TMS Agent Troubleshooting procedures for Cisco TelePresence VCS and TMS

Reference Guide

Cisco VCS
Cisco TMS

April 2012

Table of Contents

Pre-requisites

Please refer to the pre-requisites outlined in the reference guides below. This guide does not cover VCS Clustering. If a VCS Cluster is in place, it is recommended that each VCS in the cluster should be operational and replicating configuration before enabling TMS Agent replication.

Reference guides

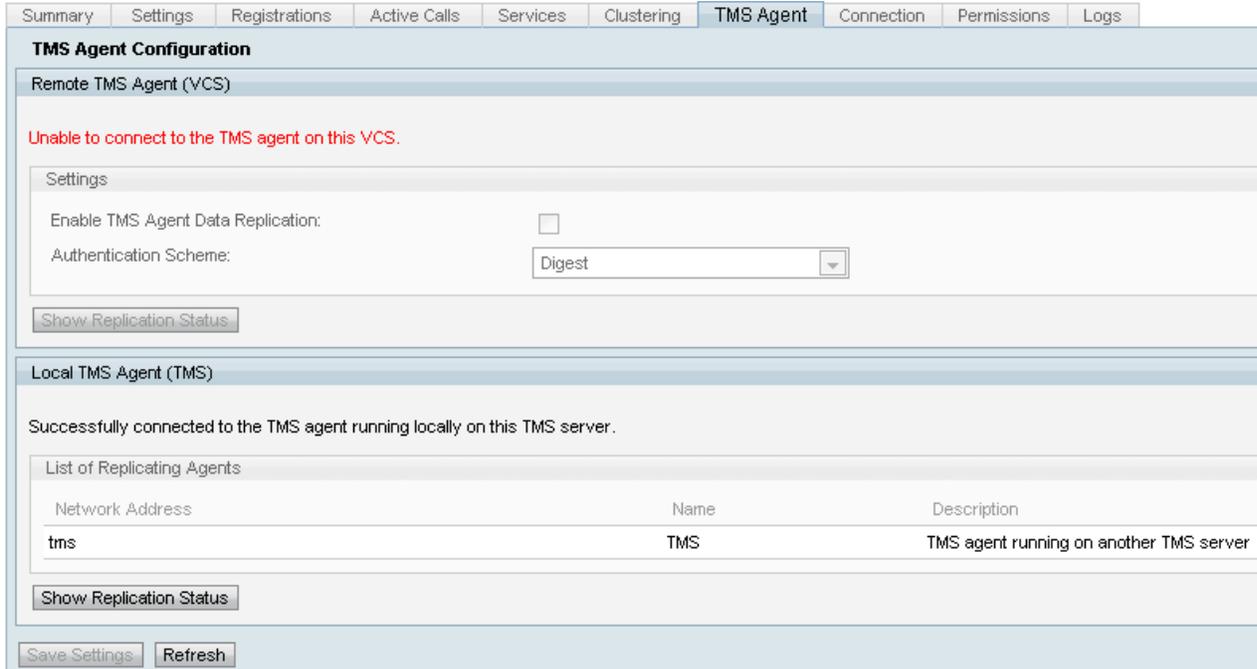TMS Provisioning Deployment Guide

TMS Provisioning Troubleshooting Guide

VCS Authenticating Devices Deployment Guide X7.1

VCS Authenticating Devices Deployment Guide X7.0

VCS Authenticating Devices Deployment Guide X6.1

Errors when enabling TMS Agent on a Single VCS

Unable to connect to the Remote TMS agent

Verify that a DNS hostname is supplied in the connection tab for the VCS. DNS needs to be setup correctly for the TMS Server to be able to properly connect to the Remote TMS Agent. See DNS Items to Check. Also verify that the Device provisioning key is installed. If it is installed try to reboot the VCS Control. If you see this message on a VCS Expressway this is normal behavior, as a VCS Expressway should not have the device provisioning key installed.

