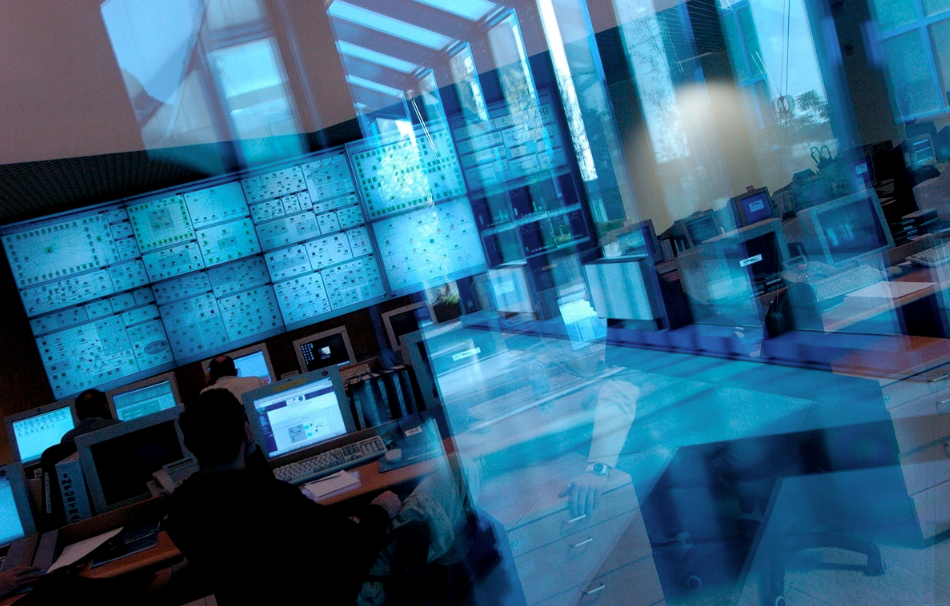
Performed By: Fargham Butt | Senior PFE

Microsoft Corporation



**Analytics Platform System**

**Health Check**

**MetLife**

**Production**

March 16th, 2020

Microsoft has conducted a health check of your APS environment through staff interviews and by running a suite of tools to collect data from APS servers and their dependencies such as clustering. The accredited Microsoft professional from the Premier Field Engineering (PFE) organization, analyzed the collected data and prepared this key finding report.

## Program Phases

The APS Health Check is divided into three phases to provide you with accurate and reliable results. These include the Environmental Assessment phase, Analysis and Reporting phase, and the Remediation phase.

### Environmental Assessment Phase

Microsoft-accredited Health Check personnel executed a series of steps to establish a thorough picture of your specified SQL Server Parallel Data Warehouse environment's technical and operational risks. A qualified engineer used tools to collect in-depth data about your current APS environment, and also conducted an interview with your staff that focused on key risk areas such as operations, disaster recovery, and environmental dependencies. Both of these provided tremendous value because the engineer was able to transfer knowledge about what makes an APS environment reliable and stable. These discussions were centered on understanding your current pain points, reviewing SQL Server best practices and other methodologies, and identifying solutions to address your highest risk issues.

### Analysis and Reporting Phases

Your data, together with the interview results, have been systematically analyzed and compared to Microsoft best practices to identify both the significant gaps and opportunities for improvement. This report reflects the outcome of that analysis, including a detailed Microsoft assessment of your current risks, plus recommendations for addressing those risks currently present in your SQL Server environment.

### Remediation Phase

The recommendations provided by Microsoft will enable you to improve the performance and availability of your SQL Server Parallel Data Warehouse environment and also contribute to an overall reduction in Critical Situation support incidents. The remediation activities described in this report will be reviewed by your Microsoft representative to assist you in resolving any technical or operational issues

# Health Check Scorecard

## Scorecard Legend

The following scorecard is a consolidated view of the health check, based on the collected data and the answers provided during the survey. Using a scale of High, Medium and Low, the scorecard illustrates the likelihood of encountering issues in a specific category

|  |  |
| --- | --- |
| **No Issues** | No Issues were identified during the Health Check. |
| **Low** | Indicates that no significant issues were found in this area that posed a future risk to service. |
| **Medium** | Indicates that issues were identified which should be addressed in the near-term to prevent future disruptions in service. |
| **High** | Indicates that issues were identified which should be addressed immediately to prevent significant disruptions in service |
| **Critical** | Indicates that issues were identified which must be addressed immediately to prevent significant disruptions in service. |

Additionally, overall risk levels for each major category are determined based on the cumulative results of the associated subcategories. Categories containing at least one high-risk issue will be presented as High risk. Categories containing Medium or Low risk issues will be presented as such unless the cumulative values of the identified issues indicate a high-risk level.

