Tech Note

Using VMware vMotion with ClearPass Virtual Appliances

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Document Revision History

Date	Modified By	Comments
March 12th, 2014	Danny Jump	Initial Published Version

Table of Contents

Table of Figures

Overview

The following guide has been produced to help educate our customers and partners in the use of VMware Hardware vMotion and ClearPass. This version of the guide was written to accompany the CPPM 6.3 release. This guide will be updated and republished to reflect new and improved functionality we deliver in subsequent software releases. Please check back regularly for updates.

Note: We have tested CPPM 6.2.0 and CPPM 6.3.0 successfully. Following the investigation we with CPPM 6.2.0 we made several improvements to the underlying VM hardware configuration such as modifying the Ethernet interfaces to use VMXNET3 and upgrading the VMware Tools software to the latest version to provide a better user experience for the CPPM 6.3.0 product release.

Note: Where you see a red-chili  this is to signify a **'hot'** important point and highlights that this point is to be taken as a best-practice recommendation.

Background

Customers become dependent on solutions and applications to help them run their business. Part of the deployment will typically include planning to ensure that the deployed systems are available and they provide a level of availability in line with the demands of the application and business. For example it's not as important to plan for the same uptime in an application used to process luncheon-vouchers as that of an enterprise wide identity store providing authentication and authorization for the entire employees of a company, e.g. ClearPass Policy Manager.

Customers plan for availability in multiple ways and generally leverage multiple different hardware and software components. As an example many large enterprise customers will incorporate technology such as multiple Storage Area Networks to consolidate data, for high-availability this may include synchronous or asynchronous replication between them. Typically x86 and x64 environments will have been consolidated onto VMware ESXi. This virtualized technology encompasses multiple features to enable high availability for these virtualized servers. We will discuss the use of vMotion specifically in this Tech Note to assist in providing a layered HA solution.

In the area of availability, CPPM itself utilizes clustering at a software level to provide scale and Availability.

ClearPass High Availability

Multiple CPPM instances can be deployed locally or in a distributed environment to provide scale and to enable High-Availability. We will classify this solution as an active/passive software solution with regard to HA.

In a cluster of CPPM instances a CPPM can be either a Publisher or a Subscriber. Any CPPM instance can process authentications/authorization for clients but a Publisher is required in the cluster as this system is responsible for the configuration of the cluster and for database writes, such as the creation of Guest accounts or the creation of Onboard client certificates. If we lose the Publisher then we can still authenticate users to the network but we are unable to make configuration changes or create new Guest accounts.

In the event of a Publisher failure, CPPM provides for an automatic and a manual solution for this failure, as discussed below.

Manual Solution

A CPPM subscriber instance can be manually promoted to a Publisher via the GUI as shown below. Under **Administration > Server Manager > Server Configuration > [select CPPM]**, then click the **Promote to Publisher** link, and click **Yes** to confirm the promotion as shown below.

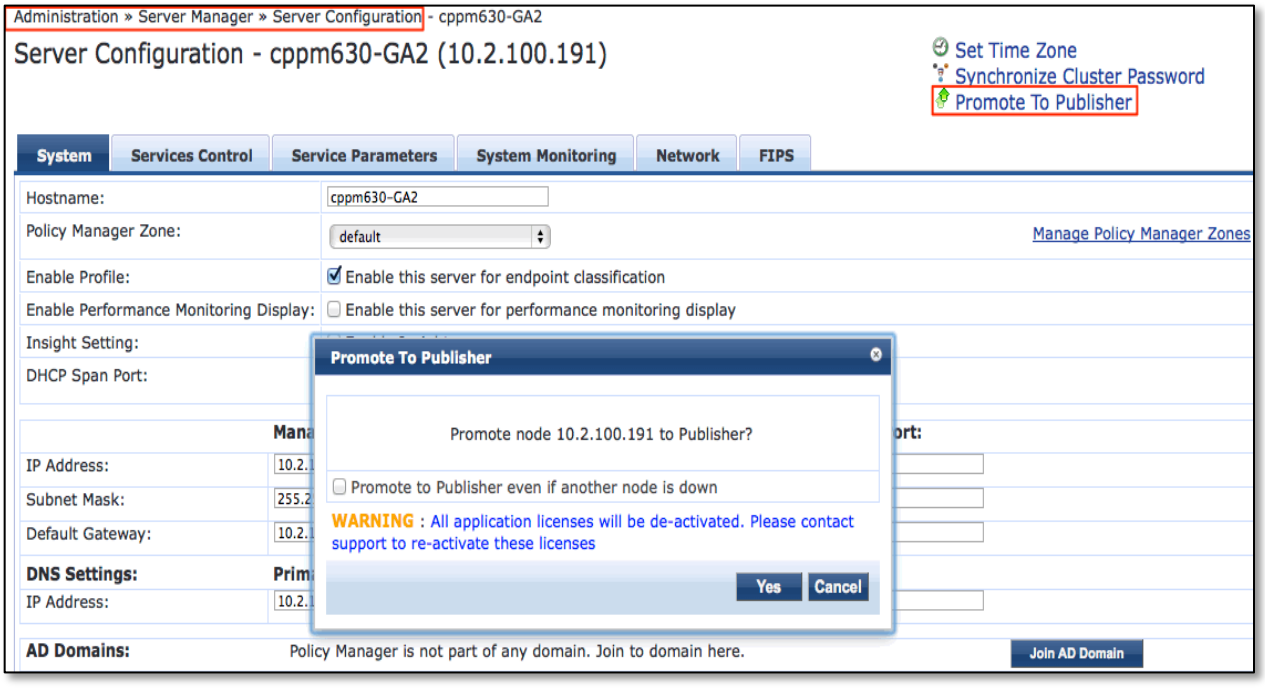

Figure 1 - Manually promoting a Subscriber to a Publisher in the GUI

A CPPM Subscriber can also be manually promoted to a Publisher via the CLI, using the command **cluster make-publisher** an example is shown below.

