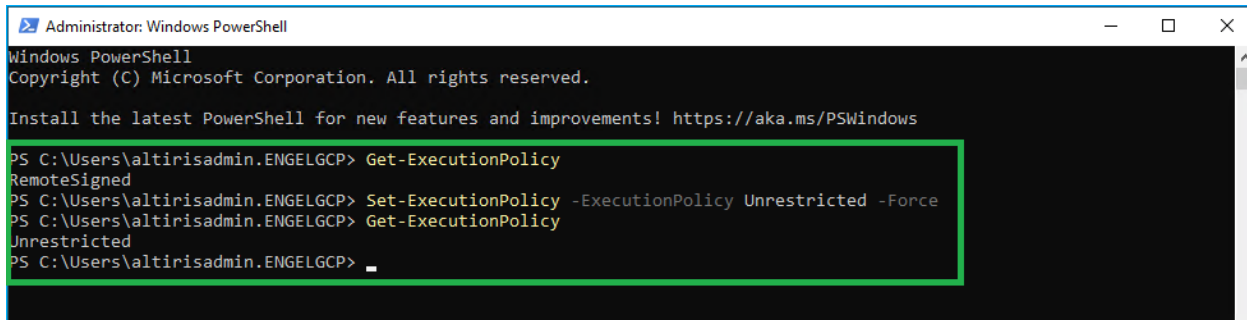# SMP Diag Script

Important: In order to execute this PowerShell script, you must first change the execution policy on the SMP server. To do this, open a PowerShell session as an administrator and run the following command: Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Force
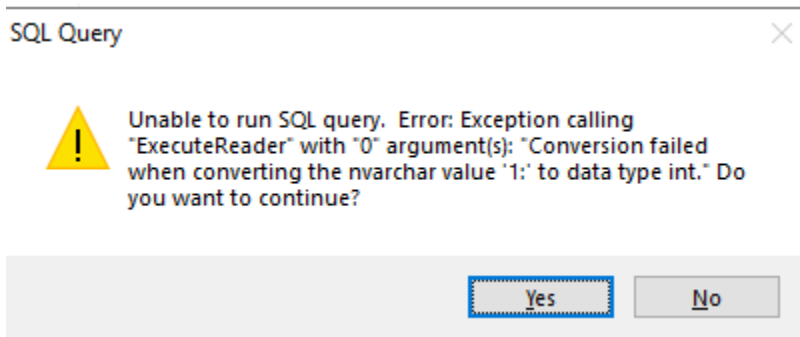

This script needs to run as the Application Identity. Please make sure to login to the SMP server with this account. This is required because the application identity account should have access to run the SQL queries inside the script.

When executing the script you may receive the following warning. You should click Yes to continue. If you continue receiving this warning, most likely SQL queries are failing to execute. At times one query will fail, but others will succeed.

When executing this script the following checks will be performed:

- Make sure this script is running as the Application Identity Account. We check the AeXSvc service Logon Name to make sure it matches the currently logged in user.
  - If this fails, the entire script will stop running.

- Check to see if this script is running on an SMP server by checking the HKLM:\SOFTWARE\Altiris\eXpress\Notification Server registry path.
  - If this fails, the entire script will stop running. Script must be run from SMP server.

- Creates a directory on C drive of SMP called SMPDiagLog

- Creates an HTML file in c:\SMPDiagLog called SMPDiag.html

- Attempt to get the SQL Server name from the registry
  HKLM:\SOFTWARE\Altiris\AIM\Configuration\NsConfiguration SqlServerName value
  - If this fails the script will stop running

- Retrieve the SMP Database name. For example Symantec_CMDB. From
  HKLM:\SOFTWARE\Altiris\AIM\Configuration\NsConfiguration DatabaseName value
  - If this fails the script will stop running

- Need to ping SQL Server name to make sure it's accessible. The script needs to be able
  to communicate with the SQL server.
  - If it cannot be resolved through a ping test, the script will stop running.

If the above is successful the script will now begin running tests.

If any of the following tests fail to run, it will prompt the end user to continue or not. This is done
because one test may fail, yet the rest may run.