Subsequent to the consolidated scorecard, the High, Medium and Low scorecards are presented to show you the specific issues within the major and minor categories that were identified in each of these risk areas.

# Appliance Specifications

The following Appliance was analyzed during this engagement.

|  |  |
| --- | --- |
| Appliance | FABDOM |
| Appliance Description | Production |
| Appliance AU Level | AU5 |
| Appliance Build | 10.0.8015.0 |
| Topology | 4+2 |
| OEM | HP |

**Consolidated Scorecard**

|  |  |  |
| --- | --- | --- |
| **Scorecard** |  | **Health Score** |
| **Appliance Configuration** | |  |
| DNS Configuration |  | **No Issues** |
| Instant File Initialization (IFI) enabled |  | **Low** |
| Integrated Authentication |  | **No Issues** |
| Time Synchronization |  | **No Issues** |
| Appliance Version and Patch Level |  | **Medium** |
|  | |  |
| **Appliance Health** | |  |
| BMC Logs |  | **No Issues** |
| Ethernet Switch Logs |  | **No Issues** |
| Infiniband (IB) Switch Logs |  | **No Issues** |
| Database Volume Storage Check |  | **No Issues** |
| Database Volume Utilization |  | **No Issues** |
| Local Storage Check |  | **No Issues** |
| PDW Logs and System Dumps |  | **No Issues** |
| Windows Event Logs |  | **No Issues** |
|  | |  |
| **Environment Checks** | |  |
| PAV output |  | **No Issues** |
| PDW Alerts |  | **No Issues** |
|  | |  |
| **Maintenance** | |  |
| Database Backups |  | **High** |
| MRA Compliance |  | **Medium** |
| WSUS Patch Management |  | **High** |
|  | |  |
| **Data Health** | |  |
| CCI Table Health |  | **Medium** |
| Data Skew |  | **High** |
| Failed Data Loads |  | **No Issues** |
| Large Replicated Tables |  | **Medium** |
| Statistics |  | **High** |
|  |  |  |
|  | |  |
| **Database Configuration** | |  |
| Database Autogrow |  | **No Issues** |
| Database Space |  | **No Issues** |
|  | |  |
| **Security** | |  |
| Logins - Password Expiration |  | **Low** |
| Logins - Password Policy |  | **No Issues** |
|  | |  |
| **Operational Excellence** | |  |
| Backups Implemented |  | **No Issues** |
| Disaster Recovery |  | **Low** |
| DW Insight Dashboard |  | **Low** |
| SCOM Monitoring |  | **Low** |

# Appliance Configuration

|  |
| --- |
| **DNS Configuration** |
| Description |
| DNS is the service that is used to resolve machine names (such as FABDOM-HST01.FABDOM.local) to IP addresses. In APS, it is installed and configured on the Active Directory Domain Controller VMs (-AD01 and -AD02).  As APS is a ring-fenced environment that has no direct visibility out to your corporate environment, DNS Forwarders are used to allow DNS requests to be relayed to DNS Servers in your corporate environment. This allows for AD integration to be implemented.  A condition may exist in your environment that has the DNS servers on AD01 and AD02 to cross-reference each other, in this case you may experience connection timeouts for incoming queries. The cross-linked references are not needed and can safely be deleted. |
| Recommendation |
| DNS Forwarders to your corporate DNS Servers enables the Appliance to communicate outside of the ring-fenced environment, for AD Integration and WSUS purposes.  If you have corporate policies that prohibit these communications, then do not configure the Forwarders. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **Instant File initialization (IFI)** |
| Description |
| Instant file initialization is a SQL Server feature that allows data file operations to run more quickly. Checking the box to turn Instant File Initialization on will improve performance of SQL Server PDW. However, if this poses a security risk for your business, then leave the box unchecked.  When instant file initialization is enabled, SQL Server does not overwrite deleted bits with zeros. This behavior could create a security vulnerability if unauthorized users gain access to deleted data. However, SQL Server PDW mitigates this risk by ensuring that the SQL Server database and backup files are always attached to an instance of SQL Server; only the SQL Server service account and the local administrator can access the deleted data on SQL Server PDW.  Data and log files are initialized to overwrite any existing data left on the disk from previously deleted files. Data and log files are first initialized by filling the files with zeros when you perform one of the following operations:  • Create a database.  • Add files, log or data, to an existing database.  • Increase the size of an existing file (including AutoGrow operations).  • Restore a database or filegroup.  File initialization causes these operations to take longer. However, when data is written to the files for the first time, the operating system does not have to fill the files with zeros. |
| Recommendation |
| Checking the box to turn Instant File Initialization on will improve performance of SQL Server PDW. However, if this poses a security risk for your business, then leave the box unchecked. |
| Issues Found |
| Instant File Initialization is not enabled for nodes. |