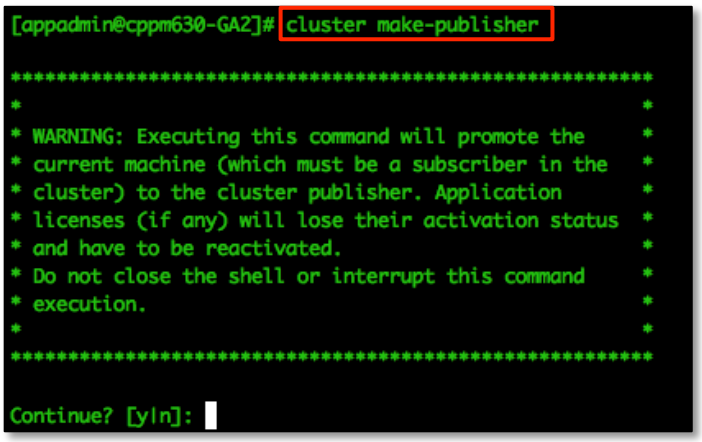

Figure 2 - Manually promoting a Subscriber to a Publisher from the CLI

Automatic Solution

CPPM provides for a Subscriber to not only process authentications/authorizations etc. but it can also function in a role as a 'Standby Publisher'. This provides for the Subscriber to monitoring the health and availability of the active-Publisher, it monitors for the availability of the Publisher DB every 60 seconds. In the event of a failure, i.e. it is not able to connect to the Publishers DB based upon the 'Failover Wait Time' it will begin the process of promoting itself to a Publisher. The default Timeout is 10 minutes, with a minimum value of 5 minutes and a maximum of 60 minutes. During this process all the necessary changes to its configuration and databases to allow it to function as a Publisher will be made. Any other Subscribers in the cluster that need to communicate with the Publisher are informed that this system is now the Active-Publisher and it is now responsible for any configuration changes and that they must now replicate changes from this node.

Configuring the automatic fail-over does depend on the fact that the ClearPass servers have previously been configured in a cluster.

Under **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Standby Publisher >** set **Enable Publisher Failover** to **TRUE**, and then select the Designated Standby Publisher.

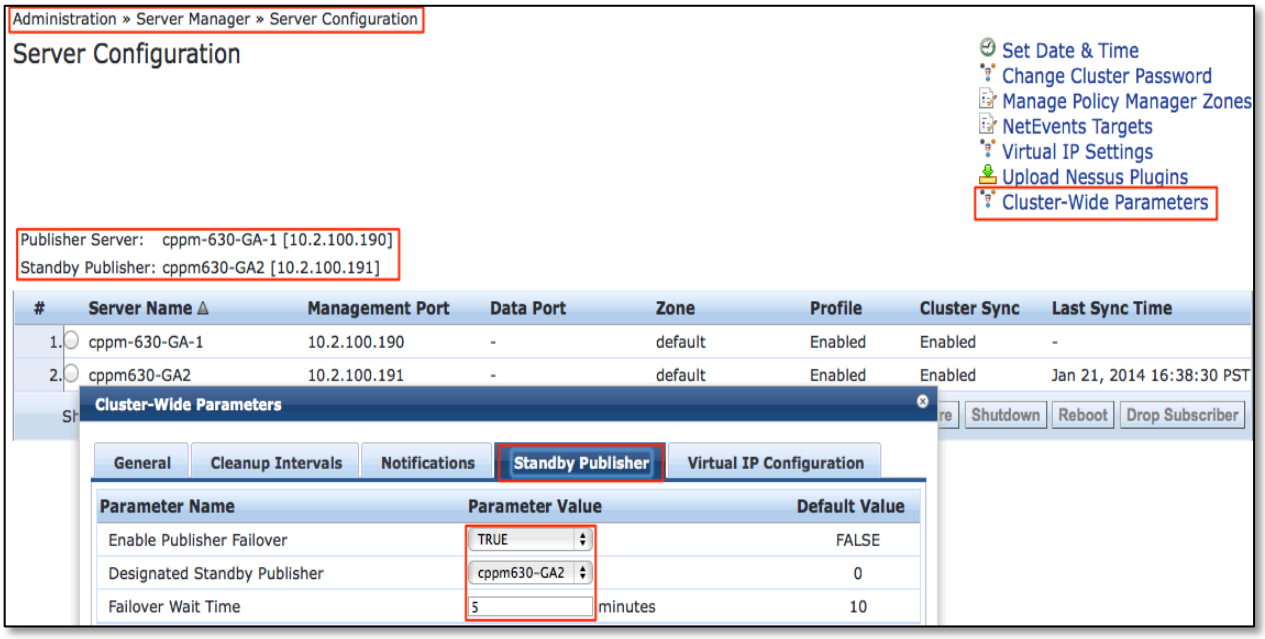

Figure 3 - Configuring automatic Subscriber promotion

The option to have a CPPM node self-promoting itself to be the Active-Publisher is extremely useful. However there is a delay that could be deemed as too long by some. The time it takes for a system to effectively become the Active-Publisher from the time the Primary-Publisher fails can be as long as 7-8 minutes.

Applications for vMotion

Having discussed at a high-level that we have in our architecture the necessary features to provide for scale and availability in CPPM why would you want to invest in additional hardware/software to enable a more real-time active-active HA solution?

Some Enterprises who offer for example Guest access for Public Venues need to have the ability to constantly create accounts, a failure of 7-8 minutes may not be acceptable. Remember, when creating Guest accounts for users this must be performed on a Publisher. If this has failed or been taken out of service then no new accounts can be created.

Using a solution such as VMware vMotion allows an enterprise to provide an additional level of application availability. For example, if an ESXi host needs to be taken out of service for maintenance or upgrades then the process today to ensure that the availability of a standalone CPPM or the Publisher within a cluster is maintained is not real-time.

VMware vMotion provides the ability to Live Migrate a CPPM VM under load with little (approximately 2-3 seconds) to zero downtime. Most of the delay is dependent on the processing ability of the ESXi host, the amount of Memory in the VM and the underlying network to transport/replicate the memory pages between systems.

Requirements for vMotion

To successfully use vMotion requires a product like vSphere vCenter Server and multiple VMware vSphere Hypervisor (ESXi) hosts. There are many VMware products that include the functionality required to vMotion a VM. Refer to www.vmware.com/products to decide what is right for your environment.

Ensure that hosts that use vMotion are configured to use shared storage. During a migration with vMotion, the migrating VM must be on storage accessible to both the source and target hosts. Shared storage is typically a storage area network (SAN), but can also be implemented using iSCSI and NAS shared storage.

