Product Support Notice

PSN #	PSN020151u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 27-Oct-14. This is Issue #4, published date: 24-May-16. | Severity/risk level | High | Urgency | When convenient

Name of problem Issues to be aware of when running CM in a Virtualized Environment (VE) or on AVP.

Products affected

Avaya Aura® Communication Manager (CM), Releases 6.2 and higher

Problem description

These problems occur in Avaya Aura® Communication Manager (CM) Releases 6.2 and higher.

The following problems are not Avaya CM problems (CM product issues), but problems that can occur when running CM in an Avaya Aura® Virtualized Environment (VE - installed on a VMware® vSphere virtualized infrastructure) or on the Avaya Aura® Appliance Virtualization Platform (AVP). These problems are caused due to the VMware virtualized environment and must be addressed by the entity responsible for VMware infrastructure and environment support.

Note: If Avaya Support is requested to troubleshoot VMware infrastructure/environment issues for CM running in a Virtualized Environment (VE), Time and Materials (T&M) charges will likely apply.

PROBLEM 1

In a duplicated server configuration the CM servers might end up in an active/active state temporarily. The active CM server hangs, CM interchanges to the standby server, the active server returns from a hung state, CM runs in an active/active state for a brief period until the CM arbiter resolves the dual active state and CM returns to the expected active/standby state again. In this specific scenario CM is working as designed. The reason for the active server hanging is the root cause of the problem and should be addressed.

For this issue the CM ecs logs will show something similar to the following:

Previously standby (now active) server ecs logs showing an interchange due to the active server being in a hung state:

```
2015-1117-221749 was standby.log:
20151123:101602408:716:Arbiter(5802):MED:[Heartbeat Timeout from alt side]<<< Standby lost heartbeat to Active
20151123:101602408:717:Arbiter(5802):MED:[  with errno=Interrupted system call[4]]
20151123:101602408:718:Arbiter(5802):HIGH:[Heartbeat Timeout from ACTIVE]
20151123:101602408:719:Arbiter(5802):MED:[STANDBY->ACTIVE :other side reset]
20151123:101602408:720:Arbiter(5802):MED:[finite_state_machine():State Transition: STANDBY to ACTIVE ]
20151123:101602408:721:Arbiter(5802):MED:[reset_active_timer: bucket 17.0 to 0]
20151123:101602408:722:Arbiter(5802):HIGH:[Interchange STANDBY/AUXSTBY TO ACTIVE]<<< Interchange to Standby
20151123:101602409:723:Arbiter(5802):MED:[finite_state_machine(): Interchange Reason: Hung Server]
```

Previously active (now standby) server ecs logs after the server is no longer in a hung state and now in a dual active state:

```
20151123:101626007:816266:Arbiter(5735):MED:[dual-active detection: me 0@14 vs msg 0@17]<<< Active/Active State
20151123:101626007:816267:Arbiter(5735):MED:[update: Received IPAT_ACTV message from the Standby server]
20151123:101626007:816268:Arbiter(5735):MED:[remot: gmm 0100, pcd 00/00, dup 230, wd 01, hmm 01, pe 0304, actv
017]
20151123:101626007:816269:Arbiter(5735):MED:[State of other side is ACTIVE ]
20151123:101626007:816270:Arbiter(5735):MED:[dual-active resolution: I stay active]
20151123:101626008:816271:Arbiter(5735):MED:[dual-active detection: me 0@14 vs msg 0@0]
20151123:101626008:816272:Arbiter(5735):MED:[remot: gmm 0300, pcd 00/00, dup a30, wd 01, hmm 01, pe 0304, actv
000]
20151123:101626008:816273:Arbiter(5735):MED:[ACTIVE ->STANDBY:dual-active backoff]<<< Dual Active Resolution
20151123:101626008:816274:Arbiter(5735):MED:[finite_state_machine():State Transition: ACTIVE  to STANDBY]
```

Previously active (now standby) server ecs logs might show the active server getting "backed up" (hung), similar to the following:

