**Prior to Installing SQL**

1. Someone from the Infrastructure Team will be initially setting up the server and drives on the server for the Database Team.
2. Verify the drives are setup properly:

Temp (E:)

Log (F:)

Data1 (G:)

Data2 (H:) etc. (If additional Data Drives are setup on the server)

If there is a drive setup for Indexes, that should be (N:)

If there is a drive setup for Backups, that should be (X:)

1. Verify all drives are setup to utilize the NTFS file system.
2. Please check to make sure the following items have been installed on the server: Winzip with command line interface and RoboCopy.

**SQL 2016 Installation with SP1**

1. Login to the server as SQLServerAccount (or the account setup for the server). If it is a dbcin…account, it will not have access to the location of the SQL installation – if that is the case, just login as you to do the installation.

***NOTE:*** If the server is **NOT** a production server, you should use the SQLServerTest account (or the account setup for the server….dbcinxxx….) everywhere that the SQLServerAccount is referenced in these instructions. \*\*\*\***UPDATE:** **In some test environments SQLServerTest may not have the appropriate network permissions and SQLServerAccount may need to be used for the Proxy Account and the Agent.**

1. Navigate to the appropriate folder for the version you want to install and run the **Setup.exe**:
   1. [\\shermfin.com\dfs\CIN\Software\Microsoft\SQL\SQL2016\](file:///\\shermfin.com\dfs\CIN\Software\Microsoft\SQL\SQL2016\) ( all version)
2. On the SQL Server Installation Center window, click on **Installation** in the left pane.
3. Click on the option for the installation (example: for a new installation, select “New SQL Server stand-alone installation or add features to an existing installation”)
4. The Setup Support Rules screen appears – this checks to see if problems might occur when installation SQL Server. Make sure there are no failures, warnings, or anything is skipped. Click OK.
5. On the Product Key window, verify the product key is entered on the screen and click next.
6. Select “I accept…” on the **License Terms** screen and Click **Next**.
7. You may get a pop up saying “Computer restart required…..One or more affected files have operations pending. You must restart your computer after the setup process is completed.” Click OK.
8. On the Setup Support, click Install.
9. The Setup Support Rules window may have a warning for the “Windows Firewall”. This is OK. Click Next.
10. On the Setup Role screen, make sure SQL Server Feature Installation is selected, Click Next.
11. On the Feature Selection screen, select the options you would like to install. Click Next.
12. Make sure there are no failures on the Installation Rules screen. Click Next.
13. On the Instance Configuration screen, Verify Default Instance is selected and you need to change the Instance Root Directory to point to the G:\ drive (the data drive on the server). Click Next.
14. One the Disk Space Requirements screen, verify the space needed/available and click next.
15. On the Server Configuration screen, you need to enter the Account Name and Password for what will be the SQL Account setup on the server (SQLServerAccount, DBCINSOM01SVC, etc.). You can also select the startup type of the services (Manual, Automatic, or Disabled). Click on the Collation tab at the top to verify the Collation of the server is SQL\_Latin1\_General\_CP1\_CI\_AS.
16. On the Database Engine Configuration screen, you need to select mixed mode and enter the sa password. You can also add the system administrators in this window. Click on the Data Directories tab and verify all the directories are correct.

|  |  |
| --- | --- |
|  | **Data Directories** |
| Data root directory: | G:\ |
| System database directory: | G:\MSSQL13.MSSQLSERVER\MSSQL\Data |
| User database directory: | G:\MSSQL13.MSSQLSERVER\MSSQL\Data |
| User database log directory: | F:\MSSQL13.MSSQLSERVER\MSSQL\Data |
| Temp DB directory: | E:\ MSSQL13.MSSQLSERVER\MSSQL\Data |
| Temp DB log directory: | E:\ MSSQL13.MSSQLSERVER\MSSQL\Data |
| Backup directory: | G:\ MSSQL13.MSSQLSERVER\MSSQL\Backup |

When finished, click **next**.

