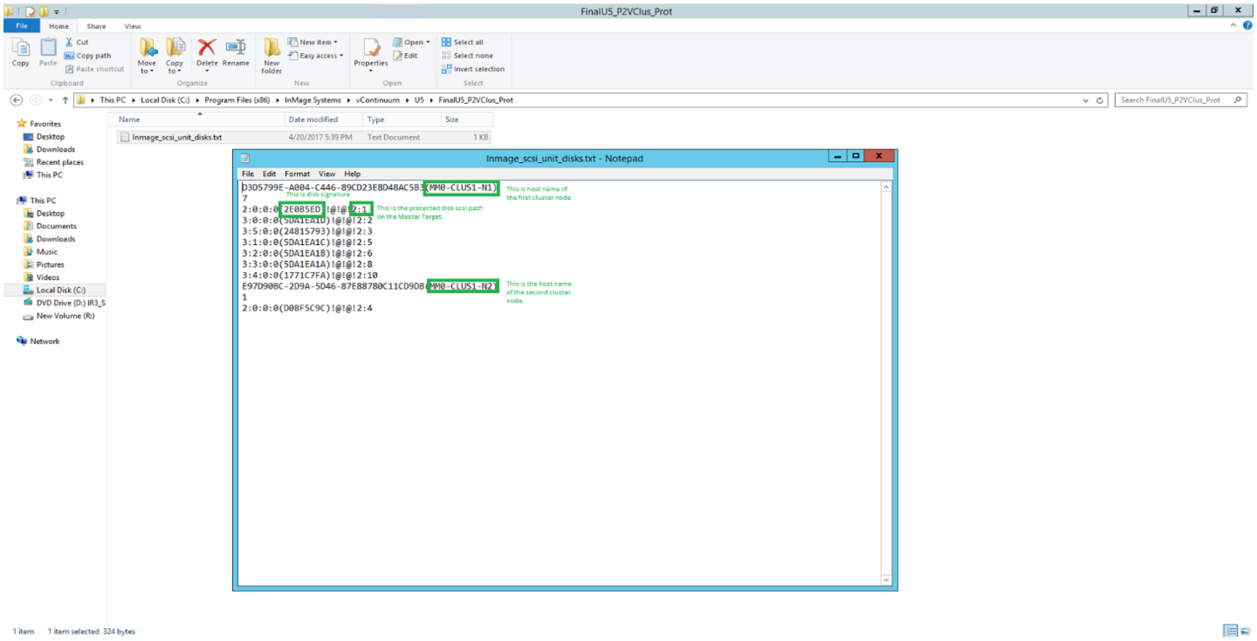
Disk File: [iSCSI-Shared-1TB] MM0-CLUS1-N1/DRIVE0.vmdk

Disk Provisioning
Type: Thick Provision Eager Zeroed
Provisioned Size: 42 GB
Maximum Size (GB): 677.44

Virtual Device Node: SCSI (0:1) Hard disk 3

Mode
☐ Independent
Independent disks are not affected by snapshots.
○ Persistent
Changes are immediately and permanently written to the disk.
○ Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.

10. Note the SCSI path of the protected disk in Master Target which is 0:1 in the figure shown above. These two values represent the SCSI controller and SCSI Target in the target ESX Host. Increment the SCSI Controller value by 2. Currently the SCSI Controller value is 0 and if you increment it by 2, it will be come 0 + 2 = 2. Now the SCSI path of this Master Target disk becomes 2:1. Now open the Inmage_scsi_unit_disks.txt file as shown in step 6 above and identify the row where the scsi path 2:1 is present. If you see the example SCSI unit disks text file that have chosen in step 6, it will match with the row
2:0:0:0(2E0B5ED)!@!@!2:1.
This file represents the mapping of the SCSI tuple of protected physical source disk with that of the protected target disk on the Master Target. The source and target SCSI tuple is separated by the symbols !@!@!. The value on the left side of this symbol represents the scsi tuple of the protected source disk and that on the right side represents the scsi tuple of the protected target disk on Master Target. The one within the parenthesis is the disk signature. In the current example it is **2E0B5ED.** Observe the following diagram.



```
D3D5799E-A004-C446-89CD23E8D48AC5B3(MM0-CLUS1-N1)
7
2:0:0:0(2E0B5ED)!@!@!2:1
3:0:0:0(5DA1EA1D)!@!@!2:2
3:5:0:0(24815793)!@!@!2:3
3:1:0:0(5DA1EA1C)!@!@!2:5
3:2:0:0(5DA1EA1B)!@!@!2:6
3:3:0:0(5DA1EA1A)!@!@!2:8
3:4:0:0(1771C7FA)!@!@!2:10
E97D90BC-2D9A-5D46-87E88780C11CD9DB(MM0-CLUS1-N2)
1
2:0:0:0(D08F5C9C)!@!@!2:4
```

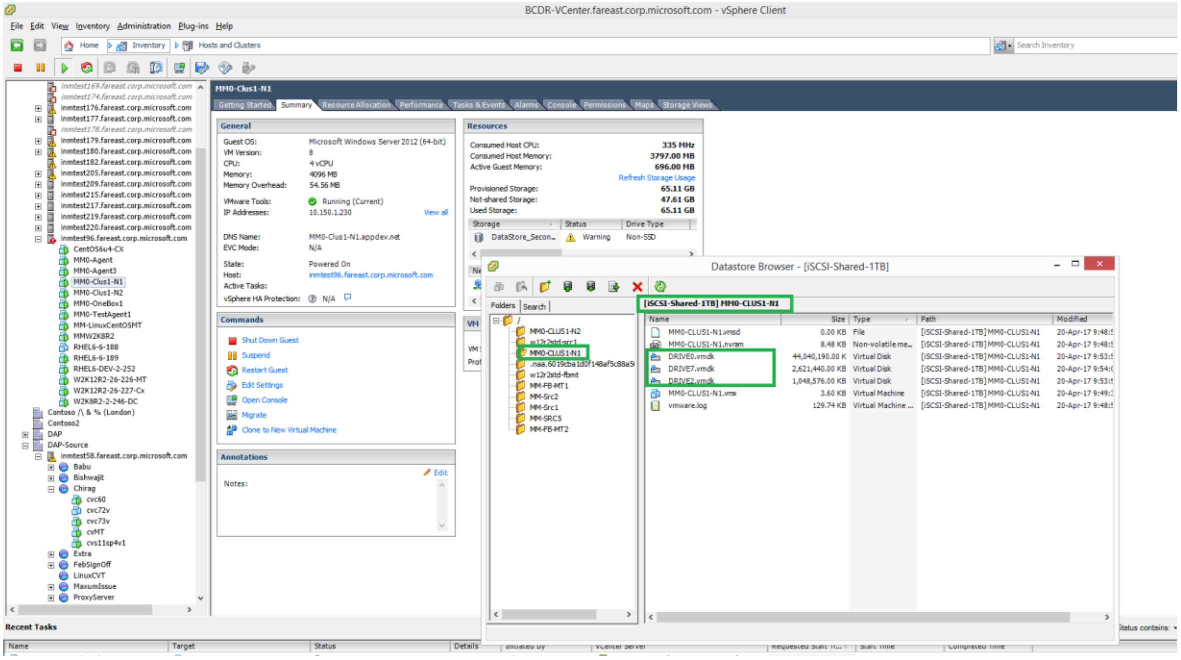
This is host name of the first cluster node

This is disk signature

This is the protected disk scsi path on the Master Target.