How vMotion works

To say we are moving a VM from one ESXi server to another with vMotion is a bit of a lie, we don't actually move the data at all, this stays on the shared storage, it's only the VM's memory contents that are moved from one ESXi server to another. The VM on the first ESXi server is duplicated on to the second ESXi server and then the original is deleted, during vMotion the first ESXi server creates an initial pre-copy of memory from the running VM into the second ESXi server, during the copy process, a log file is generated to track all changes during the initial copy phase (it is referred to as a *memory bitmap*). Once the VM's are practically at the same state, this memory bitmap is transferred to the second ESXi server, before the transfer of the bitmap file the VM on the first ESXi server is put into a *quiescent* state. This state reduces the amount of activity occurring inside the VM that is being migrated, it allows the bitmap to become so small that it can be transferred very quickly, it also allows for rollback if a network failure occurs, this means that the migration will have to be successful or unsuccessful. When the bitmap has been transferred the users are then switched to the new ESXi server and the original VM is removed from the first ESXi server.

You need the following to perform a vMotion, the below requirements are for both ESXi servers involved

- Shared storage visibility between the source and destination ESXi servers
- A VMkernel port group on a vSwitch configured with 1Gbps or faster (10GB ideally) on the vMotion network, it will require a separate IP address.
- Access to the same network, preferably not going across L3 switches/routers, etc.
- Consistently labeled vSwitch port groups
- Compatible CPUs

vMotion Configuration

To configure vMotion on your ESXi hosts there are a few very basic requirements.

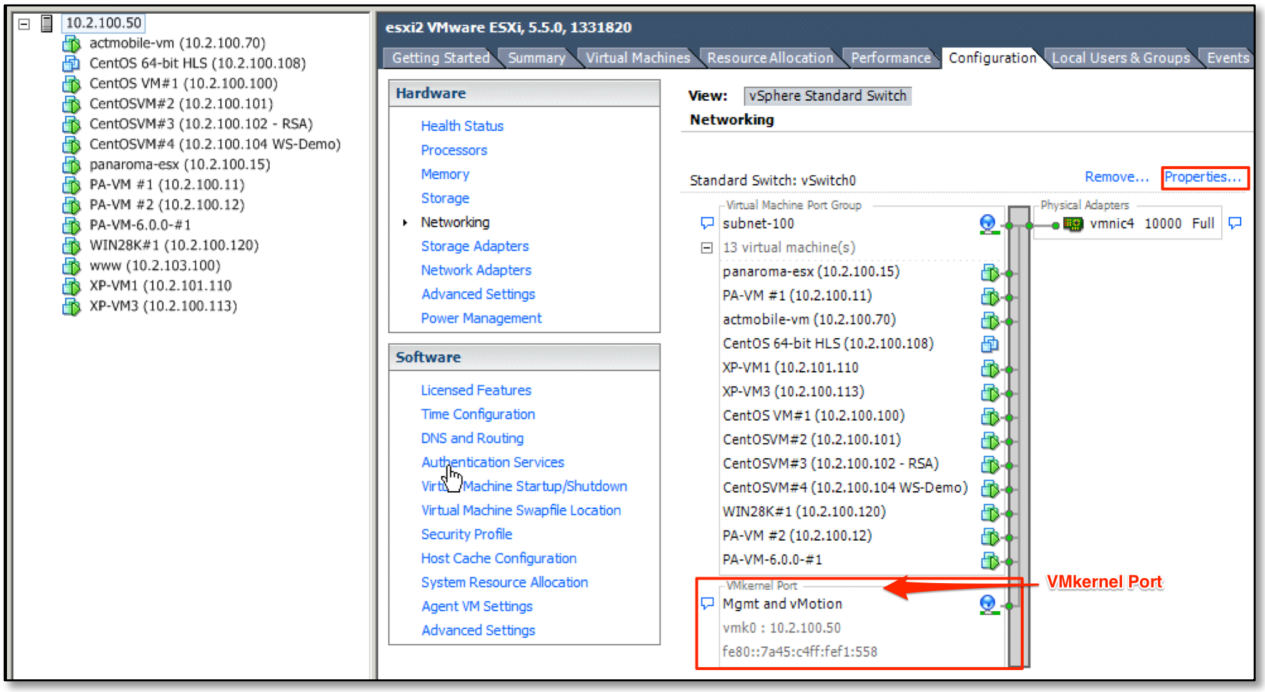

Figure 4 - vMotion on Management Network

You must ensure that vMotion is enabled on your VMkernel management network. If not messages similar to the below will be shown when you try to run a vMotion on a VM.

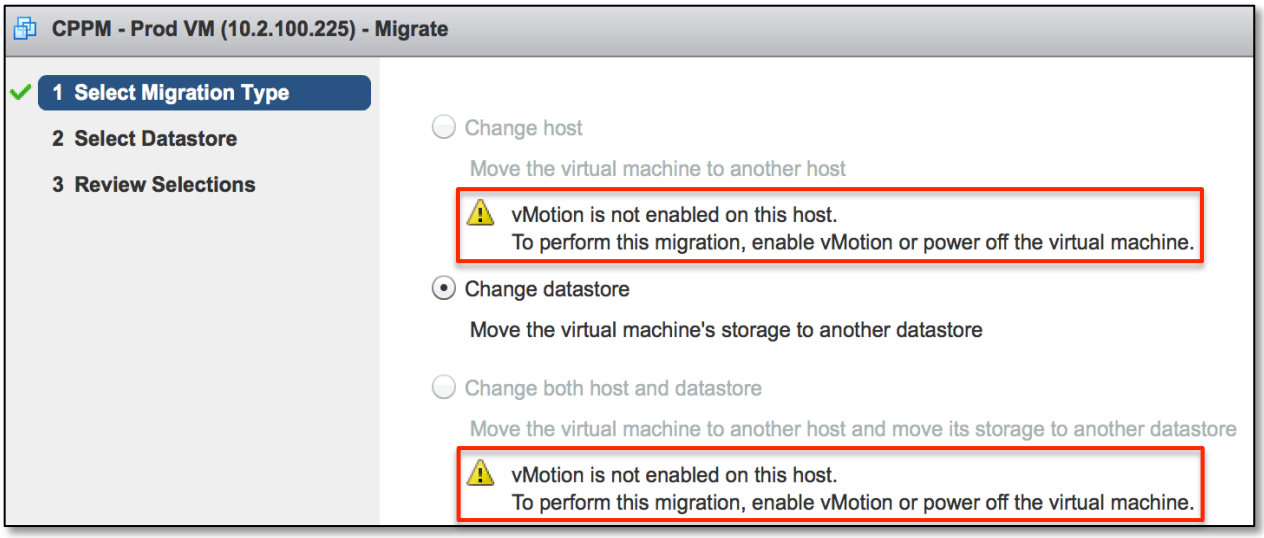

Figure 5 - Example vMotion failure messages

If you do experience messages similar to the above then configuration changes will be required to the underlying VMware networking interfaces.