Include SHERMAN\S-SUB-CIN-DBAdmin to specify SQL Server administrators

1. Do Not select any options on the Error and Usage Reporting screen. Click next.
2. On the Installation Configuration Rules screen, verify there are no failures or warnings. Click **next**.
3. The Ready to Install screen will show a summary of everything. Click **Install** when ready.
4. The Installation Progress window will show you the status of the install.
5. On the Complete screen, click **Close**.
6. **Reboot** **the server when installation is complete.**

**SQL 2016 SP1 Installation**

1. Navigate to [\\shermfin.com\dfs\CIN\Software\Microsoft\SQL\SQL2016Sp1\](file:///\\shermfin.com\dfs\CIN\Software\Microsoft\SQL\SQL2016Sp1\) and run the exe file **SQLServer2016SP1-KB3182545-x64-ENU.exe**
2. On the SQL Server 2016 update screen, make sure no failures or warnings and clicked Next.
3. Select **I Accept** on the License Terms screen and Click **Next**.
4. Click **Next** on the Select Features screen.
5. On the Check Files In Use screen, verify no files or process are locked preventing you from installing the service pack. Click Next.
6. Click **Install** on the Ready to Update screen.
7. Verify everything is successful and Click Close on the Complete screen.
8. **Reboot** **the server when installation is complete.**

**Install SQL Server Management Studio**

1. Run Latest SSMS Installer from [\\shermfin.com\dfs\CIN\Software\Microsoft\SQL\SQL2016\SSMS](file:///\\shermfin.com\dfs\CIN\Software\Microsoft\SQL\SQL2016\SSMS)

**SQL Hardening**

1. Navigate to [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\SQL Hardening](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\SQL%20Hardening) and run the script entitled hardening.sql.
2. Run db\_ShowPlan.sql in the Model database.

**Access using only TCP/IP**

1. Go to the SQL Server Configuration Manager and disable Shared Memory.
   1. SQL Server 2005 Network Configuration
   2. SQL Native Client Configuration
2. Make sure TCP/IP is the only protocol on the list enabled. **\*\*\* Disable all but TCP/IP \*\*\***

**Add Operators and Alerts**

1. You can find the Operators to be added in the folder [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\Operators](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\Operators)
2. You can find the Alerts to be added in the folder [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\Alerts](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\Alerts)
3. **NOTE:** You may receive error messages when running these scripts as some of them use other operators/alerts that you have not yet installed. Verify manually that all operators and alerts have been installed when you are finished running all of the scripts

**Adding ADSI Linked Server**

1. Navigate to [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\LinkedServers](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\LinkedServers) and Run **LinkedServer\_ADSI.sql** script to add the ADSI Linked Server.

**Adding DBAdmin Database**

1. Create a database in Simple Mode called **DBAdmin** with the following:
   * DBAdmin\_Data, Location on the Data drive (G:\MSSQL.1\MSSQL\Data\), Space allocated (100MB). Set to Automatically grow in 100 MB and unrestricted file growth
   * DBAdmin\_Log, Location on the Log drive (F:\MSSQL.1\MSSQL\Data\), Space allocated (100MB). Set to Automatically grow in 100 MB and unrestricted file growth

* **NOTE:** You may need to create the path on the F:\ Drive.

**Adding tables to the DBAdmin Database**

**NOTE:** All procedure scripts listed in the steps below are located [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\DBAdminTables](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\DBAdminTables).

1. Run **dbo.CheckJobsForBackupsAndDBCC\_Exceptions.TAB.sql** script in the DBAdmin database.
2. Run **dbo.dbaAdmin.TAB.sql** script in the DBAdmin database.
3. Run **dbo.dbaAdmin metadata.sql** script to populate dbaAdmin table.
4. Run **dbo.dbaDatabaseSpace.TAB.sql** script in the DBAdmin database.
5. Run **dbo.dbaIndexHistory.TAB.sql** script in the DBAdmin database.
6. Run **dbo.dbaJobHistory.TAB.sql** script in the DBAdmin database.
7. Run **dbo.dbaObjectPermissions.TAB.sql** script in the DBAdmin database.
8. Run **dbo.dbaRecordCount.TAB.sql** script in the DBAdmin database.
9. Run **dbo.dbaRoleMembers.TAB.sql** script in the DBAdmin database.
10. Run **dbo.fragStats.TAB.sql** script in the DBAdmin database.
11. Run **dbo.SQLsafeAdmin.TAB.sql** script in the DBAdmin database.