This is the host name of the second cluster node.

11. Now from the above diagram go to the protected target disk path in the target data store. This path is obtained from the step 9 shown above.



General

Guest OS: Microsoft Windows Server 2012 (64-bit)
VM Version: 8
CPU: 4 vCPU
Memory: 4096 MB
Memory Overhead: 54.56 MB
VMware Tools: Running (Current)
IP Addresses: 10.150.1.230
DNS Name: MM0-Clus1-N1.appdev.net
EVC Mode: N/A
State: Powered On
Host: inmtest96.fareast.corp.microsoft.com
Active Tasks:
vSphere HA Protection: N/A

Resources

Consumed Host CPU: 335 MHz
Consumed Host Memory: 3797.00 MB
Active Guest Memory: 696.00 MB
Provisioned Storage: 65.11 GB
Not-shared Storage: 47.61 GB
Used Storage: 65.11 GB

Storage	Status	Drive Type
DataStore_Secon...	Warning	Non-SSD

Datastore Browser - [iSCSI-Shared-1TB]

[iSCSI-Shared-1TB] MM0-CLUS1-N1

Name	Size	Type	Path	Modified
MM0-CLUS1-N1.vmsd	0.00 KB	File	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Apr-17 9:48:5
MM0-CLUS1-N1.nvram	8.48 KB	Non-volatile me...	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Apr-17 9:48:5
DRIVE0.vmdk	44,040,190.00 K	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Apr-17 9:53:5
DRIVE7.vmdk	2,621,440.00 KB	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Apr-17 9:54:0
DRIVE2.vmdk	1,048,576.00 KB	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Apr-17 9:53:5
MM0-CLUS1-N1.vmx	3.60 KB	Virtual Machine	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Apr-17 9:49:3
vmware.log	129.74 KB	Virtual Machine ...	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Apr-17 9:48:5

12. Now rename vmdk file in the format as given below….
    <Source Host Name>_<Source Disk Signature>.vmdk
    So the disk **[iSCSI-Shared-1TB] MM0-CLUS1-N1\DRIVE0.vmdk** should be renamed as **[iSCSI-Shared-1TB] MM0-CLUS1-N1\MM0-CLUS1-N1_2E0B5ED.vmdk**.
    This renaming can be done by opening the Target ESX Shell and executing the following command from the path **/vmfs/volumes/<datastore name>/<Host Folder Name>.**
    The command to rename the vmdk file as described above is …

    vmkfstools -E <old vmdk file with name> <new vmdk file name>

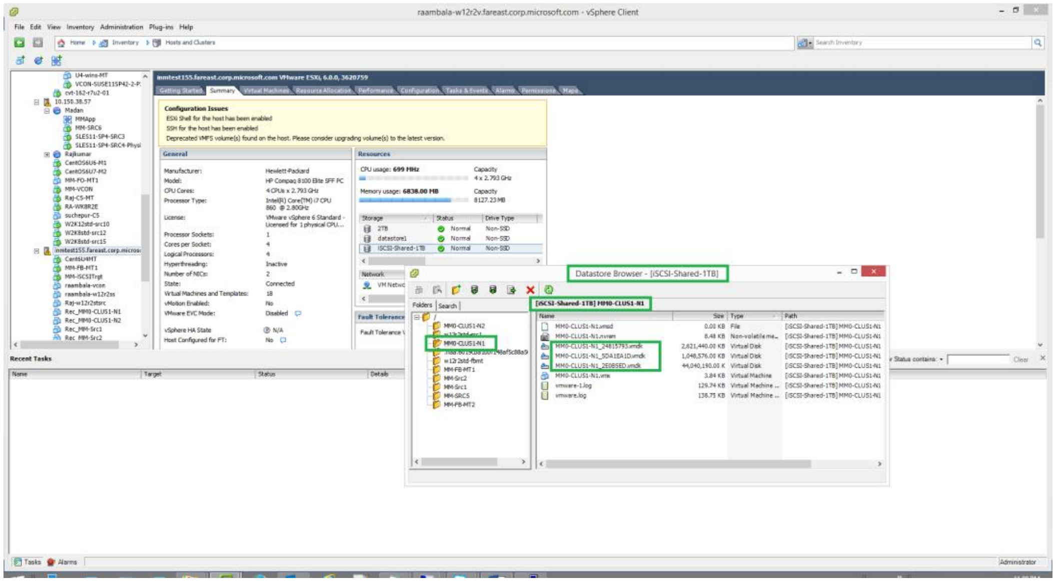
    Example:

    1. Go to the path /vmfs/volumes/iSCIS-Shared-1TB/MM0-CLUS1-N1

    2. Rename the vmdk file DRIVE0.vmdk like this…

    vmkfstools -E DRIVE0.vmdk MM0-CLUS1-N1_2E0B5ED.vmdk

Like this rename for all the protected disks of MSCS cluster protected in P2V mode.
After renaming the target ESX datastore .vmdk files name in the new format and it would show up as shown below.

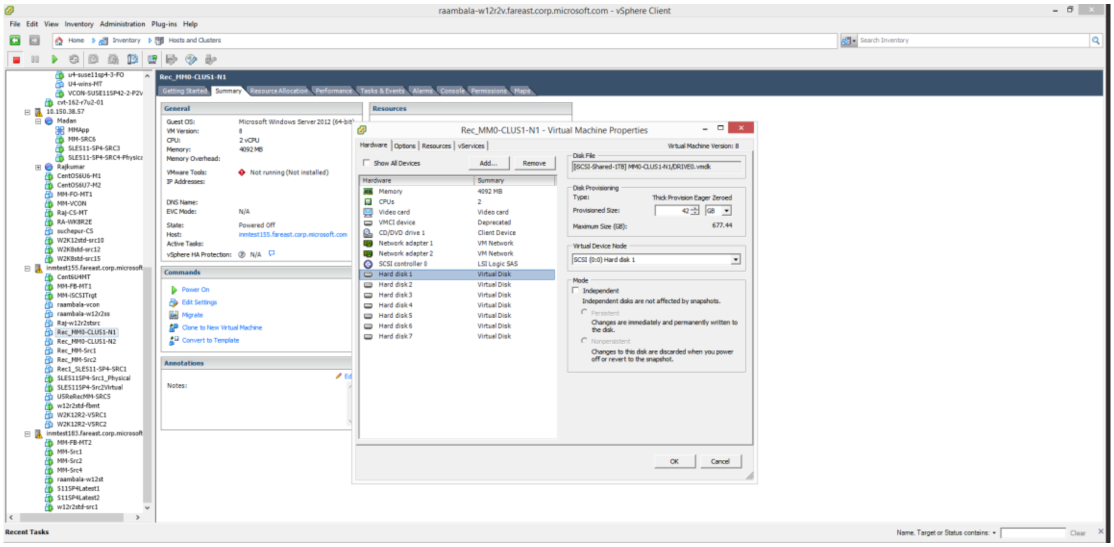


Datastore Browser - [iSCSI-Shared-1TB]