|  |
| --- |
| **Integrated Authentication** |
| Description |
| As an APS security best practice, we recommend the use of Windows Authentication to connect to an APS appliance. Windows Authentication Mode in APS can leverage the organization-wide Active Directory, account, group and password policies, thereby making access more secure. |
| Recommendation |
| It is a best practice to use only Windows logins whenever possible. Using Windows logins with SQL Server achieves single sign-on and simplifies login administration. Password management uses the ordinary Windows password policies and password change APIs. Users, groups and passwords are managed by system administrators; SQL Server database administrators are only concerned with which users and groups are allowed access to SQL Server and with authorization management.  In the APS help file / MSDN, under the “Security - Configure Domain Trusts” it is possible to get some information how to configure it. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **Time Synchronization** |
| Description |
| By default, the APS Domain Controllers do not automatically synchronize their time with the customer domain. In order to maintain consistent time with the customer environment, the APS ring-fenced domain can be configured to reference a NTP server to obtain a time signal to synch with, the Appliance will be configured to obtain the NTP time signal in the AD DCs (AD01 and AD02), and the rest of the Appliance will synch to one of these. |
| Recommendation |
| Configure NTP Time synch to the corporate domain or local AD01 and AD02. Configuring it to sync with the corporate domain is the recommended and preferred way.  ADU can be used to configure Time synchronization. |
| Issues Found |
| No Issues Found |

# 

|  |
| --- |
| **Appliance Version and Patch Level** |
| Description |
| APS is updated in ‘Appliance Updates’ (AU’s), these are roughly analogous to SQL Server Service Packs (though an AU may contain a SQL Server SP, or even a new edition of SQL Server).  AU’s are major upgrade to APS and can include significant new functionality and compatibility that isn’t available in previous releases.  Hotfixes are incremental upgrades on AU’s and may also include SQL Server SP’s as well as other functionality and break-fixes.  Applying an AU is a major operation and can take 1-2 days downtime. These are always installed by a PFE.  Apply a Hotfix is normally a short-term operation, taking 1 – 2 hours. These are always installed by a PFE.  As with patching any system, it is always recommended to take appropriate DR precautions, such as backing up databases before applying te AU or Hotfix. |
| Recommendation |
| We always recommend the latest AU should be installed. Your DSE or TAM can provide a briefing on the changes implemented in the AUs as they are released.  Look for Hotfix summary emails from your DSE or TAM, to determine if released hotfixes could benefit your environment, and schedule the installation as appropriate. |
| Issues Found |
| The appliance in on AU5 (10.0.8015.0). The current AU level is AU7.5. In order to benefit for the additional features and fixes it is recommended to upgrade to the latest AU level. |

|  |
| --- |
| **BMC Logs** |
| Description |
| BMC is the ‘Baseboard Management Console’, this is implemented as different technology by Vendor – Dell as iDRAC, HP as iLO.  BMC captures and exposes hardware level issues for the physical servers in your Appliance, such as local HDD Failures, RAM or CPU issues, etc. |
| Recommendation |
| And issues identified in the BMC logs should be handled by opening a ticket with the HW vendor for remediation. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **Ethernet Switch Logs** |
| Description |
| Your APS Appliance will have two Ethernet switches per Rack.  Errors noted in the Eth switch logs may indicate an error in the hardware that requires attention. |
| Recommendation |
| And issues identified in the Ethernet Switch logs should be handled by opening a ticket with the HW vendor for remediation. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **InfiniBand Configuration** |
| Description |
| Your APS Appliance will have two InfiniBand switches per Rack.  Errors noted in the IB switch logs may indicate an error in the hardware that requires attention.  The Infiniband networks are managed networks and much more tightly constrained than Ethernet networks. Mismatched components can cause performance or connectivity issues on the network. All like Components on the IB Network(s) should be at the same FW levels - all connected HBAs should be on the same FW revision level, and all Switches should be on the same FW revision level. |
| Recommendation |
| Any issues identified in the Infiniband Switch logs should be handled by opening a ticket with the HW vendor for remediation.  Any FW Revision level mismatches should be handled by bringing mismatched components to the appropriate FW revision level as defined in the Appliance MRA for the AU installed. |
| Issues Found |
| No Issues Found |