Failed to enable TMS agent data replication

If you get the following message "Failed to enable TMS agent data replication" message from the activity status page and there are no errors regarding the reason for failure, follow the steps below. If a reason for failure exists, check the other common errors included in this guide.

Rebuilding the TMS Agent database on VCS

WARNING: The following steps will cause Movi user login failure. Current logged in users will remain logged in but new users will be unable to login until replication has completed.

Disabling replication on TMS

1. On the TMS's Systems navigator page, click on the VCS and then select the TMS Agent tab. Verify that the replication check box is unchecked on each VCS.
2. Wait for the process to complete (this will take several minutes. It will be completed when it reports complete on the activity status page.)

Reinstalling the TMS Agent database on VCS

1. SSH into each VCS peer using the root login.
2. Type tmsagent_destroy_and_purge_data on each VCS.
3. Read the disclaimers and press Y
   Do this until it says OK

If these continue to fail after about 3 times type the following commands in the order listed below:
4. /etc/init.d/S77provisioning stop
5. /etc/init.d/S76opends stop
6. /etc/init.d/S76opends uninstall
7. /etc/init.d/S76opends start
8. /etc/init.d/S77provisioning start

If it still fails, remove the device provisioning key and wait about 2-5 minutes. Reboot the VCS, add the key back, and wait another 2-5 minutes. Next run the tmsagent_destroy_and_purge_data command to get visual confirmation of it working. Replication can now be enabled.

Directory Service not running

If an alarm exists on the VCS indicating that the directory service is not running, reboot the VCS. If the alarm remains please follow the above instructions for Rebuilding the TMS Agent database on VCS.

VCS was not found in the list of replicating agents

The VCS will not show up in the list of replicating agents until the TMS Agent has successfully replicated the provisioning data to it. If you receive the following error on the TMS Agent tab in Systems -> Navigator follow the steps below:

> TMS agent data replication is enabled, but the network address of this VCS was not found in the list of replicating agents read from the local TMS agent. If you have recently enabled data replication for this system, please wait and refresh after the background event on the TMS Server setting up the replication has finished. If not, try to reenable the replication by turning if off and then back on again.

1. Wait and refresh after 2-5 minutes. Try to re-enable the replication by disabling and enabling again. If it fails again, check to make sure the TMS can communicate with the VCS on the following ports:

Service	Protocol	Port	Direction (relative to TMS)	
			In	Out
TMS-Agent data	TCP	8989	X	X
TMS-Agent Administrative functions	TCP	4444	X	X

Port 8989 is the replicating port used between all replicating partners meaning this port needs to be open between each TMS and VCS in the network. The traffic exchanged on this port is encrypted.

If a firewall is located between the TMS and VCS, port 80 (http) and 443 (https) will need to be open in addition to the ports above.

DNS Errors enabling replication

If you receive the following error:

- Unable to enable replication for 'vcs'. A DNS lookup of the TMS host name on this VCS does not match the TMS IP address.
- Failed to enable TMS agent data replication for 'vcs'
- The event failed to complete. Details: TMS agent data replication setup failed for the following system(s): vcs

DNS Items to Check

1. Remote Desktop into the TMS, open command prompt and execute the command: nslookup of the FQDN which matches the Network Address at the bottom of the TMS Agent settings page. The page can be found by selecting Administrative Tools -> Configuration. TMS example: **nslookup TANDBERG-MS.tandberg.com**

If TMS is in a redundant set up, each TMS will need a resolvable forward record.

The records do not have to match the physical hostname of the windows box, but if you have more than one forward or reverse lookup assigned to a different hostname or ip address this can cause the DNS lookup to fail.

Once the forward record for the TMS are created this should no longer be a problem.

We have seen cases where multiple DNS reverse records could cause issues in older TMS versions. To eliminate this issue only one reverse record is recommended. You can verify this by doing a nslookup of the ip address. Example: nslookup 10.10.0.1

Restoring the local TMS Agent from the Remote TMS Agent

Note: This is used if the TMS Agent database on the TMS Server is corrupt but the VCS database is operational or if a known working backup from the TMS does not exist.