[iSCSI-Shared-1TB] MM0-CLUS1-N1

Name	Size	Type	Path
MM0-CLUS1-N1.vmsd	0.00 KB	File	[iSCSI-Shared-1TB] MM0-CLUS1-N1
MM0-CLUS1-N1.nvram	8.48 KB	Non-volatile me...	[iSCSI-Shared-1TB] MM0-CLUS1-N1
MM0-CLUS1-N1_24815793.vmdk	2,621,440.00 KB	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1
MM0-CLUS1-N1_5DA1EA1D.vmdk	1,048,576.00 KB	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1
MM0-CLUS1-N1_2E0B5ED.vmdk	44,040,190.00 K	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1
MM0-CLUS1-N1.vmx	3.84 KB	Virtual Machine	[iSCSI-Shared-1TB] MM0-CLUS1-N1
vmware-1.log	129.74 KB	Virtual Machine ...	[iSCSI-Shared-1TB] MM0-CLUS1-N1
vmware.log	138.75 KB	Virtual Machine ...	[iSCSI-Shared-1TB] MM0-CLUS1-N1

13. Once the vmdks are renamed in the new format, go to the DR VMs in the target ESX and detach the old disks (old .vmdk files) and attach the newly renamed disks (new .vmdk files). For this first identify the DR VM. This DR VM is obtained from the diagram shown in Step 1 under the field "New Display Name". Open the vSphere client and select the target ESX Host and from there identify the DR VM with the help of "New Display Name" field. Click on edit settings and remove all the disks that are attached. After that attach the newly renamed vmdk files to each DR VM available in the P2V cluster protection plan.
    The following diagram shows the DR VM and its disks in the vSphere client before detaching the older disks…



Rec_MM0-CLUS1-N1 - Virtual Machine Properties

Virtual Machine Version: 8

Hardware	Summary
Memory	4092 MB
CPUs	2
Video card	Video card
VMCI device	Deprecated
CD/DVD drive 1	Client Device
Network adapter 1	VM Network
Network adapter 2	VM Network
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Hard disk 5	Virtual Disk
Hard disk 6	Virtual Disk
Hard disk 7	Virtual Disk

Disk File: [iSCSI-Shared-1TB] MM0-CLUS1-N1/DRIVE0.vmdk

Disk Provisioning Type: Thick Provision Eager Zeroed

Provisioned Size: 42 GB

Maximum Size (GB): 677.44

Virtual Device Node: SCSI (0:0) Hard disk 1

Mode: ☐ Independent

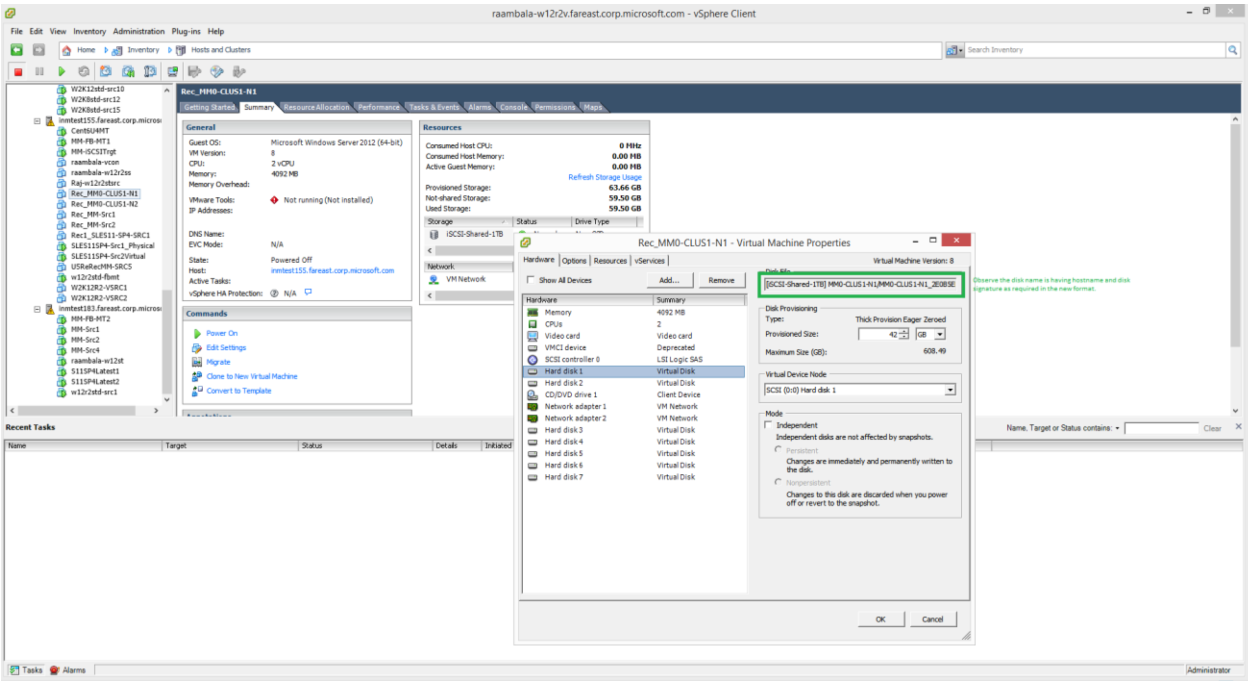
Guest OS: Microsoft Windows Server 2012 (64-bit)

VMware Tools: Not running (Not installed)

State: Powered Off

Host: inmtest155.fareast.corp.microsoft.com

The following figure shows the disks path in the DR VM after attaching the new vmdk files


raambala-w12r2v.fareast.corp.microsoft.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps
Commands
Power On
Edit Settings
Migrate
Clone to New Virtual Machine
Convert to Template
Refresh Storage Usage
Recent Tasks
Name Target Status Details Initiated
Name, Target or Status contains:
Clear
Tasks Alarms
Administrator
Hardware Options Resources vServices
Add...
Remove
OK
Cancel

W2K12std-src10
W2K8std-src12
W2K8std-src15
inmtest155.fareast.corp.micros
Cent6U4MT
MM-FB-MT1
MM-iSCSITrgt
raambala-vcon
raambala-w12r2ss
Raj-w12r2stsrc
Rec_MM0-CLUS1-N1
Rec_MM0-CLUS1-N2
Rec_MM-Src1
Rec_MM-Src2
Rec1_SLES11-SP4-SRC1
SLES11SP4-Src1_Physical
SLES11SP4-Src2Virtual
U5ReRecMM-SRC5
w12r2std-fbmt
W2K12R2-VSRC1
W2K12R2-VSRC2
inmtest183.fareast.corp.micros
MM-FB-MT2
MM-Src1
MM-Src2
MM-Src4
raambala-w12st
S11SP4Latest1
S11SP4Latest2
w12r2std-src1

Rec_MM0-CLUS1-N1

General

Guest OS: Microsoft Windows Server 2012 (64-bit)
VM Version: 8
CPU: 2 vCPU
Memory: 4092 MB
Memory Overhead:
VMware Tools: Not running (Not installed)
IP Addresses:
DNS Name:
EVC Mode: N/A
State: Powered Off
Host: inmtest155.fareast.corp.microsoft.com
Active Tasks:
vSphere HA Protection: N/A