# 

|  |
| --- |
| **Database Volume Storage Check** |
| Description |
| The database volume storage in your Appliance is directly connected to the compute node servers, from local storage enclosures. Each logical disk volume used to store the databases is comprised of two physical disks in co-located disk enclosures, this arrangement provides for fault tolerance though mirroring the data across the physical volumes.  Disk errors do occur over time, and while the Windows Storage Spaces used to mirror the physical disks understands the physical layout of the disks and will automatically handle disk failures to ensure that the mirroring / Fault Tolerance is maintained, there are limited hot spare disks available for swapping out failed drives.  This test will validate that the physical drives are healthy and will also check for the likely failures by checking for I/O Errors and Latency. |
| Recommendation |
| Any issues identified in the physical disks should be taken care of by replacing the failed or predictive failure drive(s). |
| Issues Found |
| No Issues Found  C:\Users\farghamb\AppData\Local\Temp\SNAGHTML10564948.PNG |

|  |
| --- |
| **Database Volume Utilization** |
| Description |
| Databases in APS are stored in local SQL Server instances, on the Compute nodes. Each data-store database is initially configured identically on each Compute node.  Data is ideally spread evenly across all compute nodes – each replicated table is stored once in each data store, and each distributed table is spread across 8 distributions on each compute node.  In the real-world, data is rarely spread exactly evenly across distributions across compute nodes. Each distribution is hosted in a SQL Server filegroup on a specific pair of virtual drives, from the Database Storage Volumes. If a filegroup on any database expands to fill the available space, due to an uneven data distribution, then the filegroups (one for each database on the Appliance) can no longer grow. This implies that the available space on an Appliance is limited by the smallest free space of any volume pair in the Appliance.  This check looks for Database Storage Volumes that are less than 20% free space. |
| Recommendation |
| If full volumes are identified, and utilization if relatively even, you should consider expanding the Appliance or moving data out of non-essential databases, Hadoop (on-premises or in Azure) can be used to provide the ‘near-line’ storage, allowing direct access with PolyBase.  If full volumes are identified, and utilization if uneven, you should review the data skew to identify which tables in which databases are causing the uneven utilization. Redistributing the data can reduce uneven space utilization. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **Local Storage Check** |
| Description |
| Each physical server hosts two drives, used for the Server OS, and to provide storage for iSCSI drives (these are used for Storage Space stability). The physical drives are mirrored to provide fault tolerance. If one of these drives fail, the server will be at risk with no fault tolerance. If both drives fail, the server will be offline until it can be rebuilt.  The local drive state is viewed though the BMC interface. |
| Recommendation |
| Any issues identified in the physical disks should be taken care of by replacing the failed. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **PDW Logs and System Dumps** |
| Description |
| The PDW logs and System Dumps are checked to identify any issues that occurred on each of the nodes.  On APS when a Service 'crash' occurs - either an A/V, assert or some other uncaught code error in DWEngine, DWDMS, or SQL Server service a dump file is created.  Dump file contains a snapshot of the running process – and parts or all of the memory space of that process.  The snapshot also contains the call stack of every thread the process has created. |
| Recommendation |
| If the PDW Logs contain errors or System Dumps are produced, these should be escalated to Microsoft PDW Support for resolution. |
| Issues Found |
| No Issues Found. |

|  |
| --- |
| **Windows Event Logs** |
| Description |
| The windows event logs are checked to identify any issues that occurred on each of the nodes |
| Recommendation |
| Issues noted in the Windows Event Logs should be reviewed. If issues impact performance of functionality, tickets should be raised with Microsoft for resolution. |
| Issues Found |
| No Issues Found |

# Environment Checks

|  |
| --- |
| **PAV** |
| Description |
| The SQL Server APS Appliance Validator tool validates the hardware and software configuration of an APS Appliance using various utilities related to CPU/RAM/disk to validate the hardware and verifier.exe to validate that the right software is installed on the appliance. This tool uses a combination of PowerShell scripts as well as utilities written in C++ and C#.  The core components of the tool are:  \* Verification framework for executing utilities – based on PowerShell scripts  \* Utilities– memspd, diskspd, verifier, software verifications, and sanity using dwsql.exe  . |
| Recommendation |
| If PAV identified any outstanding issues, please raise a ticket with Microsoft support for resolution |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **PDW Alerts** |
| Description |
| The APS engine is queried to check for any alerts that have been generated.  APS creates alerts for hardware and software issues that need attention. Each alert contains a title and a description of the issue.  APS logs alerts in the sys.dm\_pdw\_component\_health\_alerts DMV. The system retains a limit of 10,000 alerts and deletes the oldest alert first when the limit is exceeded.  sys.dm\_pdw\_component\_health\_alerts (Transact-SQL):  <https://msdn.microsoft.com/en-us/library/mt631629.aspx> |
| Recommendation |
| If Alerts are raised, please raise a ticket with Microsoft support for resolution |
| Issues Found |
| No Issues Found |