Note: We renamed our port to make it a more sensible name/label. We used **'Mgmt and vMotion'**. Click on 'Properties' and ensure as shown below that vMotion is enabled on the port on this vSwitch.

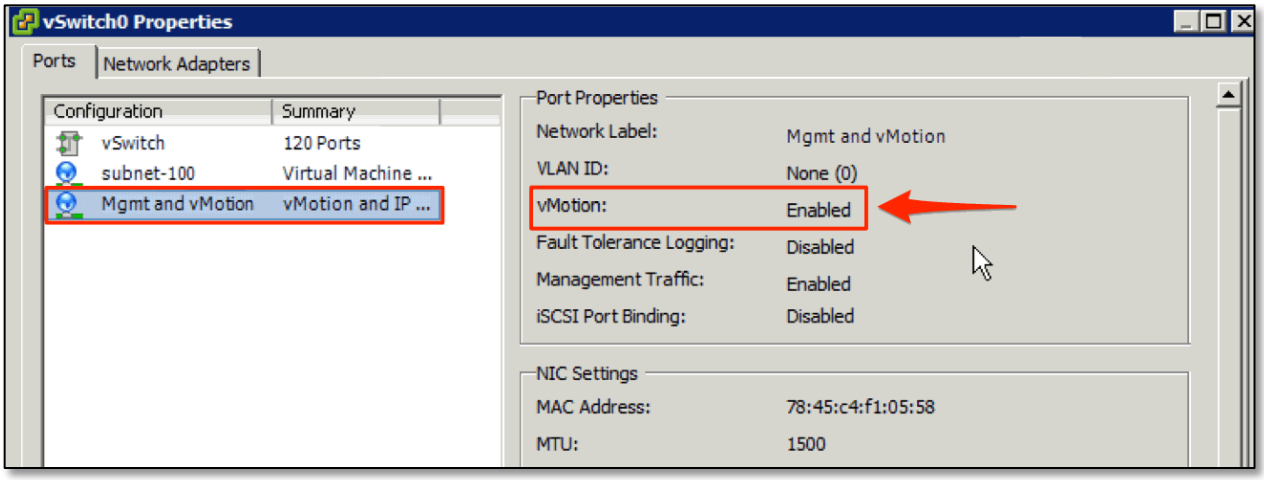

Figure 6 - Checking vMotion is enabled on Port

If vMotion is not enabled, click 'Edit' on the 'vMotion and IP Storage Port' and then enable and save as shown on the following screen.

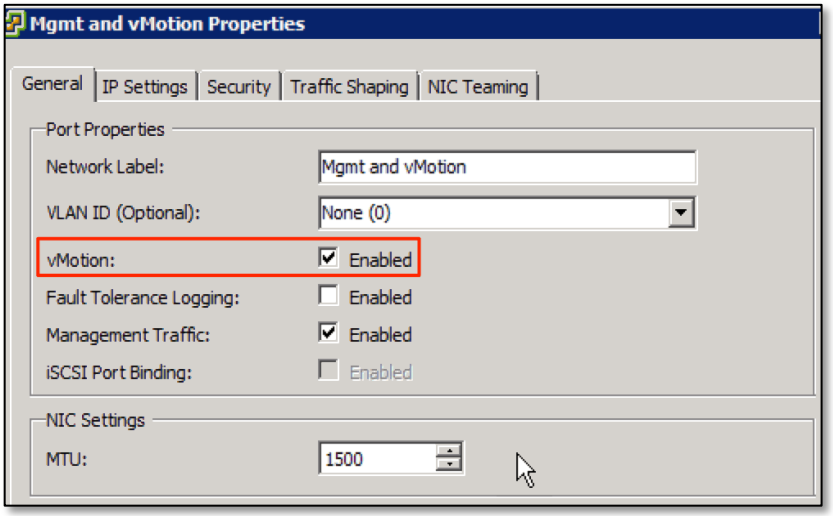

Figure 7 - Enabling vMotion on Port Properties

Beyond the basics of configuring the base ESXi system and configuring a *standard* CPPM VM and ensuring that the vMotion as shown above is configured that is all you need to do.

Using vSphere Web Client to vMotion an active-CPPM VM

There are multiple methods available from within vCenter's GUI to initiate a vMotion. Below we have shown one option. We have navigated to and we are displaying all the VM's that are registered and managed by vCenter. Another option would be to view the individual ESXi host and see the VM's installed on that host as another method.

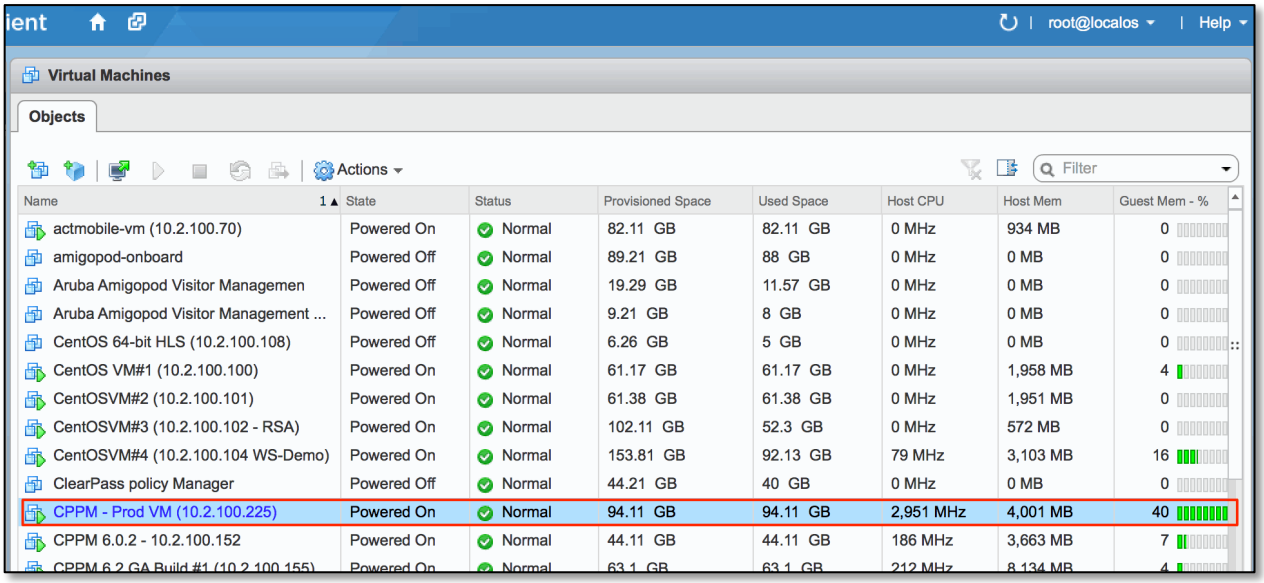

Figure 8 - Summary list of VM's

By right clicking on the VM we have selected (CPPM – Prod VM (10.2.100.225), under '**All vCenter Actions**' we can see an option to '**Migrate**' the VM.