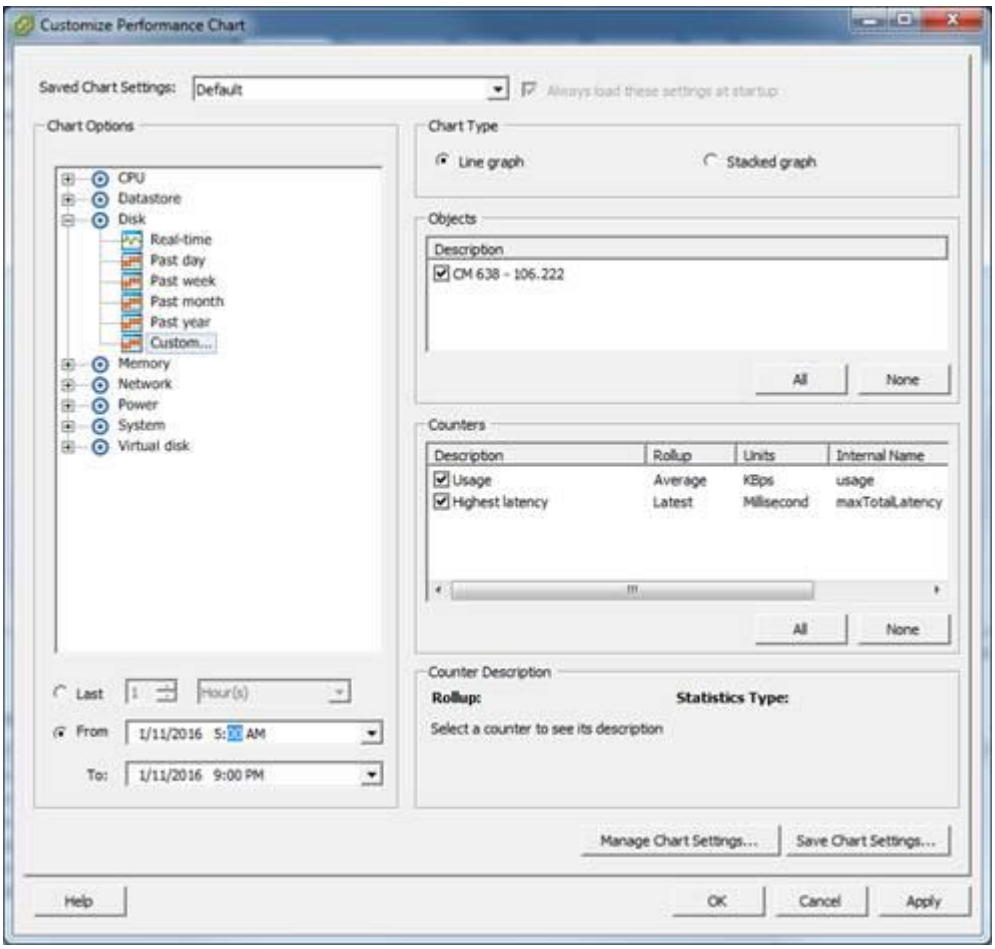
```
20140802:032528611:7581530:tim(9913):MED:[def_main: backed up cur_max 106 max 123]
20140802:032530718:7581531:tim(9913):MED:[def_main: caught up cur_max 106 max 123]
20140802:034234744:7581673:tim(9913):MED:[def_main: backed up cur_max 63 max 123]
20140802:034235976:7581675:tim(9913):MED:[def_main: caught up cur_max 63 max 123]
```

Note the "cur_max" value shows the amount of time (in 20ms intervals) the server was backed up/hung at the time of the log entry, and the "max" value shows the largest amount of time (in 20ms intervals) the server has been backed up/hung historically. For example, the "cur_max 63" entry means the server was backed up/hung for 63 x 20ms = 1,260 ms or 1.26 seconds.