Resources

Consumed Host CPU: 0 MHz
Consumed Host Memory: 0.00 MB
Active Guest Memory: 0.00 MB
Provisioned Storage: 63.66 GB
Not-shared Storage: 59.50 GB
Used Storage: 59.50 GB

Storage	Status	Drive Type
iSCSI-Shared-1TB		

Network
VM Network

Rec_MM0-CLUS1-N1 - Virtual Machine Properties

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	4092 MB
CPUs	2
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
CD/DVD drive 1	Client Device
Network adapter 1	VM Network
Network adapter 2	VM Network
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Hard disk 5	Virtual Disk
Hard disk 6	Virtual Disk
Hard disk 7	Virtual Disk

Disk File
[iSCSI-Shared-1TB] MM0-CLUS1-N1/MM0-CLUS1-N1_2E0B5E

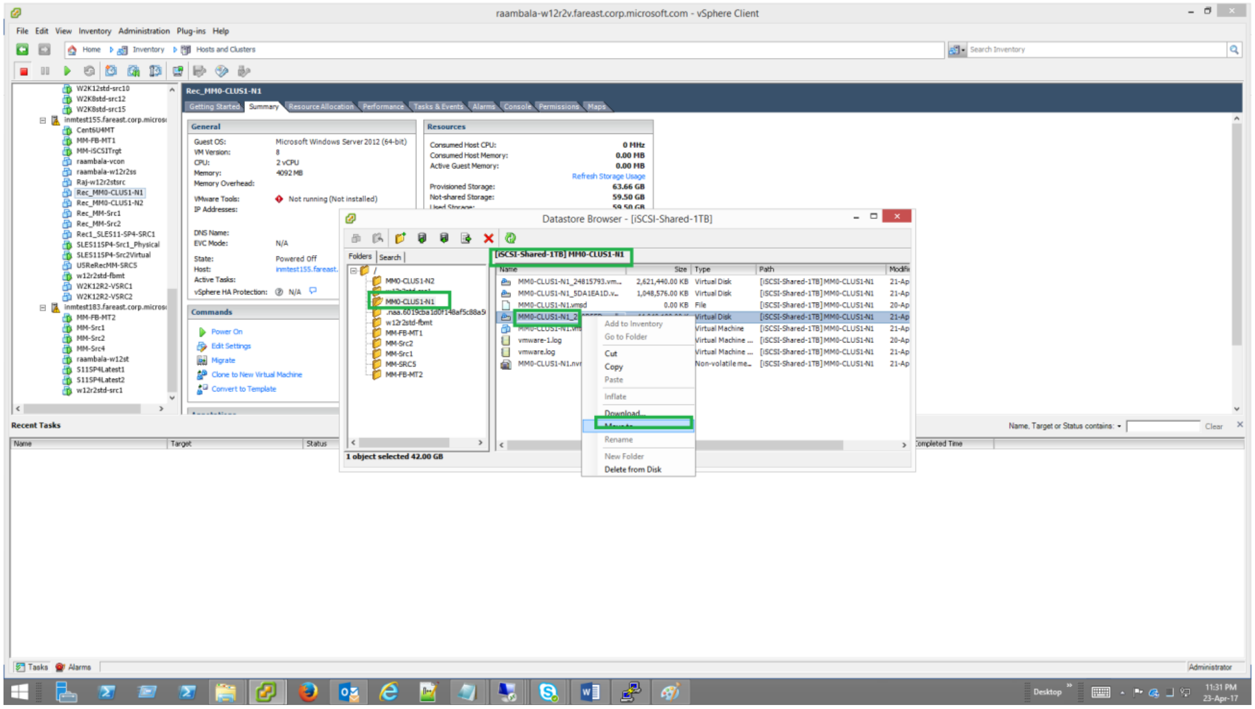
Disk Provisioning
Type: Thick Provision Eager Zeroed
Provisioned Size: 42 GB
Maximum Size (GB): 608.49

Virtual Device Node
SCSI (0:0) Hard disk 1

Mode
□ Independent
Independent disks are not affected by snapshots.
○ Persistent
Changes are immediately and permanently written to the disk.
○ Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.

Observe the disk name is having hostname and disk signature as required in the new format.

14. The next step is to protect the MSCS cluster again in P2V mode as the protection is removed in Step 4. The cluster disks can move from one node to the other and as they move from one cluster node to the other cluster node, the disks become active on the new node and passive on the old node. So, at the time of protection of this cluster earlier, the active – passive disks on each node could be different than what is the current active – passive disks on each cluster node. So, if a cluster disk is found to be passive now and active earlier, then you have to move the vmdk file from the older path to the new path in the target ESX datastore. This can be done quite easily as now the vmdk files are having the disk signatures in their names. So, the end user should check if a disk is passive on that node, then she should note the disk signature and check for the availability of the vmdk file with that disk signature on the Target ESX Data Store folder. If the vmdk file is indeed there, then it should be moved to the new Target ESX Data Store folder by right clicking that vmdk file and choosing the new path in the Target ESX Data Store folder. By doing this step, vContinuum can re-use the disk during protection and the initial seeding time of protection will get reduced and the protection will complete faster. If this step is not done, then a new disk will be created and the older disk which is available in a different path in the ESX data store will not be re-used. Thus, this is only an optimizing step and not a mandatory step.



raambala-w12r2v.fareast.corp.microsoft.com - vSphere Client

Rec_MM0-CLUS1-N1

General

Guest OS: Microsoft Windows Server 2012 (64-bit)
VM Version: 8
CPU: 2 vCPU
Memory: 4092 MB
Memory Overhead:
VMware Tools: Not running (Not installed)
IP Addresses:
DNS Name:
EVC Mode: N/A
State: Powered Off
Host: inmtest155.fareast.
Active Tasks:
vSphere HA Protection: N/A

Resources

Consumed Host CPU: 0 MHz
Consumed Host Memory: 0.00 MB
Active Guest Memory: 0.00 MB
Provisioned Storage: 63.66 GB
Not-shared Storage: 59.50 GB
Used Storage: 59.50 GB