1. Stop TMS agent replication for the VCS following the Disabling Replication Instructions
2. Go to the Maintenance -> Backup and restore page on the VCS and click the "Create TMS Agent backup file" button.
   The file will save as a tar.gz file.
3. Open the tar.gz file in 7-Zip and click the folders until it looks like the picture below

Name	Size	Packed Size	Modified	Mode	User	Group
config	1 154 583	1 155 072	2011-11-07 13:42	0rwxr-xr-x	root	root
replicationChanges	229 807	230 400	2011-11-07 13:42	0rwxr-xr-x	root	root
schema	580 322	581 120	2011-11-07 13:42	0rwxr-xr-x	root	root
tasks	978	1 536	2011-11-07 13:42	0rwxr-xr-x	root	root
userRoot	980 197	980 480	2011-11-07 13:42	0rwxr-xr-x	root	root
app.config	278	512	2011-10-28 09:53	0rw-r--r--	root	root

4. Extract the files to a known location
5. Select on the files and right click as seen below
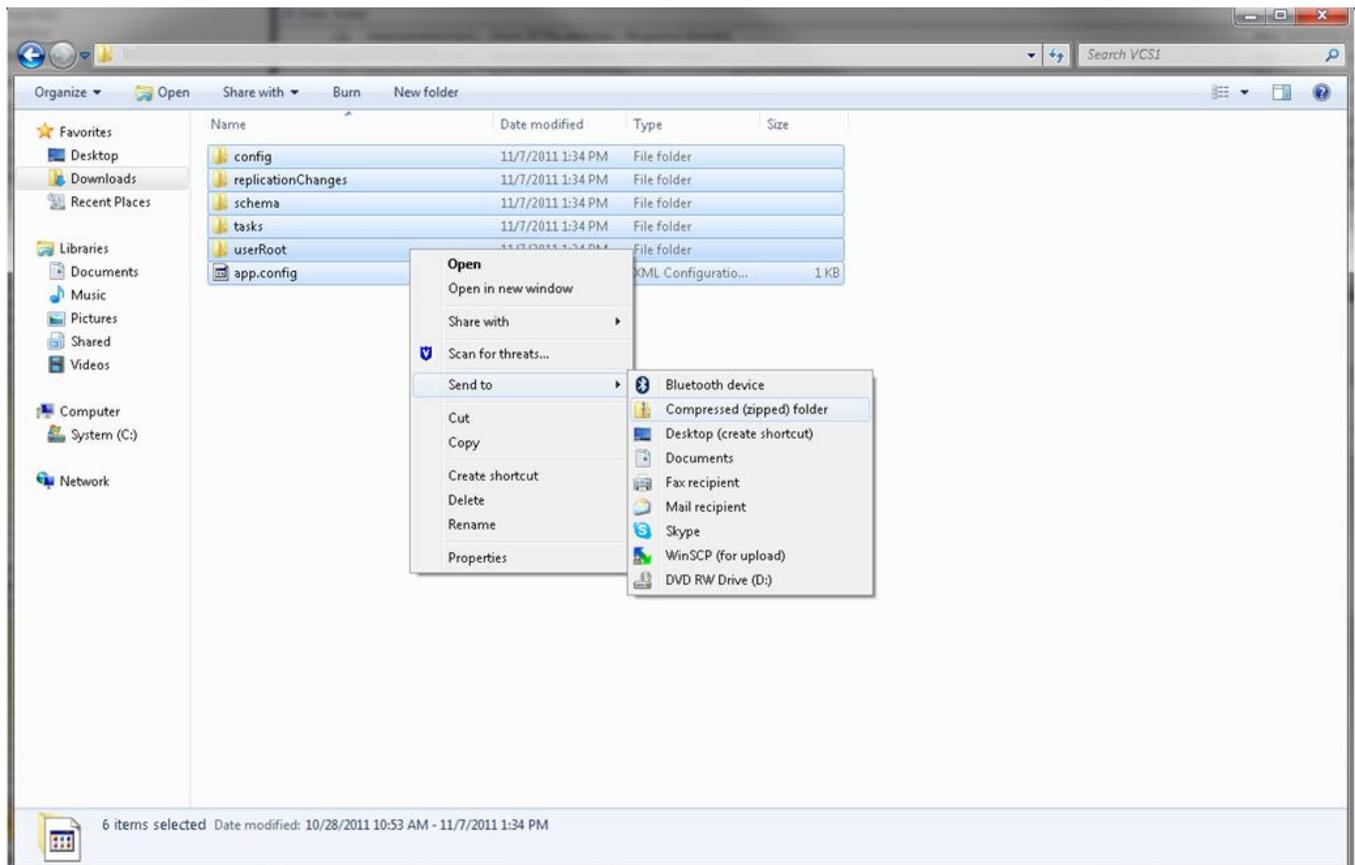
6. Once the zipped folder has been created, verify that all the folders show up within the file by double clicking on the zip folder.
Note: If you double click the zipped folder and there is a single directory that you have to click into to view the folders and app.config the process will not work!