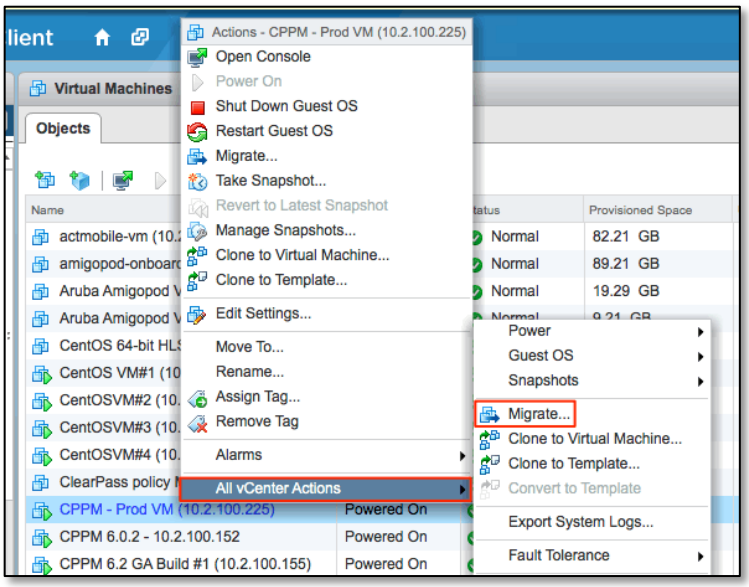

Figure 9 - Starting VMotion Migration on a VM

Choose what type of vMotion you want to perform; in our case we will change the hosting ESXi server, the first option.

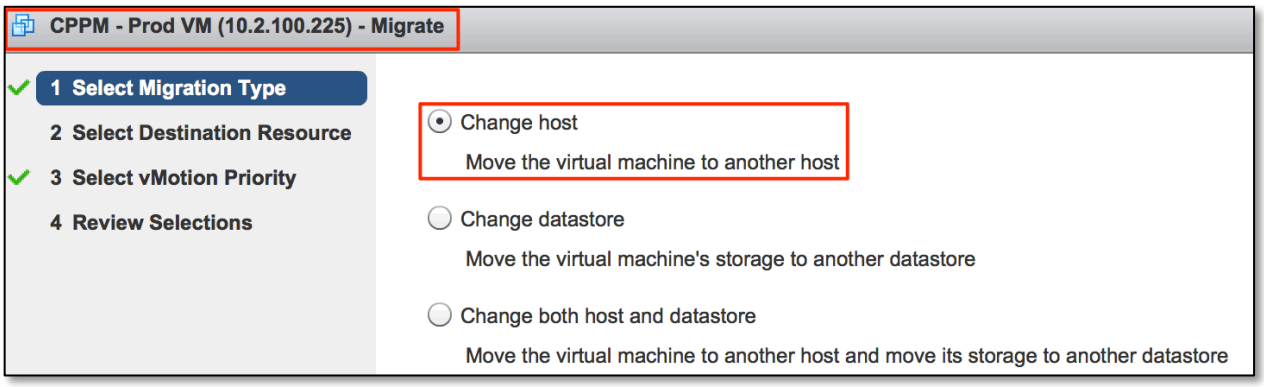

Figure 10 – Choose what type of vMotion you want to perform

Next select the target ESXi server that will be the destination server for the VM.

Figure 11 – Choose the Destination ESXi server

Once all your parameters have been selected, confirm and click on the Finish button. vCenter will now *move* the VM between the source and target ESXi servers.

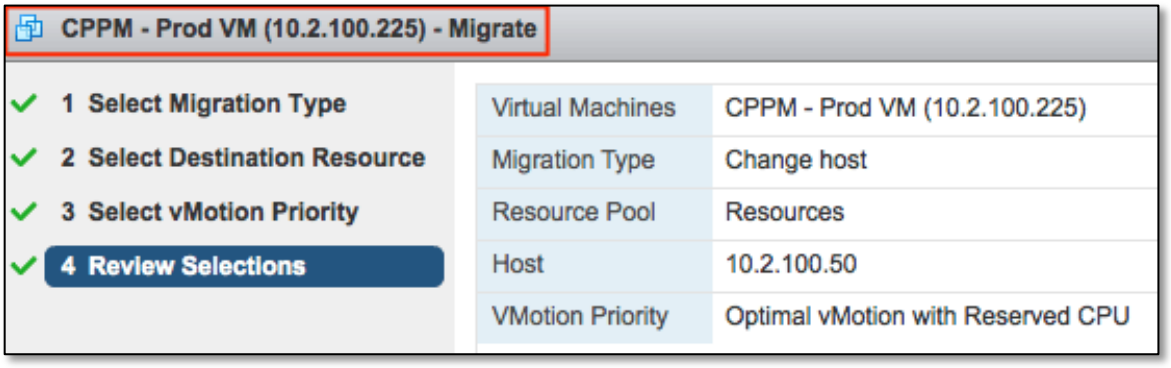

Figure 12 - Confirm the vMotion choices

Monitoring the Move

On the right-hand side of the main vCenter screen you see a visual indication under '**Recent Tasks**' of the progress of the migration. Once the move is complete a green-tick indicator is displayed as shown below for the previous vMotion we performed. You can see that the current migration is 45% complete and that the previous vMotion completed successfully.

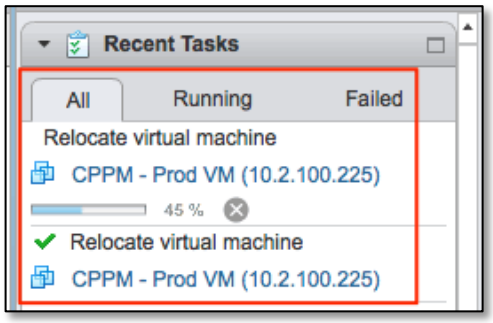

Figure 13 - In progress indicator

Note: If you use vMotion on a VM that is running ClearPass 6.2.x software, you can expect to see the following warning messages. You will still be able to successfully vMotion the VM as these are only informational messages. The messages relate to the underlying Ethernet adapter we utilize in the hardware definition of our VM when running CPPM 6.2.x. More about the changes we made to our VM hardware are detailed in - **CPPM H/W & S/W Changes between CPPM 6.3.0 v 6.2.0** later in this Tech Note.