# Maintenance

|  |
| --- |
| **Database Backups** |
| Description |
| Database backups are the first line in a Disaster Recovery plan. While APS has built-in redundancy and fault tolerance at multiple levels, there is always a possibility that a catastrophic failure will take an Appliance offline.  Another DR event is data can be inadvertently deleted from a database, accidentally or maliciously.  The most common and often least intrusive method of recovering from a DR event is to restore the database(s) to the Appliance (if available) or a DR Appliance.  Just as with any RDBMS, backups should always be taken before any servicing event on the Appliance.  This test verifies that a Backup credential has been provided to the Appliance, and that backups of the databases are current – within 7 days. |
| Recommendation |
| If the backup credential has not been provisioned, database backups cannot be completed – backups are always written to off-Appliance storage, requiring a domain credential to be provided.  If backups are taken but not current, schedule a job to run the backups to off-Appliance storage, preferably to an Infiniband connected DIP Server.  Add a Network Credential  <https://msdn.microsoft.com/library/mt204011.aspx>  Acquire and configure a backup server  <https://msdn.microsoft.com/en-us/sql/analytics-platform-system/acquire-and-configure-backup-server>  Backup and Restore  <https://msdn.microsoft.com/en-us/sql/analytics-platform-system/backup-and-restore-overview>  Backup and Loading Hardware overview  <https://msdn.microsoft.com/en-us/sql/analytics-platform-system/backup-and-loading-hardware> |
| Issues Found |
| CFDB\_Prod database failed to backup. Please review PDWBackupTestReport located at “D:\Temp\Health\_Check” |

|  |
| --- |
| **MRA Compliance** |
| Description |
| The APS Appliance is governed by a Master Reference Architecture. The MRA specifies the FW Revision levels and Driver versions that should be used in the Appliance. If the FW levels or Driver versions vary from the MRA, the Appliance is considered unsupported, and you may be required to apply the correct versions in order to get support for issues in your Appliance. |
| Recommendation |
| If drivers or FW levels are incorrect, work with a PFE to apply the correct versions. |
| Issues Found |
| Some issues related to mismatch firmware version were reported in the report. Please take a look at Validator-Problem Report “D:\Temp\Health\_Check”. |

|  |
| --- |
| **WSUS Patch Management** |
| Description |
| The Windows Update Service (WSUS) is installed on the VMM server as part of the APS factory build process. However, the service must be configured to get software updates.  WSUS is the supported method to patch the infrastructure of the Appliance.  Note that the patches applied through WSUS are strictly limited, for example, SQL Server Service Packs are NOT applied through WSUS, as this may change the behavior of the Appliance in unpredictable ways. |
| Recommendation |
| Apply WSUS Patches in a regular cadence.  A monthly cycle that matches the Microsoft patching cycle (Patch Tuesday – the 2nd Tuesday of each month) is a good cadence. If your patching window is after Patch Tuesday every month, you can be assured your APS Appliance is patched to the latest release. This will mitigate any identified vulnerabilities or other issues.  The longer your patching cycle, the more time will be required in each patching window to complete the updates, a monthly cycle will likely take 2-3 hours. Please work with your DSE, or work with your TAM to engage a PFE to set this up.  WSUS Patching for APS is handled by a specific process in APS that will run the updates and also handle stopping and restarting PDW Services, VMs and physical servers in the appropriate order. |
| Issues Found |
| The last time patching was performed in January 2020. |