**Adding stored procedures to the DBAdmin Database**

**NOTE:** All procedure scripts listed in the steps below are located [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\DBAdminProcs](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\DBAdminProcs).

1. Run **ADSItoSQLCompare\_sps.sql** script in the DBAdmin database.
2. Run **dba\_sp\_helprotect\_spr.sql** script in the DBAdmin database.
3. Run **dbaCheckJobsForBackups\_DBCC\_Reindex.sql** script in the DBAdmin database.
4. Run **dbaDatabaseSpace\_spr.sql** script in the DBAdmin database.
5. Run **dbaDbccShowcontig\_spt.sql** script in the DBAdmin database.
6. Run **dbafragStatsCleanUp\_spt.sql** script in the DBAdmin database.
7. Run **dbaIndexHistory\_spd.sql** script in the DBAdmin database.
8. Run **dbaIndexHistory\_spi.sql** script in the DBAdmin database.
9. Run **dbaIndexHistory\_spt.sql** script in the DBAdmin database.
10. Run **dbaJobActivityMonitor\_sps.PRC.sql** script in the DBAdmin database.
11. Run **dbaJobHistory\_spi.sql** script in the DBAdmin database.
12. Run **dbaObjectPermissions\_spi.sql** script in the DBAdmin database.
13. Run **dbaRecordCount\_spi.sql** script in the DBAdmin database.
14. Run **dbaRoleMembers\_spi.sql** script in the DBAdmin database.
15. Run **dbaStackDumpDetection\_spt.sql** script in the DBAdmin database.
16. Run **kill\_spt.sql** script in the DBAdmin database.

**Adding stored procedures to the master database**

**NOTE:** All procedure scripts listed in the steps below are located [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\MasterProcs](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\MasterProcs).

1. Run **admobjectspace\_sps.sql** script in the master database.
2. Run **sp\_blitzIndex.sql** script in the master database.
3. Run the following two scripts in the order given below in the master database.
   * First run **sp\_hexadecimal.sql** script in the master database.
   * Then run **sp\_help\_revlogin.sql** script in the master database.
4. Run **sp\_lock2.sql** script in the master database.
5. Run **trace\_blackbox.sql** script in the master database.
6. Run **who\_is\_active\_v11\_00.sql** in the master database.

**Adding the Admin Jobs to the Server**

**NOTE:** All SQL Job scripts listed in the steps below are located [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\AdminJobs](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\AdminJobs).

1. Setup a folder on the G:\ drive under the MSSQL13.MSSQLSERVER\MSSQL folder called SQLJobOutput. This will need to be setup as a share (called SQLJobOutput$) with the following permissions on the share: Everyone, Full Control; and the following permissions on the folder: Administrators, SQLServerAccount (or the service account setup for the server…dbcinfax02svc), and S-SUB-CIN-DBAdmin with Full Control.
2. Run **admSQLBlackBox.sql** script in the msdb database.
3. Run **admSQLStackDumpDetection.sql** script in the msdb database.

* You need to update the first job step @Path line to point to the correct location of where the log folder is located.

1. Run **admUserScript.sql** script in the msdb database.
2. Run **admWeeklyDbccShowContig.sql** script in the msdb database.
3. Run **dbaIndexHistory.sql** script in the msdb database.
4. Run **dbaJobHistory.sql** script in the msdb database.
5. Run **dbaObjectPermissions.sql** script in the msdb database.
6. Run **dbaRecordCount.sql** script in the msdb database.
7. Run **TerminateConnections.sql** script in the msdb database.

* Also disable this job until you have the backups set up on the server. Once the backups are setup and the time is established as to when they will run, this job should be set up to run 5 minutes before the Nightly Backups kick off.
* NOT all production servers will necessarily need this job.

**Setting up SQL Server Logs for Cycling each Day**

1. Increase the Server Log History by running the script ‘**Increase Server Log History Threshold.sql**’ located in the folder [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\CycleSQLErrorlog](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\CycleSQLErrorlog)
2. Add the job **Cycle SQL ErrorLog** by running the script in the folder [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\CycleSQLErrorlog](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\CycleSQLErrorlog)

**SQL 2016 Re-Indexing Job**

**NOTE:** All SQL scripts listed in the steps below are located [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\Reindexing](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\Reindexing).