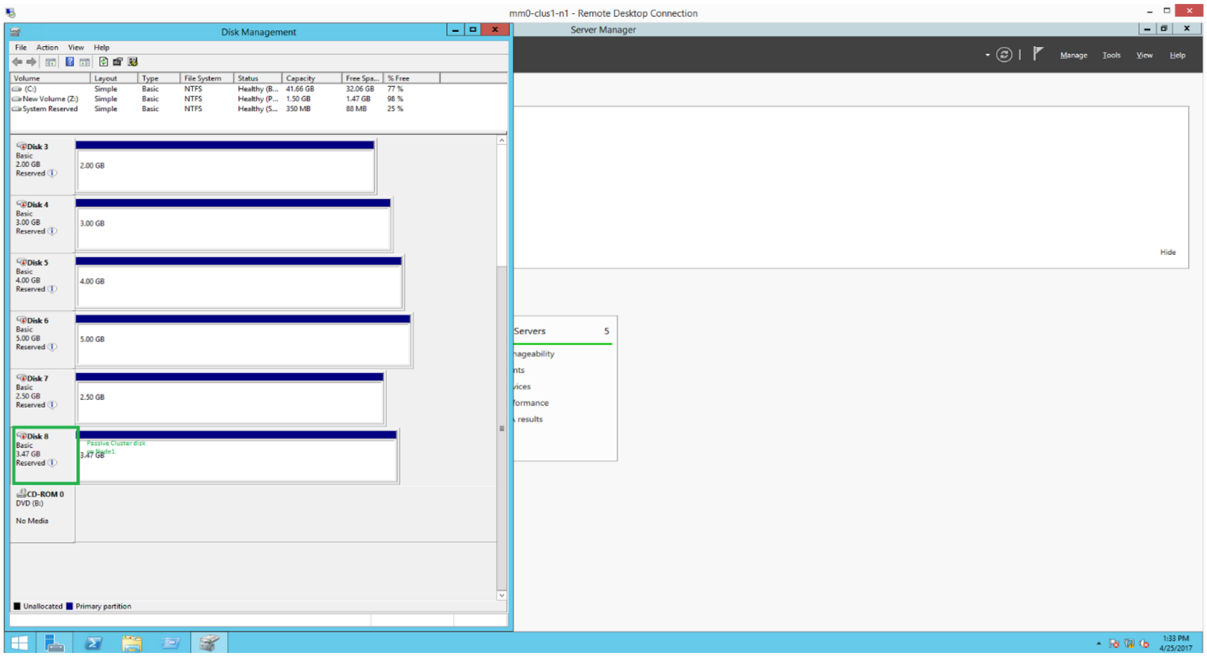
Datastore Browser - [iSCSI-Shared-1TB]

[iSCSI-Shared-1TB] MM0-CLUS1-N1

Name	Size	Type	Path	Modifi
MM0-CLUS1-N1_24815793.vm...	2,621,440.00 KB	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1	21-Ap
MM0-CLUS1-N1_5DA1EA1D.v...	1,048,576.00 KB	Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1	21-Ap
MM0-CLUS1-N1.vmsd	0.00 KB	File	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Ap
MM0-CLUS1-N1_2		Virtual Disk	[iSCSI-Shared-1TB] MM0-CLUS1-N1	21-Ap
MM0-CLUS1-N1.vm		Virtual Machine	[iSCSI-Shared-1TB] MM0-CLUS1-N1	21-Ap
vmware-1.log		Virtual Machine ...	[iSCSI-Shared-1TB] MM0-CLUS1-N1	20-Ap
vmware.log		Virtual Machine ...	[iSCSI-Shared-1TB] MM0-CLUS1-N1	21-Ap
MM0-CLUS1-N1.nvr		Non-volatile me...	[iSCSI-Shared-1TB] MM0-CLUS1-N1	21-Ap

1 object selected 42.00 GB

To explain this, further, let’s see the disk management console on one of the source node MM0-CLUS1-N1.



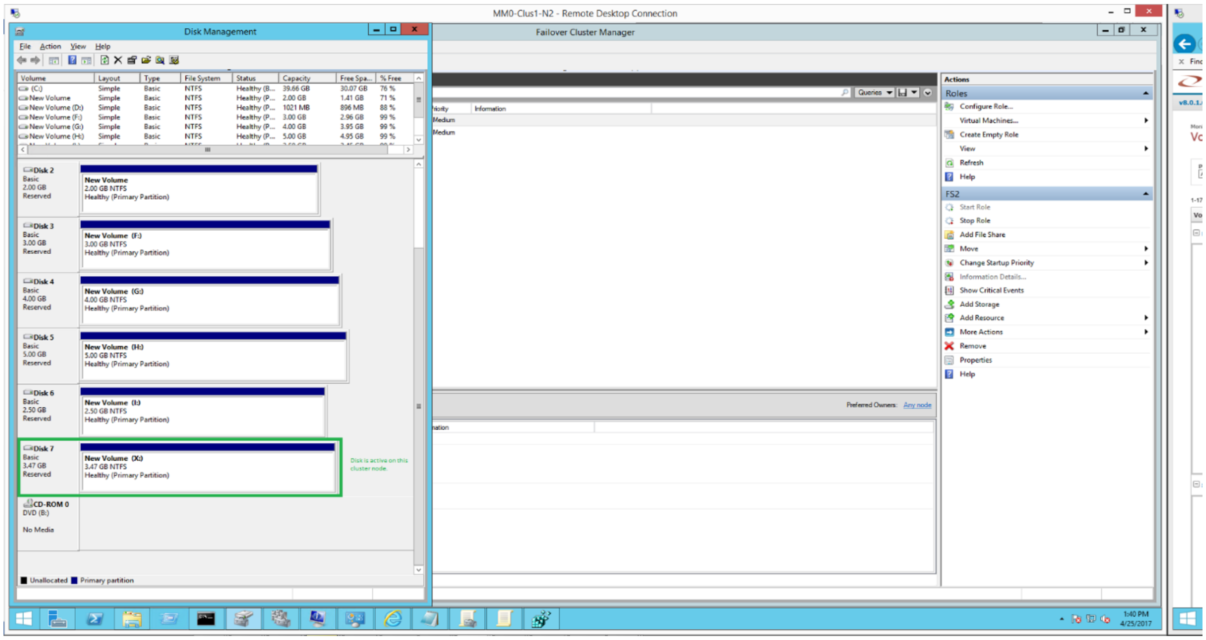
mm0-clus1-n1 - Remote Desktop Connection

Disk Management

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	41.66 GB	32.06 GB	77 %
New Volume (Z:)	Simple	Basic	NTFS	Healthy (P...	1.50 GB	1.47 GB	98 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	350 MB	88 MB	25 %

Disk 3 Basic 2.00 GB Reserved — 2.00 GB
Disk 4 Basic 3.00 GB Reserved — 3.00 GB
Disk 5 Basic 4.00 GB Reserved — 4.00 GB
Disk 6 Basic 5.00 GB Reserved — 5.00 GB
Disk 7 Basic 2.50 GB Reserved — 2.50 GB
Disk 8 Basic 3.47 GB Reserved — Passive Cluster disk Node1 3.47 GB
CD-ROM 0 DVD (B:) No Media

Observe the **Disk 8** is in **Reserved** and in-active on MM0-Clus1-N1.
Now, check the state of this disk on the second cluster Node MM0-CLUS1-N2 in the disk management console.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	39.66 GB	30.07 GB	76 %
New Volume	Simple	Basic	NTFS	Healthy (P...	2.00 GB	1.41 GB	71 %
New Volume (D:)	Simple	Basic	NTFS	Healthy (P...	1021 MB	896 MB	88 %
New Volume (F:)	Simple	Basic	NTFS	Healthy (P...	3.00 GB	2.96 GB	99 %
New Volume (G:)	Simple	Basic	NTFS	Healthy (P...	4.00 GB	3.95 GB	99 %
New Volume (H:)	Simple	Basic	NTFS	Healthy (P...	5.00 GB	4.95 GB	99 %