# Maintenance

|  |
| --- |
| **CCI Table Health** |
| Description |
| Columnstore Clustered index can provide very significant improvement in data compression compared to data compression of regular clustered index. Columnstore Clustered index can also speed up your queries significantly.  Clustered Columnstore indexes are a hybrid read-only / read-write structure. Data is written to a Delta Store. This is a row-store version of the table and is treated the same as any other row-store table, for DML operations.  The row-store Delta Store is converted into read-only Column Store structures. As data is deleted from the Column Store structure, a bit-map is kept to identify the deleted rows. Over time, the deleted row count can grow, this makes the Column Store less efficient.  The process to convert the Delta Store will fire for multiple triggers, some of which will cause Column Store segments with less than the optimal row count of ~ 1M rows. This can severely reduce the efficiency of Column Store tables.  There are several conditions that will reduce the performance of CCI tables.   1. Small Row Groups   Any Row Groups less than 400K rows will impact performance.  Using a Resource class that is too small can cause this due to memory limitations– use a larger resource class for load jobs  Bulk loading can also cause this – bypasses the Delta store for RowGroups over 120K rows, going directly to compressed format.   1. Deleted rows   As data is deleted from Closed RowGroups in a CCI table, the data isn’t actually removed, a bitmap is maintained to keep track of the ‘deleted’ rows, over time this will reduce performance.   1. Open RowGroups   When data is inserted in to CCI tables, new data is added into a Delta Store, this is a HEAP row-store version of the CCI table. The Delta Store performance is very significantly worse than the compressed data in Columnar format.  Over time, as data is deleted, sub-optimal sized row-groups are created and rows are kept in the Delta Stores, the efficiency of the CCI will be degraded.  In order to restore the performance of the CCI table, it should be rebuilt, either in-place or using a CTAS command.  It should be noted that distributed CCI tables will generate one CCI table per distribution, at 8 distributions / compute node, and partitioned & distributed CCI tables will generate x CCI tables per distribution, one for each partition on each distribution.  Each CCI table will have its associated Delta Store(s). |
| Recommendation |
| Monitor the health of your CCI tables and rebuild them as appropriate.  If the CCI table is unhealthy due to smaller RowGroup sizes after a Load process, verify if the load process would benefit from a larger resource class with a larger memory allocation.  Review the listed tables are identify the appropriate actions to take as needed. |
| Medium |
| Couple of tables reported issues. Please review the CCI table health report – FABDOM\_WellnessCheck under “D:\Temp\Health\_Check” |

|  |
| --- |
| **Data Skew** |
| Description |
| Data skew occurs when the rows of a Hash distributed table are not spread uniformly across all of the distributions. A large variance in the number of rows in each distribution can negatively impact query performance.  Avoiding data skew means you want to avoid having a disproportionately large number of table rows in one distribution in comparison to the number of rows in other distributions. Since queries rely on work being performed on all distributions, even if queries finish fast in smaller distributions, you will still need to wait for the queries to finish on larger distributions before you can get the query result.  Symptoms of data skew during query execution   * The number of rows processed on a node is significantly higher or lower than those processed on other nodes. * Query execution time on a node is distinctly faster or slower than those for other compute nodes.   Other symptoms that may indicate data skew:   * One or more admin console alerts or warnings indicating a variance in disk space between compute nodes.   When rows of a distributed table are spread evenly, the database files on each disk in the compute nodes should also be similar in size. Each compute node has 16 disks for storing database data files. When a new database is created on APS, one database file is created for each disk in a compute. A typical APS compute rack consists of 10 compute nodes and 16 disks per compute node. In this scenario, 160 database files are created for each database on the appliance. Each of the 160 files should be similar in size if the rows of a distributed table are spread evenly across its distribution key.  DETECTING DATA SKEW  During the design phase, don’t worry about making a mistake when you choose the distribution column. It’s easy to re-create the table using another distribution column by using the CREATE TABLE AS SELECT (CTAS) statement.  To test your workloads with different distribution keys, you can create copies of the same table and assign a different distribution column to each table. You can then test your workloads against each table to see which distribution key gives the best overall performance. This type of iterative design and experimentation works well with SQL Server APS architecture.  OTHER CONSIDERATIONS  Before you decide to take further action, make sure you really do have a skew problem and understand what it will do to the overall workload on the appliance. Generally, a 10% difference in the number of rows among distributions is acceptable. The amount of acceptable data skew depends on your workload and performance requirements.  We have seen that 10-20% skew can be tolerable in APS when considering the grand scheme of things where many queries are going through the system concurrently. Obviously, single-run queries that are affected by the skew will naturally run slower on the skewed distributions, but before you declare defeat, make sure that your customer (end user) isn’t unhappy with performance.  Just because data may be skewed on one or a few distributions doesn’t spell disaster. Review the queries executed against the tables and determine if they will be affected.  Naturally, if the queries are doing full distribution scans, then skew will affect the performance, but this is very rare in the real world. If the distributions are also partitioned (e.g. by date) and the queries are restricted by date, then a good (possibly mixed-grain) partitioning strategy can work wonders. Yes, the queries may still run a bit slower on the skewed partitions, but the performance is relative to the scan rate so it may not be that much slower. Testing will tell for sure. |
| Recommendation |
| Monitor Data Skew across the tables in your databases using the ADU command. Any tables that exhibit more than 10% skew and are moderately-sized or larger (> 200MB) should be reviewed to identify if a better Hash distribution key can be identified.  NOTE – a NULL value or a default value in a Hash key is a common cause of Skew – NULL values always go to Distribution A on Compute node 1, and a default value will always be stored in the same Distribution.  NOTE – Hash distribution key values cannot be modified. Once the record has been written, the value cannot be changed. |
| Issues Found |
| There are tables that are showing high level of data skew. Please review the table skew report. |