Figure 14 - CPPM 6.2.x warning messages

To see additional details about the underlying vMotion process, i.e. the time it took for them to complete you can look under the **Monitor** then **Tasks** tab. You can see the start/completion times (2:31:02 – 2:31:11), to/from ESXi hosts (10.2.100.50 – 10.2.100.51)

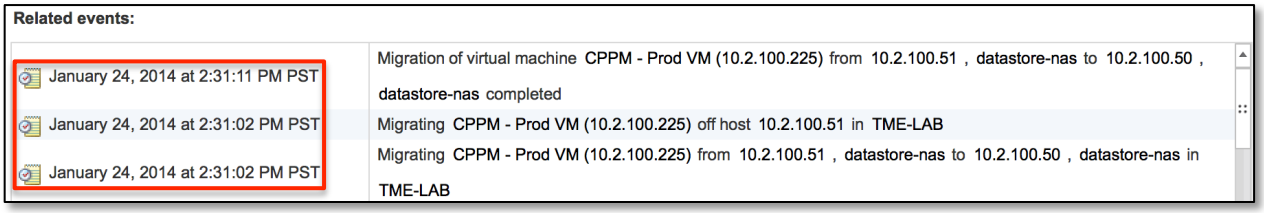

Figure 15 - Displaying vMotion Tasks (additional detail)

CPPM H/W & S/W Changes between CPPM 6.3.0 v 6.2.0

Included in CPPM 6.3.x are numerous VMware related changes, some help us specifically with vMotion, others are performance related and others are to bring the CPPM VM hardware definition up-to-date.

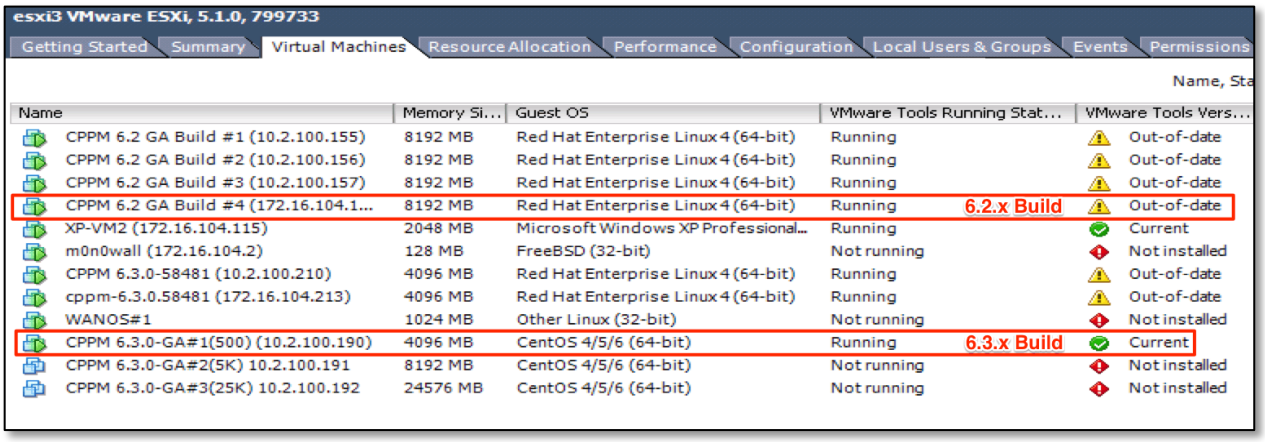

Figure 16 - CPPM VMware Tools and OS Version

We have experienced numerous instances of CPPM VMs running CPPM 6.2.x or earlier where customers have upgraded the VMware Tools we bundle with our VM's. The VMware Tools software reports as being 'Out-of-date', as shown above. However we do not support the option for the customer via the vSphere client or vCenter upgrading the VMware Tools software components. Within the CPPM 6.3 VM we have packaged the latest VMware Tools software as can be seen above for the 6.3.x VM (Current) compared to the 6.2.x VM (Out-of-date).

Additionally, changes were made in the way we report ourselves to the ESXi Hypervisor. Previously we identified ourselves as Red Hat Enterprise Linux4 (64-bit), we have corrected this and now report our base OS for CPPM as CentOS 4/5/6 (64-bit), this again can be seen above in Figure 16.

The above changes are fairly insignificant, however we also upgraded the vNIC definition we utilize when running under ESXi. Previously we used a device-driver that presented itself as a 'flexible' adapter. This would effectively run as a VMXNET adapter because VMware Tools was installed in our VM. Starting in the 6.3.x build we utilize the VMXNET3 adapter. The VMXNET3 adapter is the next generation of a para-virtualized NIC designed for performance, and is not related to the previous VMXNET or VMXNET2. It offers all the features available in VMXNET2, but adds several new features like multi-queue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery.

The below shows the Adapter type used in CPPM 6.2.x and earlier, Flexible.

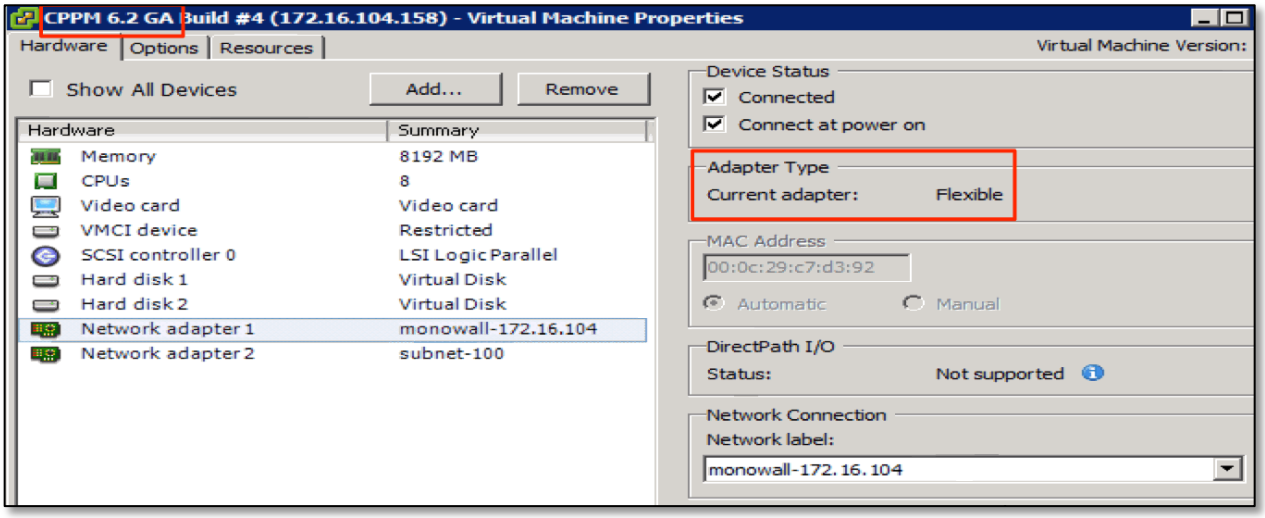

Figure 17 - CPPM 6.2.x - Flexible Adapter

The below shows the Adapter type used in CPPM 6.3.x and later, VMXNET3.