1. Create Util database with the **UtilDatabase.sql** script (If one does not exist or will not be restored from another server).

**NOTE:** You may need to update the FILENAME path to the appropriate drive letter.

1. Objects to add to the **Util** database:

* TABLES and MetaData
* Util.dbo.LogApp.Table.sql
* Util.dbo.Log.Table.sql
* Util.LogAppMetaData.sql
* Stored Procedures
* Util.dbo.Log\_sps.StoredProcedure.sql
* Util.dbo.Log\_spt.StoredProcedure.sql
* Util.dbo.Reindex\_Log\_sps.StoredProcedure.sql

1. Objects to add to the **DBAdmin** database:

* Stored Procedures
* DBAdmin.dbo.ReIndex\_sps.StoredProcedure.sql
* DBAdmin.dbo.Reindex\_spt.StoredProcedure.sql
* Tables
* DBAdmin.dbo.dbaReIndexList.Table.sql

1. Run **WeeklyRe-IndexJob.sql** script to create a new SQL job to run the re-indexing on the weekend.

* Update/verify operator of who gets notified upon failure.
* Update the time the job runs to whatever fits best for the server.
* Update the job with ALL the User Databases on the server.

**SQL 2016 Configuration Changes**

**NOTE:** All procedure scripts listed in the steps below are located [\\shermfin.com\dfs\cin\groups\dba\sql\Standard\_Build\SQL2016\Scripts](file:///\\shermfin.com\dfs\cin\groups\dba\sql\Standard_Build\SQL2016\Scripts)

1. Enable xp\_cmdshell at the server level. Run **Enable\_xp\_cmdshell.sql**.
2. Enable Ole Automation Procedures at the server level. Run **Enable\_OleAutomationProcedures.sql**.
3. Enable Public view of Metadata. Run **EnablePlublicViewOfMetadata.SQL.**
4. Enable Public execute permissions to sys.xp\_logevent. Run **xp\_logevent.SQL.**

**Database Configuration**

**NOTE:** All procedure scripts listed in the steps below are located

[\\shermfin.com\dfs\cin\groups\dba\sql\Standard\_Build\SQL2016\Scripts\AfterDBRestores\](file:///\\shermfin.com\dfs\cin\groups\dba\sql\Standard_Build\SQL2016\Scripts\AfterDBRestores\)

1. Verify that all databases are owned by sa. Run **sqldbownerScript.sql** to verify owners.
2. Verify that all databases are set to version 130 (SQL2016).

**NOTE:** The next two steps may not need to be enabled depending on the database.

i.e. Sandbox, DBAdmin.

1. Enable Database Chaining. Run **EnableDatabaseChaining.SQL. NOTE:** You will need to edit the script with the appropriate database name(s).
2. Enable Database Trustworthy properties. Run **EnableDatabaseTrustworthy.sql.** **NOTE:** You will need to edit the script with the appropriate database name(s).

**Virtual Memory Settings on ALL Servers**

1. Right Click on the Computer Name icon and Choose Properties.
2. Click the Advanced System Settings link.
3. Choose the Performance Settings button.
4. Choose the Advanced tab.
5. Click the Virtual Memory Change button.
6. Verify the System Managed Size radio button is selected. If not, select it.
7. Click the Set Button.
8. You may get prompted to reboot the server for the change to take effect.

**Local Security Policy Setting on Server**

1. Click Start, Administrative Tools, Local Security Policy.
2. Expand on Local Policies.
3. Select User Rights Assignment.
4. In the right window pane, double click **Lock pages in memory**.
5. Click the button Add User or Group.
6. Enter SQLServerAccount (or dbcinfax02svc) and click the Check Names button. Then click OK.
7. Do Steps 4 -6 for **Perform Volume Maintenance Tasks (**if you unchecked this in the installer)
8. Click OK once the account has been added.
9. Close the Local Security Settings window and stop/start the SQL Server Services.