|  |
| --- |
| **Failed Data Loads** |
| Description |
| Data loads populate the data into your APS Databases.  This test lists any failed data loads. |
| Recommendation |
| Review the failed loads listed and identify the cause of the failure to ensure future loads run without errors. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **Large Replicated Tables** |
| Description |
| A Replicated table is a table structure that exists as a full copy within each discrete SQL Server instance on the compute nodes.   * Small sets of data can be more efficiently stored in full. * Certain set operations are more efficient against full sets of data.   Schema design for the APS requires careful planning and iterative prototyping to find the ideal design for a specific end user implementation. At its most basic level, dimension tables or reference tables, are often designed and implemented as replicated tables on the APS.  The basic rule of thumb is that replicated structures are typically used for tables less than 5-10 GB in size whereas a distributed structure is used for tables greater than 5-10 GB.  It must be noted that Replicated tables can be a performance bottleneck for updates. When data in a Replicated table is updated, a lock is taken on all copies of the table in the Appliance, and a single copy is then updated. Once the single copy is updated, that copy is replicated to all Compute nodes in the Appliance. For large replicated tables, this can block queries for a significant period.  Replicated tables can consume large amount of space – each node holds a complete copy of the Replicated tables. |
| Recommendation |
| Review the listed tables, any table larger than 10GB should be reviewed to see if it can be Distributed.  In addition to the product documentation, see these wiki topics for help designing and creating databases and tables.  Choosing Distributed Versus Replicated Tables in SQL Server APS <http://social.technet.microsoft.com/wiki/hub/contents/sqlAPS/choosing-distributed-versus-replicated-tables-in-sql-server-APS.aspx> |
| Issues Found |
| Some tables are larger than 10GB. Please take a look at ReplicatedTableSize under “D:\Temp\HealthCheck”. |

|  |
| --- |
| **Statistics** |
| Description |
| SQL Server PDW generates statistics on the Control node and uses them to improve query performance by minimizing the data movement in the distributed query plan.  To create statistics on the Control node, SQL Server PDW merges the statistics-related contents of the tables residing on the Compute nodes and stores them as a single statistics object on the Control node. Since all replicated tables have the same statistics, generating statistics on the Control node only applies to distributed tables.  For the statistics on the Control node, the AUTO\_CREATE\_STATISTICS setting does not apply. Single-column statistics auto-created on Compute nodes do not get merged and stored on the Control node. Since the MPP plan, including data movement operations, is generated on the Control node, the cost-based MPP query optimizer does not auto-create single-column statistics to improve the query plan for data movement operations.  This test uses a cutoff of 7 days as an indication that the Statistics may be stale. Age may not be a reliable indicator of staleness if no data has bene updated in te table. |
| Recommendation |
| Review the listed Statistics to determine which need to be recomputed |
| Issues Found |
| Some of the stats haven’t been updated for months. Please review the LastModidfiedStatistics report under “D:\Temp\HealthCheck”. |

# Database Configuration

|  |
| --- |
| **Database AutoGrow** |
| Description |
| When you define a database in APS, there are limited configuration options available when compared to the equivalent SQL Server operation. One of the options available is to enable AutoGrow, however you can’t specify growth increments, this is set to relatively small value by design.  If AutoGrow is OFF, once a database fills up any further activity may fail. For APS, a full data store database on a single compute node (through Excessive Data Skew, for example) will cause the overall database to be reported as full.  Enabling AutoGrow should be regarded as a contingency plan, rather than a space management strategy. As a contingency plan, AutoGrow should be enabled, unless there is a definitive reason why not.  CREATE DATABASE (Parallel Data Warehouse)  <https://msdn.microsoft.com/en-us/library/mt631608.aspx>  ALTER DATABASE (Parallel Data Warehouse)  <https://msdn.microsoft.com/en-us/library/mt631606.aspx> |
| Recommendation |
| Review the databases identified below and determine if AutoGrow should be enabled. |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **Database Size** |
| Description |
| This test summarizes the appliance storage utilization.   * Total Appliance Volume Space (Used and Unused): Logical volume space for data files * Total Appliance Free Space (Unused): Free Logical Volume space for data files * Total Database Allocated Space (Reserved): Total amount of space allocated by objects in the database. * Total Actual Space (Data space): Total amount of space used by data. * Total Allocated Unused Space (Unused data space): Total amount of space reserved for objects in the database, but not yet used.   Once a database fills up any further activity may fail. For APS, a full data store database on a single compute node (through Excessive Data Skew, for example) will cause the overall database to be reported as full. |
| Recommendation |
| Review the databases flagged below, to determine if they should be grown or shrunk. |
| Issues Found |
| No Issues Found |