7. Rename the folder to "TMSAgentBackup.<year><month><day><time>" Example: TMSAgentBackup.201011071300
The time should be in 24 hour format. For instance, in my example it is 1:00pm

8. Verify that replication on all devices are disabled. This includes replication between TMS Agents in a TMS redundant setup.

9. Clear the List of Replicating Agents on the Administrative Tools -> Configuration -> TMS Agent Settings page

10. RDP into the TMS and go to the Backup Directory stated on the TMS Agent Settings page

11. Copy the new file called TMSAgentBackup.201011071300.zip into the Backup Directory.

12. Refresh the TMS Agent Settings page. This will add the newly added file into the drop down box as seen in the picture below
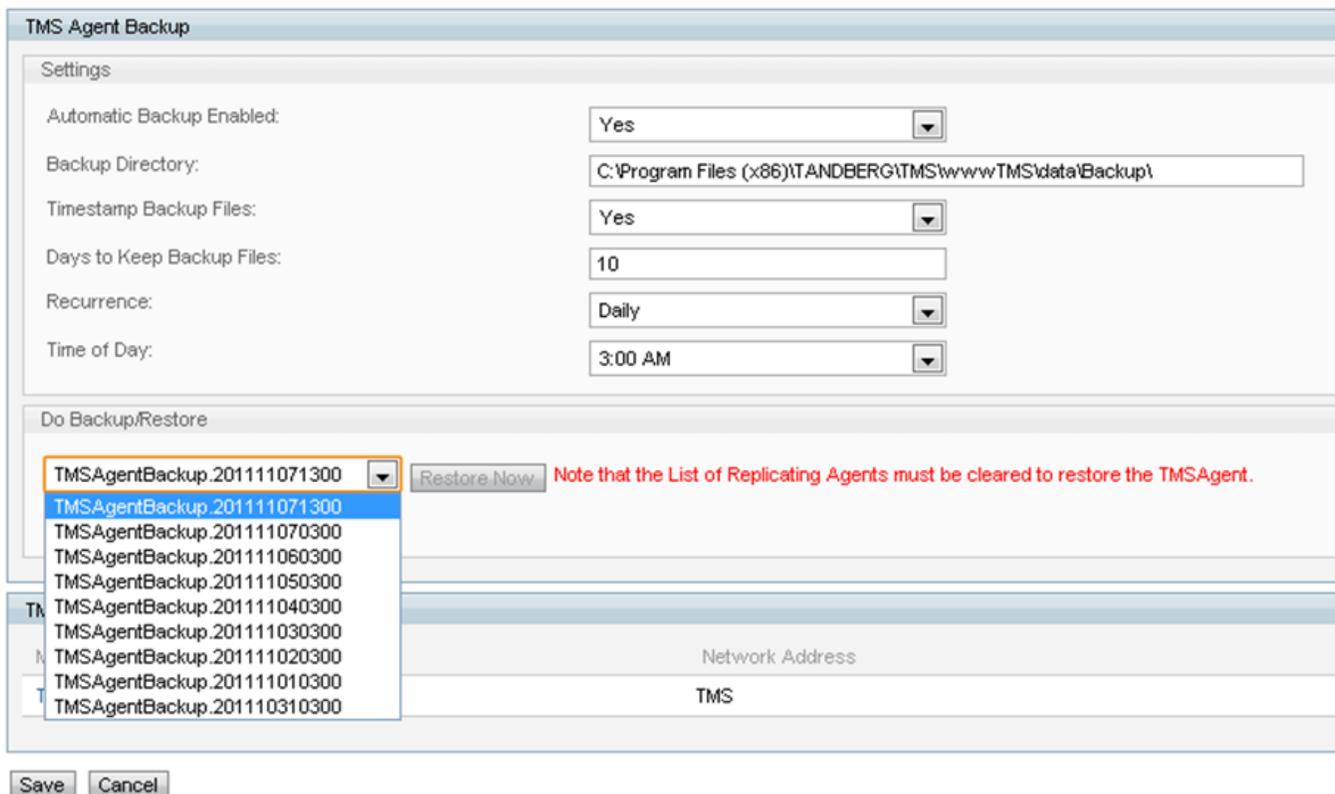
13. Then click the Restore Now button.
14. Once the TMS agent data restore is successful, run the TMS agent diagnostics on the local TMS Agent
15. Go to the provisioning directory and verify the configuration and users are showing up.
16. Re-enable replication on the VCS.