Symantec Management Platform (SMP) Tests:

1. This test will check if the log severity of the SMP server is set higher than default decimal
   value of 7.
2. This will check to see if User Access Control is set down to Never Notify.
3. Check if the registry key HKLM:\SOFTWARE\Altiris\Altiris Agent\Transport string value
   capture events folder has an entry.
4. Check if computer purging is enabled on SMP.
5. Check the amount of managed endpoints and match that to hardware recommendations.
6. This is checking the following: Are any Agent policies configured to send Basic inventory
   more often than Daily or more than every 3 days?
7. Multiple client computers have the same Symantec Management Agent GUID, which
   should be a Globally Unique ID. This makes it impossible to properly manage or account
   for these endpoints. This is usually caused by computers being deployed using an
   image which contains a Symantec Management Agent GUID already in use and known
   to the Symantec Management Platform database.
8. This test looks for the last basic inventory reported to this server from each agent. Where
   the agent has not checked in for 7 days or more It has checked in, in the last 6 months
   The agent is Active and Has not been deleted.
9. The Symantec_CMDB stores a server ID indicating the server that the resource belongs
   to in two locations. This test looks for any resources where these values do not match.

This can cause a problem when looking at the details of a task as it may look to the incorrect server for the information.

10. Licensing has a large impact on the performance and behavior of the Notification Server and its solutions. It is important to make sure that licenses have not been exceeded and AUP is not expired. This test is checking: To make sure the Status is OK. The count of computers using a license is not greater than or equal to the available licenses.
11. If a machine has not connected for a while (two weeks or more for this test), it may need to have its asset status updated or the record purged according to organization's policy.
12. If sites are defined, a site is required to have a minimum of one unconstrained site server. This test is checking: To see if any site servers are assigned to a site Defined as Constrained The site does not have at least one Unconstrained site server.
13. Test that no drives with less than 5% or 5 gig free space.
14. Package servers with a low number of packages in a ready status.
15. Each SMP agent policy should apply to a unique set of agents. Agents should not have two SMP agent policies applying to them. This is checking to see if any agent exists in two different Configuration policies.
16. Schedules should be defined in a way that the action they are performing can be performed in the time frame defined. If this is not occurring the schedule needs to be reevaluated to determine if the action being performed can be improved or if the time allotted needs to be extended.
17. Having a large number of subnets can cause performance issues in some locations in the console. This test is checking: To see if there are more than 10 times the amount of subnets than agents or greater than 20,000 subnets.
18. This is checking to see if multiple discovery methods are being used. If Network Discovery and AD Imports or Network Discovery are both running duplicates may appear as the computers may be added to the NS database twice.
19. Purging event data is an important part of maintaining the Notification Server, if too much or too little data is being kept it can affect overall server performance. This check is looking for:
    a. Settings that have been defined to be larger than the default 1,000,000 rows or 6 months.
    b. Data Classes with no maximum row count defined.
    c. Data Classes where the row count is greater more than 25% of the defined maximum
20. Check if AeXSVC or W3WP processes are using more than 80% of the available system memory.
21. When filters are created, they should use the smallest applicable scoping. This allows filter member triggers to be more efficient. For example, computer filters should use the computer scope rather than the resource or asset scope.
22. Each client needs to have a client policy that applies to it. If a client does not have a policy, it will request one on an accelerated 15 minute default schedule.
23. There are times when a computer does not get created or changed to the correct Resource Type, or exists as two different Resource Types. This test will show if there are any computers in this state.