# Security

|  |
| --- |
| **Logins – Password Expiration** |
| Description |
| Checks whether the APS logins created on the appliance have Passwords set to expire.  The following query provides that information:  SELECT Logins.[name] as [Login],  ISNULL(Roles.[name], 'Default') AS ResourceClass,  SQLAuth.is\_policy\_checked,  SQLAuth.is\_expiration\_checked  FROM  (SELECT \* FROM sys.server\_principals WHERE type IN ('S', 'U') AND [name] NOT LIKE '#%' AND [name] NOT LIKE 'NT%' ) AS Logins  LEFT OUTER JOIN sys.server\_role\_members AS rm  ON Logins.principal\_id = rm.member\_principal\_id  LEFT OUTER JOIN (SELECT \* FROM sys.server\_principals WHERE [name] in ('mediumrc', 'largerc', 'xlargerc') ) AS Roles  ON rm.role\_principal\_id = Roles.principal\_id  LEFT OUTER JOIN sys.sql\_logins AS SQLAuth  ON Logins.[name] = SQLAuth.name   * If the is\_policy\_checked column is 0, then the login fits the category. “Nothing is being enforced.” * If both columns are equal to 1 all the settings are used, including password expiration. |
| Recommendation |
| It is recommended to create logins with Expiration Checked. |
| Issues Found |
| There are several accounts that are set not to expire. Please review those accounts. |

|  |
| --- |
| **Logins – Password Policy Compliance** |
| Description |
| Checks whether the APS logins created on the appliance are complying by the password policy.  The query listed above in [Password Expiration] will provide details on the Password Policy setting for users.   * If the is\_policy\_checked column is 0, then the login fits the category. “Nothing is being enforced.” * If both columns are equal to 1 all the settings are used, including password policy. |
| Recommendation |
| It is recommended to create logins with Policy Checked. |
| Issues Found |
| No Issues Found |

Operational Excellence

|  |
| --- |
| **Backups Implemented** |
| Description |
| Database backups are the first line in a Disaster Recovery plan. While APS has built-in redundancy and fault tolerance at multiple levels, there is always a possibility that a catastrophic failure will take an Appliance offline.  This test verifies that the Backup strategy is designed to meet the SLA for your environment. |
| Recommendation |
| Design your backup strategy to meet your SLA(s). |
| Issues Found |
| No Issues Found |

|  |
| --- |
| **Disaster Recovery** |
| Description |
| While Database backups are the first line in a Disaster Recovery plan, the full DR plan includes considerations on how to recover from a scenario where your Production APS Appliance is no longer accessible.  The DR plan should comprise a solution that allows you to recreate your data and processing environment. This can be though reloading data from the source(s), Database Restores, dual-load strategy, etc. |
| Recommendation |
| Design your DR strategy to meet your SLA(s). |
| Issues Found |
| Although the DR plan exists, it should be tested on regular basis to make sure that DR plan can be executed and implemented as well. |

|  |
| --- |
| **DWInsight Dashboard** |
| Description |
| The DWInsight Dashboard for APS provides users the vital information related to their databases and tables residing in an Appliance.  The Dashboard compliments the built-in Admin Console and together both the dashboards provide a holistic view of the various components of an appliance.  The Dashboard covers the following areas:   * Database Properties * Database Size * Large Replicated Tables * Table Sizes * Table Skew * Table Statistics * Table List * Appliance Security * Database Security * Backup and Restore Performance * Databases with NO backups * DwLoader Runs * Errors * Performance * Warnings |
| Recommendation |
| Install the DWInsight Dashboard to gain an overall view of your Appliance. You will need a separate SQL Server instance outside of the Appliance to host the Dashboard. |
| Issues Found |
| DWInsight Dashboard is not being used. |

# 

|  |
| --- |
| **SCOM monitoring** |
| Description |
| SQL Server 2012 Parallel Data Warehouse (APS) provides comprehensive system health alert infrastructure based on distributed diagnostics framework. This gives ability to surface the alerts across the entire APS appliance related to the hardware/software failures and overall system health.  System Center Operation Manager (SCOM) can be used to provide alert delivery mechanism. |
| Recommendation |
| SCOM Monitoring does not appear to be implemented, by the lack of a SCOM User account in the APS Appliance.  Implement SCOM Monitoring of your APS Appliances, if SCOM is available in your environment. APS comes with the necessary SCOM licenses.  The SCOM base management pack can be downloaded using the link given below  <http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=11436>  The monitoring pack can be downloaded using the link given below  <http://www.microsoft.com/en-us/download/details.aspx?id=38198> |
| Issues Found |
| No SCOM monitoring is being used. |