**Administration Tasks**

1. Run the following command from a query window:

USE master

DENY EXECUTE ON sp\_replwritetovarbin TO public

1. Setup any Link Servers needed.
2. Setup any Network Alias’ needed. (TEST and DEV servers should have all production servers aliased to itself or the appropriate Test or Dev Server.)
3. Setup any File Shares as needed with the appropriate permissions.
4. Set the SQL Proxy Account by going into the Server Properties and to the Security Page. Click the check box for Enable Server Proxy Account. Click on the ellipse button, Update the Location to Entire Directory, enter SQLServerAccount and click on Check Names to get the full proper account, click OK. Enter the SQLServerAccount password as the proxy account.

NOTE: The SQL Proxy Account is not set on all servers.

1. Change Login Auditing to Both Failed and Successful Logins on the SQL Server Properties/Security Tab.
2. Change the SQL Services to auto startup.
3. Set the job history appropriately in SQL Server Agent Properties on the History Tab. This depends on the number of jobs and how often the jobs run as to what the job history should be set to. It may be beneficial to look at a similar server to see how it should be set.
4. Set the trace flags on Startup for deadlocks –T1222 and –T3605.

Also - T1204 for 2016

For SQL Server 2016, open the SQL Server Configuration Manager. Click on SQL Server Services in the left pane. Right click on “SQL Server (*servername*)” and select properties. Click on the Startup Parameters Tab and type in each flag in the “Specify a startup parameter” box and click Add.

1. Set up Database Mail by running the script **Setup database mail.sql** in the folder [\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard\_Build\SQL2016\DatabaseMail](file:///\\shermfin.com\dfs\CIN\Groups\DBA\SQL\Standard_Build\SQL2016\DatabaseMail) . This script will also send a test email to [E-CIN-DBA@resurgent.com](mailto:E-CIN-DBA@resurgent.com).
   1. **NOTE:** Use **Setup database mail - Dev and Test.sql** if this is for a test or development server.
   2. For 64-bit, all code referencing xp\_sendmail needs to be rewritten to use sp\_send\_dbmail.
2. Enable the SQL Server Agent to use database mail by right-clicking SQL Server Agent in the Microsoft SQL Server Management Studio. Select Properties. Click on “Alert System”. Check the box “Enable mail profile”. The default values should be ok. Click OK. You will need to restart the SQL Server Agent for this to take effect.

For SMS server name: smtp.shellpointmtg.com under outgoing mail

1. Verify the **SQLSupportPager** Operator e-mail name includes: [E-CIN-DBAPaging@sfg.com](mailto:E-CIN-DBAPaging@sfg.com)
2. Verify **SQL Server Login Failure** Alert is configured for All Databases and is set to have an email sent to the DBA team.
3. Verify **SQL Server Deadlock** Alert is configured for All Databases and is set to have an email sent to the DBA team.
4. Verify **DB Log File is Full** Alert is configured for All Databases and is set to have an email sent to the DBA team and SQLSupportPager AND is set to page the SQLSupportPager. (**NOTE:** If this is a TEST or DEV box, do NOT set the paging option on the Alert.)
5. Verify **Scheduler** **Hung** Alert is configured for All Databases and is set to have an email sent to the DBA team and SQLSupportPager AND is set to page the SQLSupportPager. (**NOTE:** If this is a TEST or DEV box, do NOT set the paging option on the Alert.)
6. If this is a TEST or DEV box, make sure the SQLSupportPager Operator is disabled.
7. Test that alerts are being emailed by attempting to login to the SQL Server with SQL Server Authentication and use the name “Loginfailuretest”. An email should be sent to E-CIN-DBA if the alerts are set up correctly.
8. Ensure that the “Everyone” group does not have more than Read access to the SQL Server registry keys.
9. Configure NTFS permissions on the SQL Error Logs folder (G:\MSSQL.1\MSSQL\LOG) properly. Setup the folder as a share with the name SQLLOG$, and the permissions on the share are Everyone Full Control. Depending on the SQL Server depends on if Development needs access to the Log folder. Security on the folder would be setup with the following accounts:
   1. R-CIN-Development (List Folder Contents and Read)
   2. R-CIN-DevelopmentCont (List Folder Contents and Read)
   3. SQL Service Account (Full Control)
10. If WinZip is installed, Set the path **C:\Program Files\WinZip** in the system variables. Login to the server, right click the computer icon, and select properties. Click the Advanced System Settings link, and click on the Environment Variables button. In the System Variables box, highlight **Path** and click on Edit. At the end of the line, add the following: “**;C:\Program Files\WinZip**”. There should be NO spaces between the ; (semi-colon).
11. Verify DTC is enabled on the OS. Infrastructure should do this but check to make sure it is enabled. Start, Administrative Tools, Component Services. Drill down on Component Services, Computer, My Computer, Distributed Transaction Coordinator. Right click Local DTC and select Properties. Select Security tab. Select **Network DTC Access,** and **Allow Remote Administration.** Select **Allow Inbound, Allow Outbound,** and **Mutual Authentication Required.** Click OK, Click OK.
12. **REBOOT** **THE SERVER WHEN COMPLETE WITH THE ADMIN TASKS.**