24. Windows Search services can cause CPU and disk congestion during NSE processing, replication, or other heavy disk I/O.
25. These policies have been rerunning on these agents multiple times. Generally, sub-agent policies do not need to be run more than one time.
26. Check for excessive NSEs in the Event Queue directory.
27. Check IIS Provider Order for [232242](#)
28. Test to see if any agent plug-in installs/upgrades are running with an aggressive repeat schedule. Such as during the 24 hour window, repeat every 1 hour. If found, alert the user because they need to check because these could be running continually due to the check-in for configuration being beyond the repeating schedule. For example, the endpoint checks in every 4 hours, but the agent plug-in policy repeats every1 hour. This would cause the endpoint to run the policy every hour until it checks in again at the 4 hour mark.
29. TestCheckNSAgentIdentityPermissions - This test is looking through the SMP logs to find the pattern The current user 'NS Agent Identity' does not have the required permission 'read' to load item. If found this indicates a problem described in https://knowledge.broadcom.com/external/article/162109 and should be reviewed.
30. TestCheckTotalManagedComputers - This test is running a count query against the vcomputer where ismanaged is equal to 1

SQL Specific Tests:

1. Test to check if arithmetic abort is enabled or disabled.
2. Test to see if optimize for Ad hoc Workloads is enabled. When enabled this allows more memory to be used for the buffer pool cache, rather than for procedure caching of single-use batches.
3. Test to make sure Auto Shrink is set to False.
4. Test for any blocking queries in the database.
5. Test for recovery model. Should be set to simple
6. Test for possible potential beneficial indexes
7. Test Max Degree of Parallelism

Task Based Tests:

1. Check the Clean up Task Data task located at: Settings > Notification Server > Task Settings for failures.
2. In order for client machines to execute basic Management Platform Tasks correctly, the current Altiris Client Task Server Agent must be installed on the managing NS/Site Server. Differences in version between Agent and Server can result in task information sent to clients to not be understood and executed correctly.
3. The 'Update Summary Data' task runs daily and updates the Task data class tables using summaries as well as hierarchy replication. This test checks if there have been failures in task run history for this task.

4. This checks for Task Servers which have more clients registered to it than the maximum best practice for Task Servers: 100 Clients on the NS 5000 Clients on a Task Server.

Patch Management Solution Tests:

1. Check the status of Patch Licenses
2. Check the status of Patch Windows System Assessment Scan Tool Package on site servers.
3. There are several key Filters and Targets used by patch that need to be updated. If any of these have gotten into a state where they are no longer being updated or have zero members, patching will be adversely affected.
4. Creating Software Update Policies with too many software updates may cause timeout issues when saving changes. The limitation is around 50 Updates. Keep in mind each Bulletin holds multiple updates. Best practice is to limit a Software Update Policy to all Bulletins released that month, however having multiple languages enabled or Bulletins with a large number of Updates could make it so that even the months need to be split up.
5. This is testing to verify that computers are only in one Software Update Agent Configuration Policy. If a computer exists in more than one policy it can cause unexpected results.
6. Policies with settings defined outside of the default
7. Check for excessive software update download tasks. More than 50.
8. The PMImport data is an integral part of the Patch Management solution. Ensuring that it comes down in a timely manner is important. This test is looking at the last 7 days: Where there is no end time, indicating it is still running. The PMImport schedule is running for more than 8 hours.
9. The KnownAs key is used to merge products and components. An example of an ambiguous knownas lookup key is using '*ms*' for Microsoft.
10. The PMImport data is an integral part of the Patch Management solution. Ensuring that it comes down successfully is very important. This test is looking for failures in the last 7 days.

Inventory Solution Checks:

1. The setting "Throttle inventory reporting evenly over a period of" allows inventory reporting to be staggered over a period of time. The SMP can become slow or less usable if hundreds or thousands of inventory NSE files are sent to the server at the same time.Throttling over 1 to 8 hours can even out the spike in NSE traffic and allow the NS to operate normally.
2. Check if File Properties is checked for any Inventory Policies as a verification warning

Revision History:

Version: 2.0.0.2: 12/5/2023:
Added the following two checks to Symantec Management Platform Tests
- TestCheckNSAgentIdentityPermissions - This test is looking through the SMP logs to find the pattern The current user 'NS Agent Identity' does not have the required permission 'read' to load item. If found this indicates a problem described in https://knowledge.broadcom.com/external/article/162109 and should be reviewed.
- TestCheckTotalManagedComputers - This test is running a count query against the vcomputer where ismanaged is equal to 1