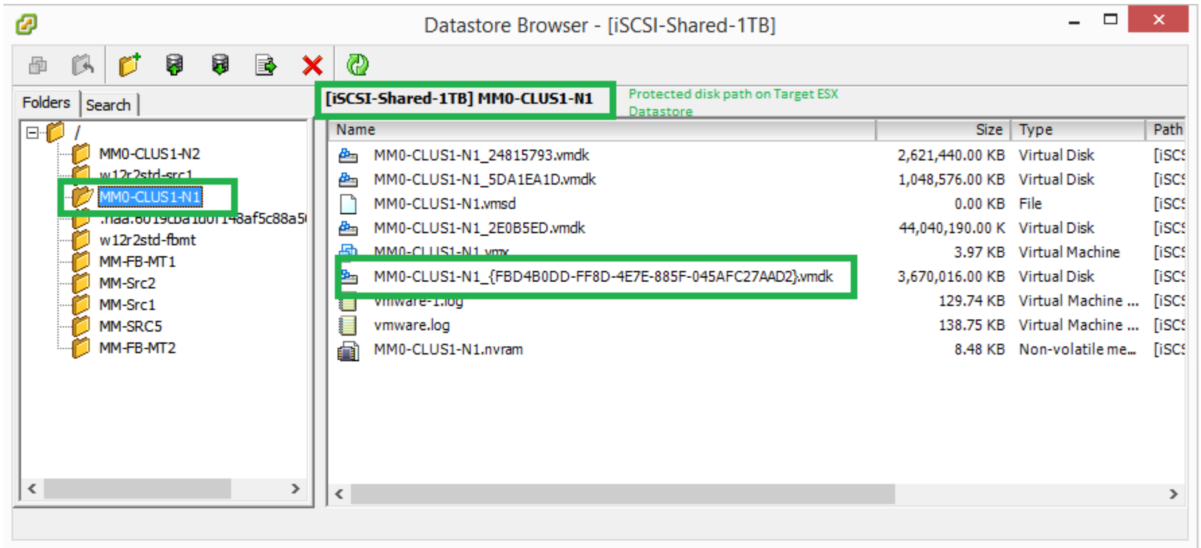
Disk	Volume
Disk 2 Basic 2.00 GB Reserved	New Volume 2.00 GB NTFS Healthy (Primary Partition)
Disk 3 Basic 3.00 GB Reserved	New Volume (F:) 3.00 GB NTFS Healthy (Primary Partition)
Disk 4 Basic 4.00 GB Reserved	New Volume (G:) 4.00 GB NTFS Healthy (Primary Partition)
Disk 5 Basic 5.00 GB Reserved	New Volume (H:) 5.00 GB NTFS Healthy (Primary Partition)
Disk 6 Basic 2.50 GB Reserved	New Volume (I:) 2.50 GB NTFS Healthy (Primary Partition)
Disk 7 Basic 3.47 GB Reserved	New Volume (X:) 3.47 GB NTFS Healthy (Primary Partition)
CD-ROM 0 DVD (B:) No Media	

Disk is active on this cluster node.

■ Unallocated ■ Primary partition

So, from the above figure, it is clear that the disk is passive on MM0-CLUS1-N1 and active on MM0-CLUS1-N2.

Now, go to the data store of MM0-Clus1-N1 on the Target ESX host and check the availability of this disks corresponding vmdk file by going to the target ESX data store path **[iSCSI-Shared-1TB] MM0-CLUS1-N1**.

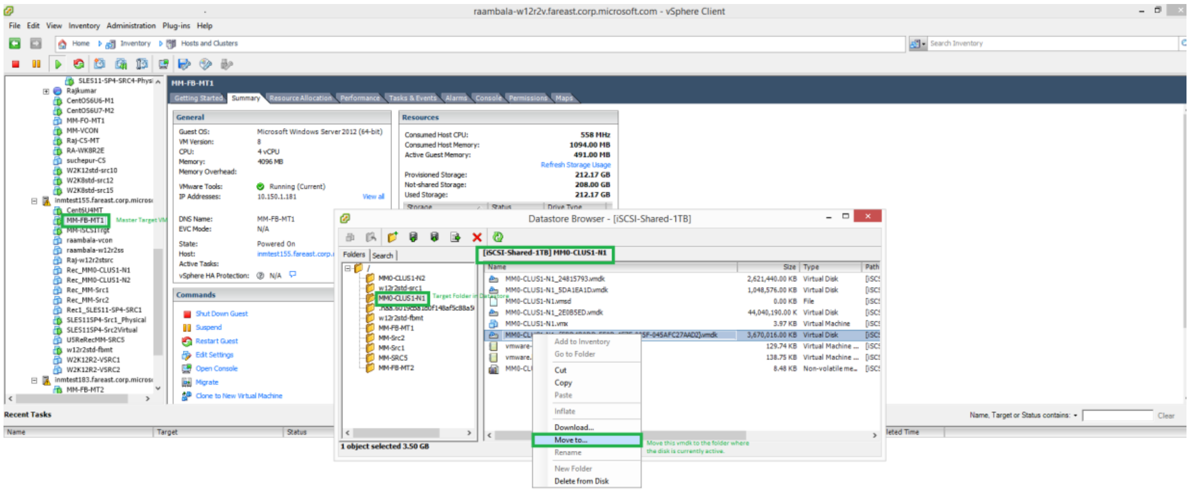


[iSCSI-Shared-1TB] MM0-CLUS1-N1

Protected disk path on Target ESX Datastore

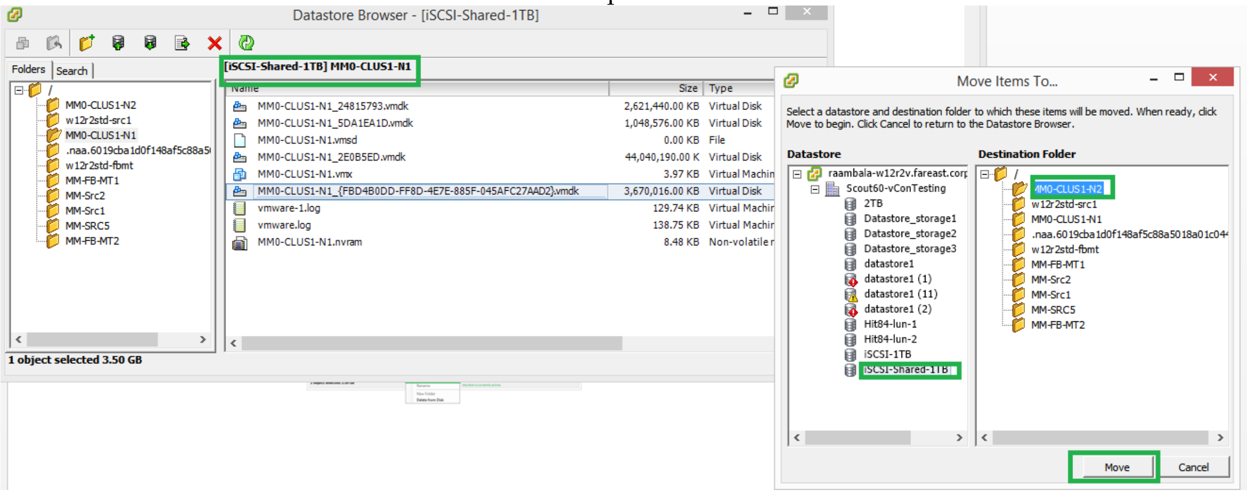
Name	Size	Type	Path
MM0-CLUS1-N1_24815793.vmdk	2,621,440.00 KB	Virtual Disk	[iSCS
MM0-CLUS1-N1_5DA1EA1D.vmdk	1,048,576.00 KB	Virtual Disk	[iSCS
MM0-CLUS1-N1.vmsd	0.00 KB	File	[iSCS
MM0-CLUS1-N1_2E0B5ED.vmdk	44,040,190.00 K	Virtual Disk	[iSCS
MM0-CLUS1-N1.vmx	3.97 KB	Virtual Machine	[iSCS
MM0-CLUS1-N1_{FBD4B0DD-FF8D-4E7E-885F-045AFC27AAD2}.vmdk	3,670,016.00 KB	Virtual Disk	[iSCS
vmware-1.log	129.74 KB	Virtual Machine ...	[iSCS
vmware.log	138.75 KB	Virtual Machine ...	[iSCS
MM0-CLUS1-N1.nvram	8.48 KB	Non-volatile me...	[iSCS