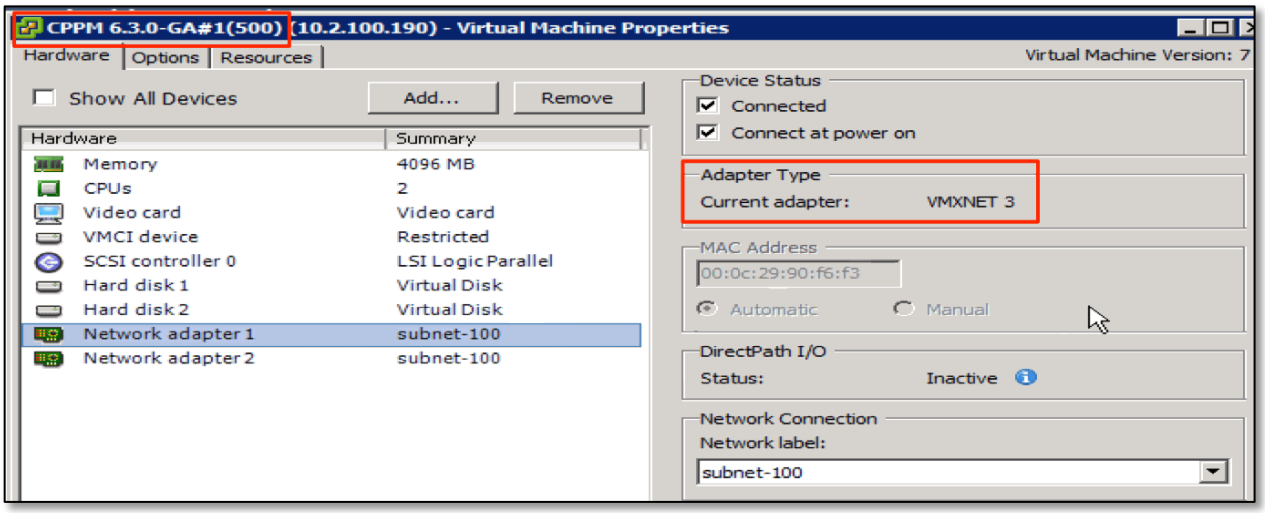

Figure 18 - CPPM 6.3.x - VMXNET3 Adapter

vMotion Failover Timings

As part of our research we performed multiple timings to understand the expected fail-over performance.

Several factors are directly related to the delay.

- Performance characteristics of the underlying ESXi Server
- Size of the CPPM VM in use
- Workload of the VM – more auth being process = more memory pages changing
- VM-500 (4GB of Memory [default] – minimum recommended size)
- VM-5k (8GB of Memory [default] – minimum recommended size)
- VM-25K (24GB of Memory [default] – minimum recommended size)
- Speed and Utilization of the underlying Network 1GB-Minimum / 10GB-Reccomended

Below is a collection of our timings; we'd expect your performance to be closely inline or better than our findings below. Whilst running the *Under-load* test we typically did not see any auth failures, we also ran a constant ping to the host with out loss of any packets.

As a rule when ran the vMotion test multiple times. The times below represent what is a 95th+ percentile of the average process time.

ClearPass 6.3.x

vMotion VM Type (RAM)	1Gbps Idle	1Gbps Under load	10Gbps Idle	10Gbps Under load
VM-500 (4MB)			~9 seconds	9 seconds
VM-5K (8MB)			~12 seconds	~14 seconds
VM-25K (24MB)			~18 seconds	~18 seconds

To expand on the testing we performed. We utilized an in-house testing tool which simulates a number of users performing RADIUS authentication and Guest Users registering through an registration portal, we also ran a constant PING to the VM. Whilst the testing automation was running we performed a vMotion'ed on the active VM, we never experienced a missed PING but did at times experience very minor Guest registration failures. In a live network, the expected user experience is that they might have to re-enter the details into the registration portal again to complete their registration.

Performance Testing was also performed for CPPM 6.2.x VM. Our results are not displayed here but the results where very similar and inline with the above for CPPM 6.3.x . However we are only officially supporting vMotion from the CPPM 6.3.x code release.

Following are copies of our 6.3 vMotion logs showing the failover times under an idle environment.

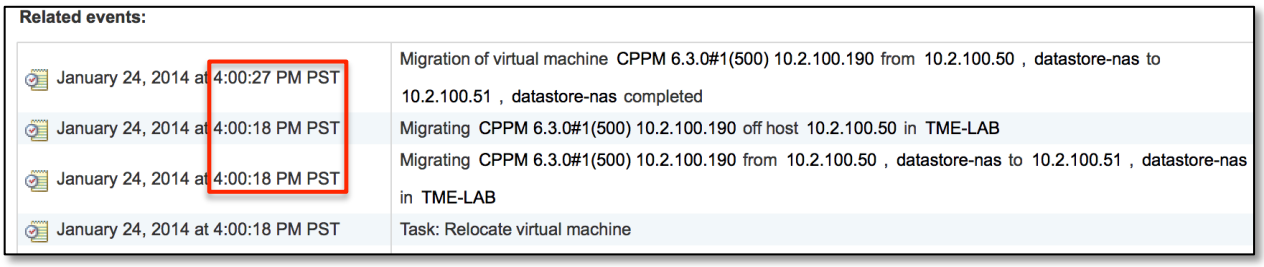

Figure 19 - CPPM 6.3.x VM-500 failover log (idle)