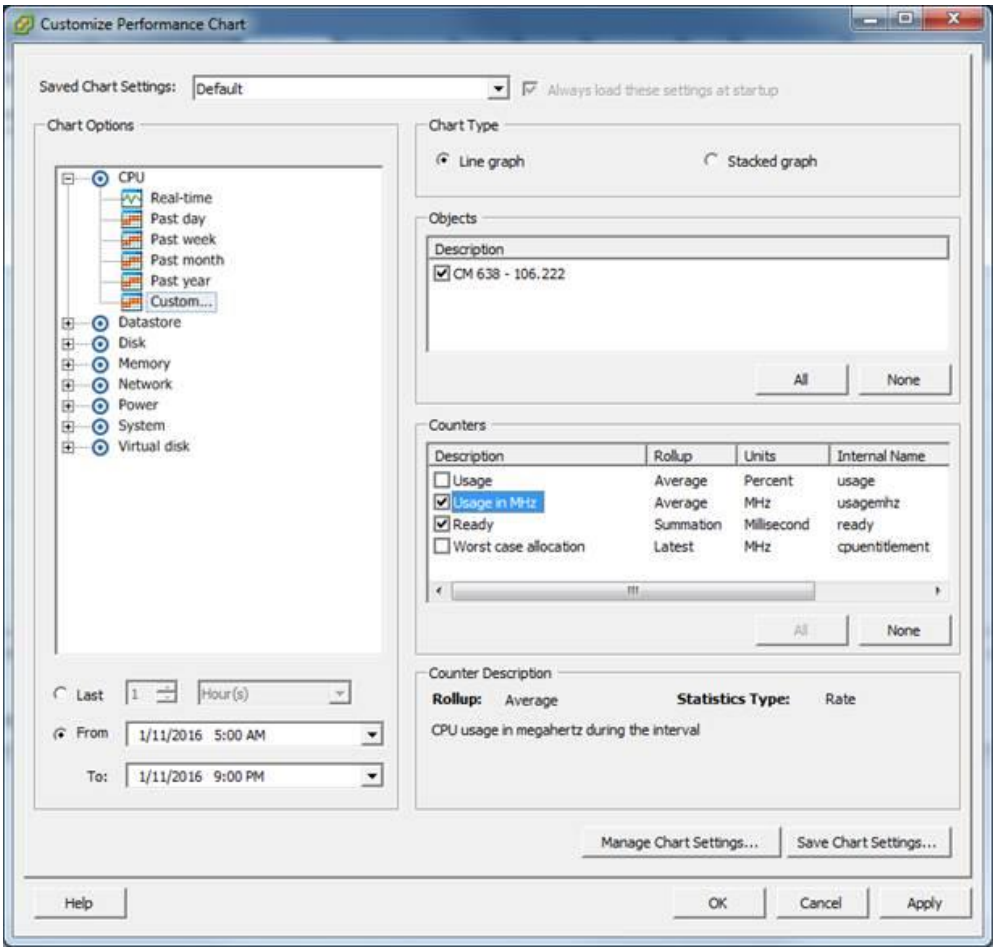
The following VMware data must be collected from the VMware ESXi and VCenter servers to determine the root cause.

- vm-support bundles from the ESXi hosts
- Performance charts from Vcenter for the CM Virtual Machines (VMs) during a time range starting (*From*) 2 hours before the interchange until (*To*) 2 hours after the interchange. If there is no access to vCenter (or if CM is running on AVP), the performance data must be collected from the ESXi client, but in this case historical data might be limited to the previous hour only:

  Collect the disk performance chart. Select *Disk* in *Chart Options* with *Custom Date/time*, and select the timeframe described in the above bullet. Make sure *Usage* and *Highest Latency* are selected. Example:



Collect the CPU usage chart for the two CM VMs for the same timeframe with *Usage in MHz* and *Ready* time selected. Example:



The problem might be caused by ESXi connectivity issues with the datastore/Storage Area Network (SAN). If this is the case, the disk usage chart will show something similar to the following. Note the end of the graph shows increased disk (datastore) latency going from virtually nothing to around 800ms (.8 seconds) for a disk write operation:

In addition, the ESXi host and datastore logs might show ESXi host connectivity issues with the datastore. Examples of ESXi host warning event Descriptions in the *Task & Events* tab for *Inventory > Datastores and Datastore Clusters*:

Lost access to volume <volume name> *due to connectivity issues. Recovery attempt is in progress and outcome will be reported shortly.*

Path redundancy to storage device <device name> *degraded. Path* <actual path> *is down. Affected datastores:* <datastore name(s)>.