But this disk is passive on this node, so before you start protection of this Cluster (MM0-CLUS1), you must move this vmdk from this path to the path where the second cluster Node's disks are present…i.e. you should move this disk to the Target ESX datastore path **[iSCSI-Shared-1TB] MM0-CLUS1-N2**.



raambala-w12r2v.fareast.corp.microsoft.com - vSphere Client
MM-FB-MT1
Master Target VM
Datastore Browser - [iSCSI-Shared-1TB]
[iSCSI-Shared-1TB] MM0-CLUS1-N1
MM0-CLUS1-N1
Target Folder in Datastore
Add to Inventory
Go to Folder
Cut
Copy
Paste
Inflate
Download...
Move to...
Rename
New Folder
Delete from Disk
Move this vmdk to the folder where the disk is currently active.
1 object selected 3.50 GB

Move the above selected disk to the new data store path.



Datastore Browser - [iSCSI-Shared-1TB]

[iSCSI-Shared-1TB] MM0-CLUS1-N1

Name	Size	Type
MM0-CLUS1-N1_24815793.vmdk	2,621,440.00 KB	Virtual Disk
MM0-CLUS1-N1_5DA1EA1D.vmdk	1,048,576.00 KB	Virtual Disk
MM0-CLUS1-N1.vmsd	0.00 KB	File
MM0-CLUS1-N1_2E0B5ED.vmdk	44,040,190.00 K	Virtual Disk
MM0-CLUS1-N1.vmx	3.97 KB	Virtual Machin
MM0-CLUS1-N1_{FBD4B0DD-FF8D-4E7E-885F-045AFC27AAD2}.vmdk	3,670,016.00 KB	Virtual Disk
vmware-1.log	129.74 KB	Virtual Machir
vmware.log	138.75 KB	Virtual Machir
MM0-CLUS1-N1.nvram	8.48 KB	Non-volatile r

1 object selected 3.50 GB

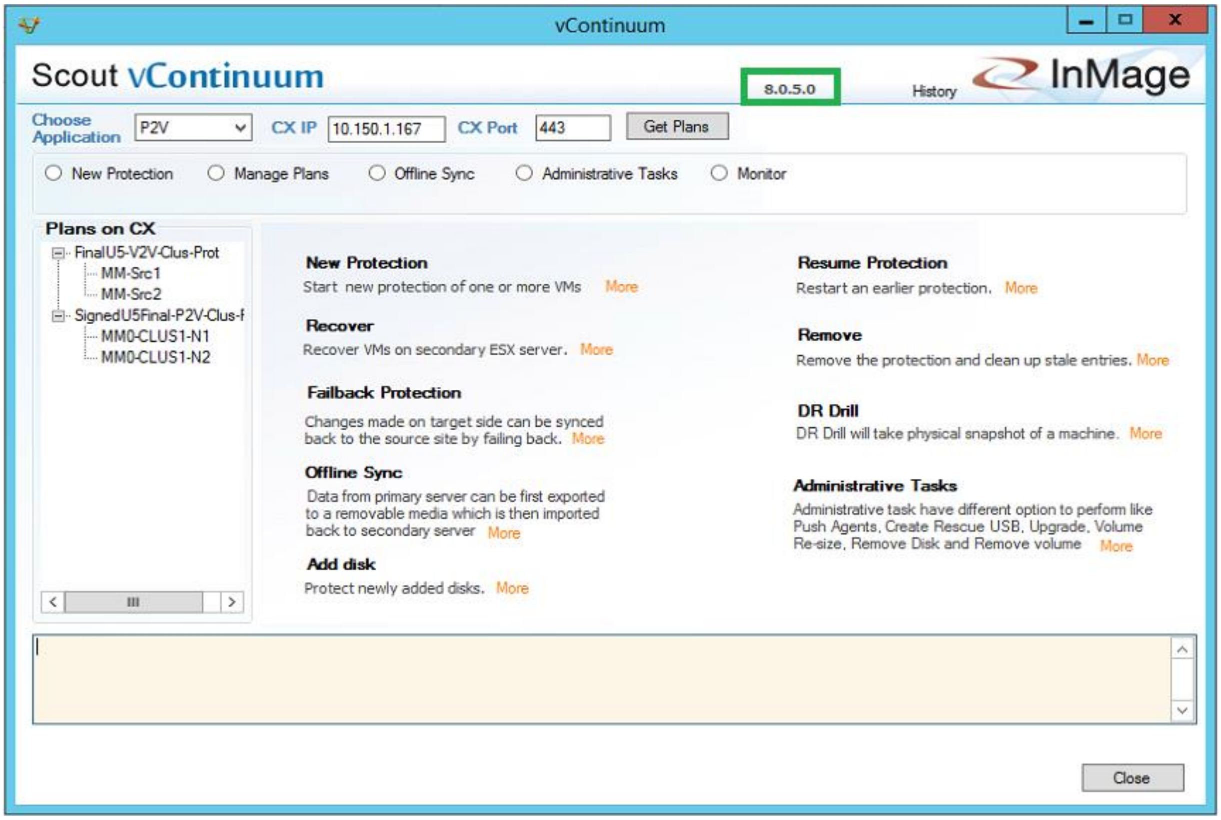
Move Items To...

Select a datastore and destination folder to which these items will be moved. When ready, click Move to begin. Click Cancel to return to the Datastore Browser.

This step is not mandatory as described above. If this step is done, then the target side ESX disks will be re-used during re-protection and otherwise, new disks will get created during re-protection.

15. Now, upgrade vContinuum to Scout 8.0.1 Update 5 by running the **vCon_Windows_8.0.5.0_GA_Update_5_11525767_20Apr17.exe** (Note: If there is any new update after update5, use the latest vContinuum update installer. For example, for update 6, vContinuum installer is vCon_Windows_8.0.6.0_GA_Update_6_11525767_21Sep17.exe. Run the installer to upgrade to latest version.)