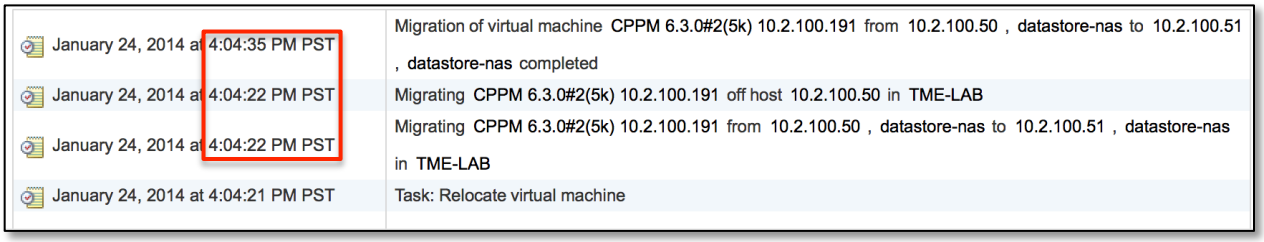

Figure 20 - CPPM 6.3.x VM-5K failover log (idle)

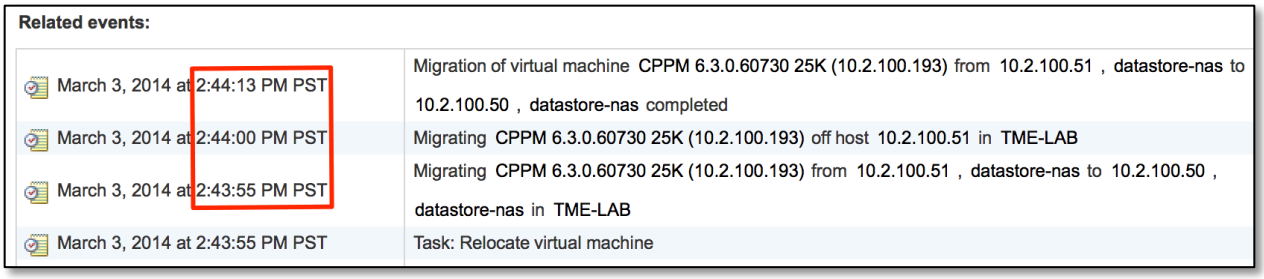

Figure 21 - CPPM 6.3.x VM-25K failover logs (idle)

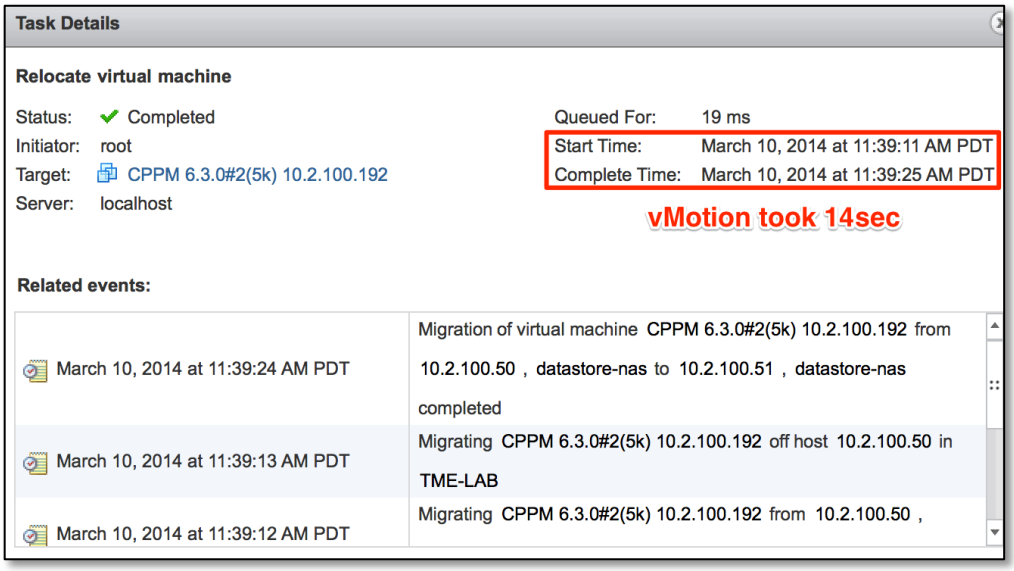

Figure 22 - CPPM 6.3.x 5K failover logs (under load)

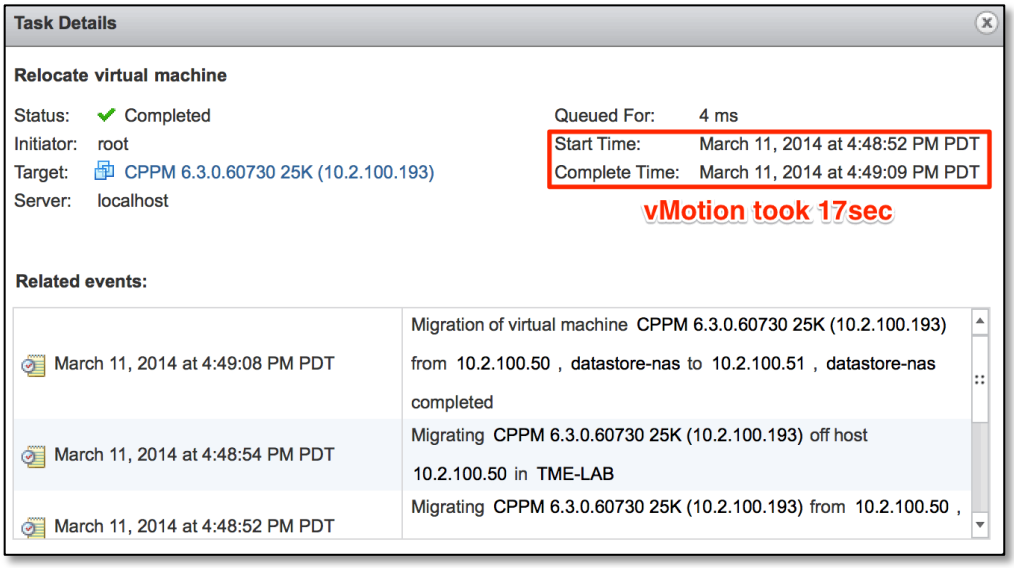

Figure 23 - CPPM 6.3.x 25K failover logs (under load)

Conclusion

Starting with CPPM 6.3.x, enabling ClearPass Virtual Machines to participate in a VMWARE vMotion HA architecture adds another dimension to the typical Networking Departments ability to engineer more available solutions and application. vMotion provides the ability to plan for network and server outages without the need to promote/reset CPPM nodes in a cluster.