**Setting SPN in Active Directory**

1. Contact infrastructure to set the SPN “Service Principal Name” in Active Directory. Give them the domain user account that’s being used as the SQL Server Service account and the port (this is usually port 1433 but you need to verify this). Once this is added to AD one can register the new SQL Server instance remotely in SQL Server Management Studio. If this is not performed you will receive the following error attempting to register the new SQL Server instance in SSMS.   
   "Cannot generate SSPI context"

Infrastructure area group domain admin

1. To verify open a command prompt on a server. Type “setspn –l sqlserveraccount” and press enter. A list will be returned of all servers listed for that account and the port that it is set to use.

**Licensing Needed for Production Servers**

1. SQL Safe Backup
2. SQL Compliance – Check to see if there are any licenses not being used.

**Setup Database Backups**

1. You can find a sample database backup in the folder [\\shermfin.com\dfs\CIN\groups\DBA\SQL\Standard\_Build\SQL2016\DailyJobs](file:///\\shermfin.com\dfs\CIN\groups\DBA\SQL\Standard_Build\SQL2016\DailyJobs)
2. In the backups for each database, you need to update the job with the appropriate database and path.
3. Setup a folder on the server (G:\ or X:\) drive called SQLBackup.
4. Then setup a share on the folder SQLBackup called SQLBackup$ with the following permissions on the share: Everyone, Full Control; and the following permissions on the folder: Administrators, SQLServerAccount, and R-CIN-DBA with Full Control.
5. For those databases that will have Transaction Log backups included on them, you need to create a folder under the SQLBackup folder called TransactionLog.
6. Set the Backup Jobs to Page the Operator SQLSupportPager on failure.
7. Update the time on the **TerminateConnections** SQL Job to run 5 minutes before the backup jobs are set to kick off.

**Set DBCC Checks**

1. You can find a sample DBCC check in the folder [\\shermfin.com\dfs\CIN\groups\DBA\SQL\Standard\_Build\SQL2016\DailyJobs](file:///\\shermfin.com\dfs\CIN\groups\DBA\SQL\Standard_Build\SQL2016\DailyJobs)
2. The name of the text file the output is saved to should be *NameOfServer\_*DailyDBCCJob.txt (ex: SQL02\_DailyDBCCJob.txt).
3. Verify the folder on the G:\ drive under the MSSQL.1\MSSQL folder called SQLJobOutput has been setup. If not, create the folder. This will need to be setup as a share (called SQLJobOutput$) with the following permissions on the share: Everyone, Full Control; and the following permissions on the folder: Administrators, SQLServerAccount, and R-CIN-DBA with Full Control.
4. Verify the job is setup with all the user and system databases to be checked and each step is setup to go to the output file mentioned above with the appropriate path to where the file will be located.
5. The first step of the job should have the ‘overwrite’ option selected on the output file while step 2 – *n* will have the ‘append’ option selected.
6. Set the DBCC Job to Page the Operator SQLSupportPager on failure.

**Adding to CommVault / Tape Backup Rotation**

A Help Desk ticket must be placed with the following information in the case:

* Name of server
* Time the tape backup should run (**NOTE:** Do not overlap the tape backup with the database backups)