The problem might be caused by CM CPU starvation due to ESXi host over-subscription without using reservations. If this is the case, the CPU usage chart will show something similar to the following two screen captures. In the first screen capture note the CM VM CPU ready time increasing to 1.5 to 2 second delays. Note the second screen capture is more extreme and the CM VM has to wait 32 seconds to get CPU time from the host.

PROBLEM 2

Duplication link bandwidth or connectivity issues might cause active/active states, filesync failures, server interchanges, server resets, or other non-deterministic behavior.

PROBLEM 3

Use of virtual machine (VM) snapshots on CM can cause interchanges or adversely impact service in other ways. Extreme caution must be exercised when using virtual machine snapshots with CM deployed on VMware.

PROBLEM 4
Use of vMotion with real-time (i.e., CM) applications can be service impacting and is not recommended.

Resolution

The Duplicated Avaya Aura® Communication Manager on VMware document provides best practices on deploying duplicated CM servers in a VE configuration and should be referenced for any duplicated CM VE deployment.

PROBLEM 1
Storage arrays (datastores) should be architected to tolerate drive failures, controller failures, and connectivity issues without disruption to service. For increased reliability and redundancy and to minimize the impact of datastore/SAN connectivity issues it is recommended that active and standby CM duplicated servers use different/separate datastores.

If ESXi hosts are over-subscribed, CM CPU reservations must be used. Refer to the Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment (6.x VE only) and/or Deploying Avaya Aura® Communication Manager in Virtualized Environment (7.x VE and AVP) documents on Avaya Support for reservation guidelines. In addition, VMware recommends allocating to each Virtual Machine (VM) only as much virtual hardware as the VM requires. Provisioning a VM with more resources than it requires can, in some cases, reduce performance of the VM as well as other VMs sharing the same host. Refer to the Performance Best Practices for VMware vSphere 5.5 document, especially the "ESXi CPU Considerations" section, for more detailed information.

PROBLEM 2
The CM duplication link must have 1Gbps total capacity and it must be dedicated to CM duplication. Due to 1 Gbps being required to support the duplication link, the duplication link interface should be a separate and dedicated interface. Refer to PSN003556u on Avaya Support for additional information.

PROBLEM 3
Snapshot operations should never be performed on the active CM VM. Before performing any snapshot operation, the application running on the VM, in this case CM, must be stopped or placed out-of-service. When the snapshot operation is complete the application should be started or brought back into service.

If the duplex Open Virtual Application (OVA) is in use, snapshot operations should be performed on the standby CM VM after ensuring the standby is refreshed. If a snapshot is taken on the active VM a service impacting interchange is likely to occur.

Snapshots should not be used as a backup/recovery mechanism. They are only intended to test an action that may result in an unpredictable outcome.

A snapshot should never remain on a system for more than 48 – 72 hours before being deleted or reverted. Additional information on snapshot removal can be found at KB1002836 .

Additionally, third party based snapshots are not supported.

Best practices for snapshots are documented in the Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment document.

PROBLEM 4
If vMotion is used, it is recommended that manual migrations with vMotion be done only during a maintenance window since the migration could be service impacting. If vMotion DRS automation is used, it is recommended that the DRS automation level be set to the most conservative level possible, such as level 2 or level 1.

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch	
n/a	
Download	
n/a	
Patch install instructions	Service-interrupting?
n/a	Yes
Verification	
n/a	
Failure	
n/a	
Patch uninstall instructions	
n/a	

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks
n/a
Avaya Security Vulnerability Classification
Not Susceptible
Mitigation
n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686