Manually Rebuild the Indexes for the local TMS Agent database

This process is to be used if you are running TMS version 13.1 or later and are receiving index errors while running the local TMS Agent diagnostics after you have clicked the "Fix" button.

1. RDP into the TMS
2. Go to start run and type: %OPENDS_HOME%\bat
3. Open the file control-panel.bat and log in with the LDAP Configuration Password (Default is TANDBERG) It should look like below:
4. Click Verify Indexes

5. This will bring up a screen like below:
6. Select all Available Indexes and click the Add > button.
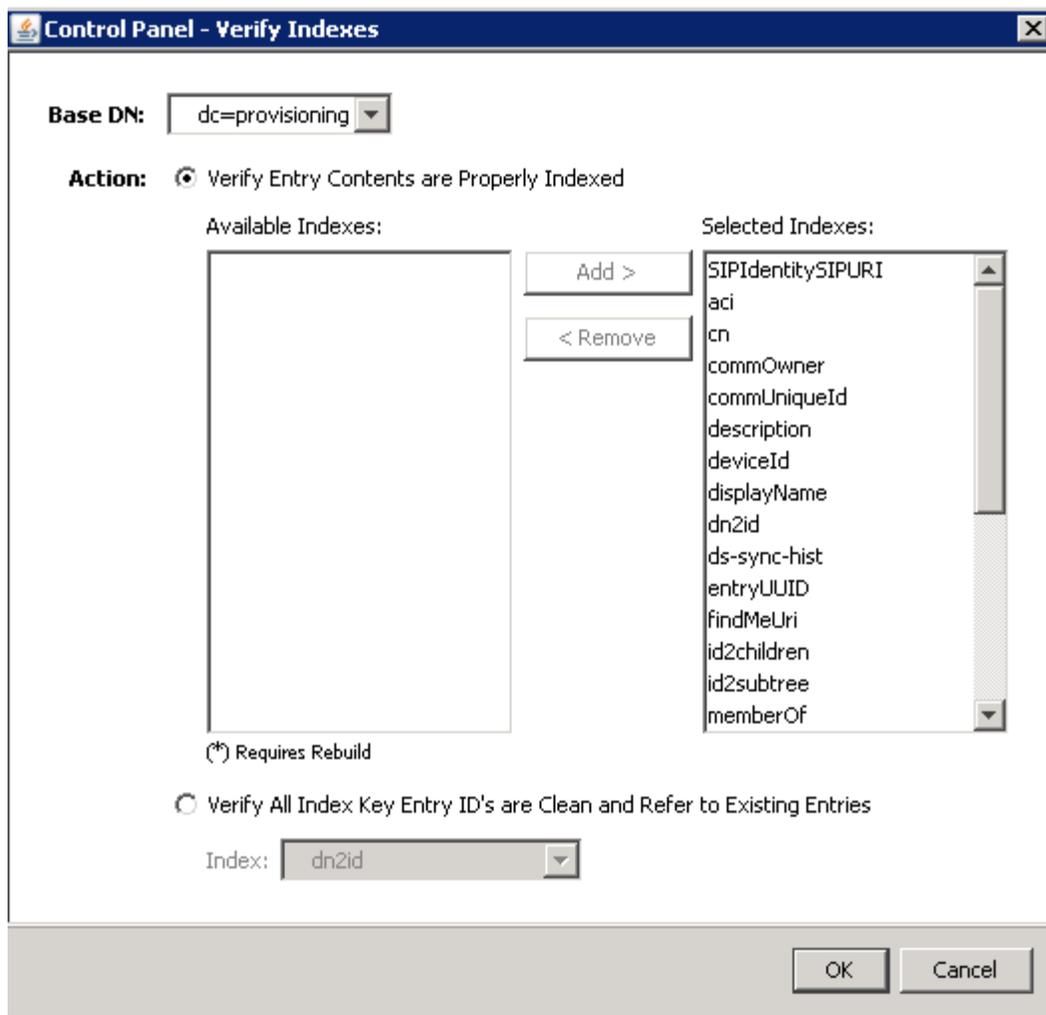
7. After this finishes, do the same thing again, but select rebuild indexes on the OpenDS control panel page.

Enabling TMS Agent in a high latency environment

When enabling replication on VCSs, 300ms is the maximum round-trip latency allowed for the TMS agent to properly operate/replicate to all of the replicating peers (any device that TMS Agent is running such as TMSs and VCSs). If the round-trip latency is above 200ms between any of these replicating peers your infrastructure may experience issues with replication.

If you have a high latency network, you will most likely experience issues while enabling replication and it will go one of three ways.

1. Replication is successful
2. Errors are received **before** the Initialize TMS agent method
3. Errors are received **after** the Initialize TMS agent method

Steps to troubleshoot the two errors:

While replication is executing, click on the Enable TMS agent data replication for system(s) event from the activity status page to track its progress.

As it is replicating you will need to refresh the page as this will not be done automatically.

If you receive errors **before** the "Initialize TMS agent on VCS Name" go to *Rebuilding the OpenDS database on VCS*

If you receive any errors **after** the "Initialize TMS agent on VCS Name" status, run the TMS Agent diagnostics for the VCS on the TMS Agent diagnostics page. If you receive mostly green checks, test your Jabber/Movi clients to see if they login. All red checks indicate the replication process has failed and requires executing the *Rebuilding the OpenDS database on VCS*

Resetting the TMS Agent database password on TMS

If you receive the unknown error when setting the TMS Agent password on the TMS Agent settings page, this procedure can be followed to reset the Directory Manager Password to the default of TANDBERG. This should be done when replication on all devices have been disabled. This includes replication between TMS Agents in a TMS redundant setup.