16. After vContinuum upgrade is over, launch vContinuum from the Start menu and you can check the updated version as below…



vContinuum

Scout vContinuum 8.0.5.0 History InMage

Choose Application: P2V CX IP: 10.150.1.167 CX Port: 443 Get Plans

○ New Protection ○ Manage Plans ○ Offline Sync ○ Administrative Tasks ○ Monitor

Plans on CX

- FinalU5-V2V-Clus-Prot
  - MM-Src1
  - MM-Src2
- SignedU5Final-P2V-Clus-F
  - MM0-CLUS1-N1
  - MM0-CLUS1-N2

New Protection
Start new protection of one or more VMs More

Recover
Recover VMs on secondary ESX server. More

Failback Protection
Changes made on target side can be synced back to the source site by failing back. More

Offline Sync
Data from primary server can be first exported to a removable media which is then imported back to secondary server More

Add disk
Protect newly added disks. More

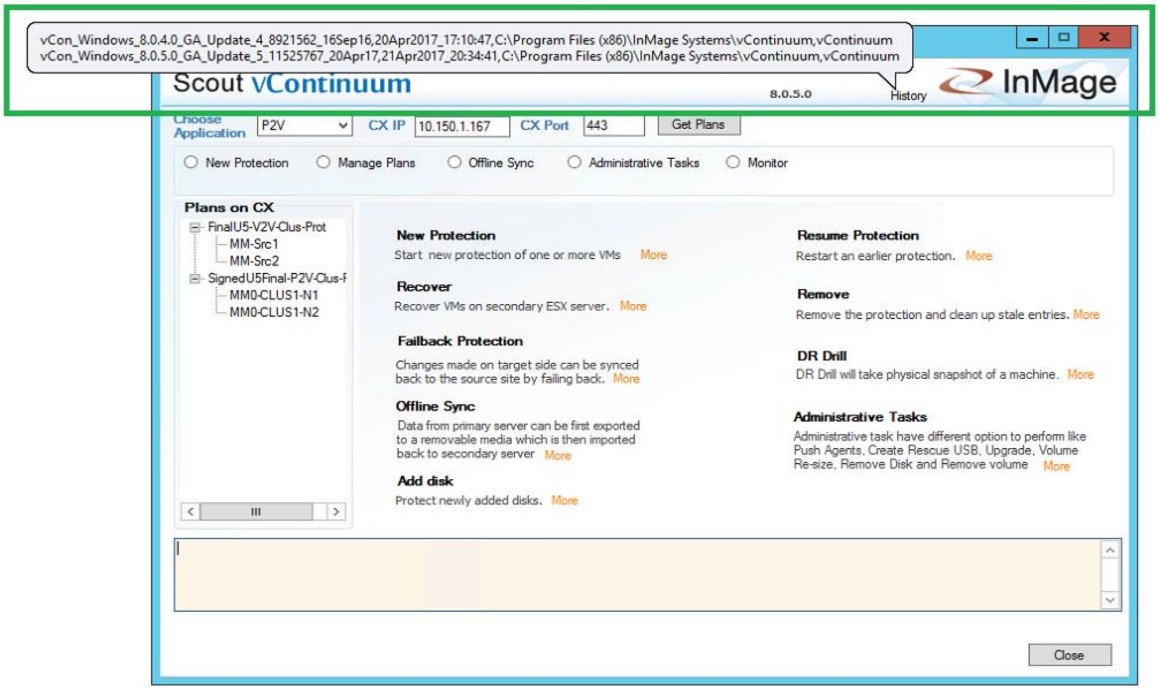
Resume Protection
Restart an earlier protection. More

Remove
Remove the protection and clean up stale entries. More

DR Drill
DR Drill will take physical snapshot of a machine. More

Administrative Tasks
Administrative task have different option to perform like Push Agents, Create Rescue USB, Upgrade, Volume Re-size, Remove Disk and Remove volume More

17. Observer the Upgrade history by hovering the mouse on “History” label on vContinuum user interface like this…



```
vCon_Windows_8.0.4.0_GA_Update_4_8921562_16Sep16,20Apr2017_17:10:47,C:\Program Files (x86)\InMage Systems\vContinuum,vContinuum
vCon_Windows_8.0.5.0_GA_Update_5_11525767_20Apr17,21Apr2017_20:34:41,C:\Program Files (x86)\InMage Systems\vContinuum,vContinuum
```

Scout vContinuum 8.0.5.0 History InMage

Choose Application: P2V CX IP: 10.150.1.167 CX Port: 443 Get Plans

○ New Protection ○ Manage Plans ○ Offline Sync ○ Administrative Tasks ○ Monitor

Plans on CX

- FinalU5-V2V-Clus-Prot
  - MM-Src1
  - MM-Src2
- SignedU5Final-P2V-Clus-F
  - MM0-CLUS1-N1
  - MM0-CLUS1-N2

New Protection
Start new protection of one or more VMs More

Recover
Recover VMs on secondary ESX server. More

Failback Protection
Changes made on target side can be synced back to the source site by failing back. More

Offline Sync
Data from primary server can be first exported to a removable media which is then imported back to secondary server More

Add disk
Protect newly added disks. More

Resume Protection
Restart an earlier protection. More

Remove
Remove the protection and clean up stale entries. More

DR Drill
DR Drill will take physical snapshot of a machine. More

Administrative Tasks
Administrative task have different option to perform like Push Agents, Create Rescue USB, Upgrade, Volume Re-size, Remove Disk and Remove volume More

18. Now protect the same Cluster which you have earlier protected in P2V mode.

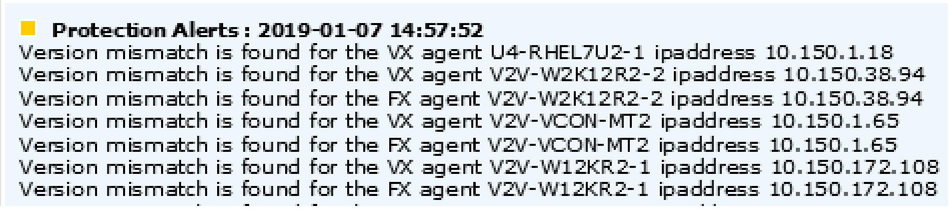
With this the upgrade to latest Scout update version completes.

13 Scout Update 7 enables TLS v1.2 support

The PHP Scripting Platform needs to be upgraded to v7.2.10 32 bit and the MySQL database needs to be upgraded to v5.7.23 on CX and RX Servers. Please refer to the steps given in the **section 7.4** of **Scout_Standard_Quick_Install_Guide.pdf.**

14 Please ignore the Version mismatch is found for the VX agent alerts in the CS UI after upgrading to Scout 8.0.7.

After upgrading the agents to 8.0.7, you may find alerts in the CS UI as shown below.



```
■ Protection Alerts : 2019-01-07 14:57:52
Version mismatch is found for the VX agent U4-RHEL7U2-1 ipaddress 10.150.1.18
Version mismatch is found for the VX agent V2V-W2K12R2-2 ipaddress 10.150.38.94
Version mismatch is found for the FX agent V2V-W2K12R2-2 ipaddress 10.150.38.94
Version mismatch is found for the VX agent V2V-VCON-MT2 ipaddress 10.150.1.65
Version mismatch is found for the FX agent V2V-VCON-MT2 ipaddress 10.150.1.65
Version mismatch is found for the VX agent V2V-W12KR2-1 ipaddress 10.150.172.108
Version mismatch is found for the FX agent V2V-W12KR2-1 ipaddress 10.150.172.108
```

You may ignore these alerts.