1. Open command prompt
2. Go to the OpenDS-2.0\bat directory:
   cd %OPENDS_HOME%\bat
3. Run this command:
   encode-password.bat -s SSHA512 -c TANDBERG > C:\ENCPASSWORD.txt
4. Stop the TMSAgents Windows Service, which will also stop the OpenDS Windows Service
5. Open the file:
   %OPENDS_HOME%\config\config.ldif
6. Find the section:
   dn: cn=Directory Manager,cn=Root DNs,cn=config
   objectClass: person
   objectClass: organizationalPerson
   objectClass: inetOrgPerson
   objectClass: top
   objectClass: ds-cfg-root-dn-user
   userPassword:
   {SSHA512}KFfaERuBiOesVUg/mf7EB4xqq5eOOPFDuVBiZCPaBetrgN92rwbeJTPiP
   Z+I3ferqN8D4UgnA5jIBLRbrtUFT9Jld/vN85dg

7. Replace the userPassword string with the sting in the ENCPASSWORD.TXT file (without the quotes)
8. Remove or rename the app.config file located in the following directory: TANDBERG\TMS\wwwTMS\Data\TMSAgent\app.config
9. Start the TMSAgent Windows Service, wait about 1 minute and it will start the OpenDS Windows Service as well.
10. In the TMS Portal, go to Administrative Tools > TMS Agent Settings
11. Change the password fields to TANDBERG
12. Once the process is complete:
Stop the TMSAgent Windows Service, which will also stop the OpenDS Service
13. Remove or rename the app.config:
TANDBERG\TMS\wwwTMS\Data\TMSAgent\app.config
14. Start the TMSAgent Windows Service, which will restart the OpenDS Windows Service

Another way to verify that the TMSAgent Windows service and OpenDS Windows service are running is to open Windows Task Manager and select the Processes tab to verify that there are 2 java.exe processes running. The first process starts quickly. The second instance may take a minute or 2 to start. This means the services are running but doesn't guarantee that they are running properly.
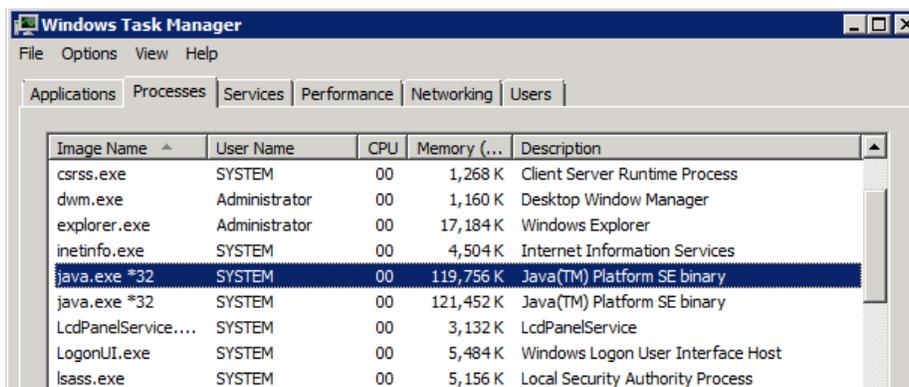
Checking the Replication Status

Checking the replication status of a VCS can help identify replication issues. To check this, go to Systems Navigator and select the VCS. Click on the TMS Agent tab and select the "Show replication status" button. You will get a drop down box that looks like the image below:

```
Replication Status

dc=provisioning - Replication Enabled
=======================================
Server : Entries : M.C. (1) : A.O.M.C. (2) : Port (3) : Security (4)
-----------------------:---------:----------:---------------:----------:-------------
TMS:4444 : 67 : 0 : N/A : 8989 : Enabled
vcs1:4444 : 67 : 0 : N/A : 8989 : Enabled

[1] The number of changes that are still missing on this server (and that have been applied to at least one of the other servers).
[2] Age of oldest missing change: the date on which the oldest change that has not arrived on this server was generated.
[3] The port used to communicate between the servers whose contents are being replicated.
[4] Whether the replication communication through the replication port is encrypted or not.

Show Replication Status
```

If there are errors in this box, it will help you determine the next steps to fix the replication issue and will also indicate if a port is being blocked.