Ahsay Backup

Ahsay Online Backup Manager v8

Microsoft SQL Server Backup and Restore Guide

Ahsay Systems Corporation Limited

11 October 2021

www.ahsay.com

A wholly owned subsidiary of
Ahsay Backup Software Development Company Limited
HKEx Stock Code: 8290

Copyright Notice

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System and Ahsay NAS Client Utility, Ahsay Mobile are trademarks of Ahsay Systems Corporation Limited.

Amazon S3 is a registered trademark of Amazon Web Services, Inc., or its affiliates.

Apple and Mac OS X, macOS, and iOS are registered trademarks of Apple Computer, Inc.

Dropbox is a registered trademark of Dropbox Inc.

Google Cloud Storage, Google Drive, Google Authenticator, and Android are registered trademarks of Google Inc.

Wasabi Hot Cloud Storage is a registered trademark of Wasabi Technologies Inc.

Backblaze B2 Cloud Storage is a registered trademark of Backblaze Inc.

MariaDB is a registered trademark of MariaDB Corporation AB.

Lotus, Domino, and Notes are registered trademark of IBM Corporation.

Microsoft Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, OneDrive, OneDrive for Business, Microsoft Authenticator, and Microsoft Office 365 are registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle 11g, Oracle 12c, Oracle 18c, Oracle 19c, and MySQL are registered trademarks of Oracle Corporation.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the U.S. and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

VMware ESXi, vCenter, and vSAN are registered trademarks of VMware, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

Ahsay Systems Corporation Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions	Type of modification
25 January 2021	Updated screenshot in Ch. 2.4; Updated PDIC diagram in Ch. 6; Updated login steps in Ch. 7	Modification
7 April 2021	Updated Ch. 6.1 & 6.2; Added sub-chapters for the detailed process diagrams in Ch. 6.3, 6.4, 6.4.1, 6.4.2 and 6.5	New / Modifications
11 October 2021	Updated login instructions in Ch. 7	Modifications

Table of Contents

1 Overview

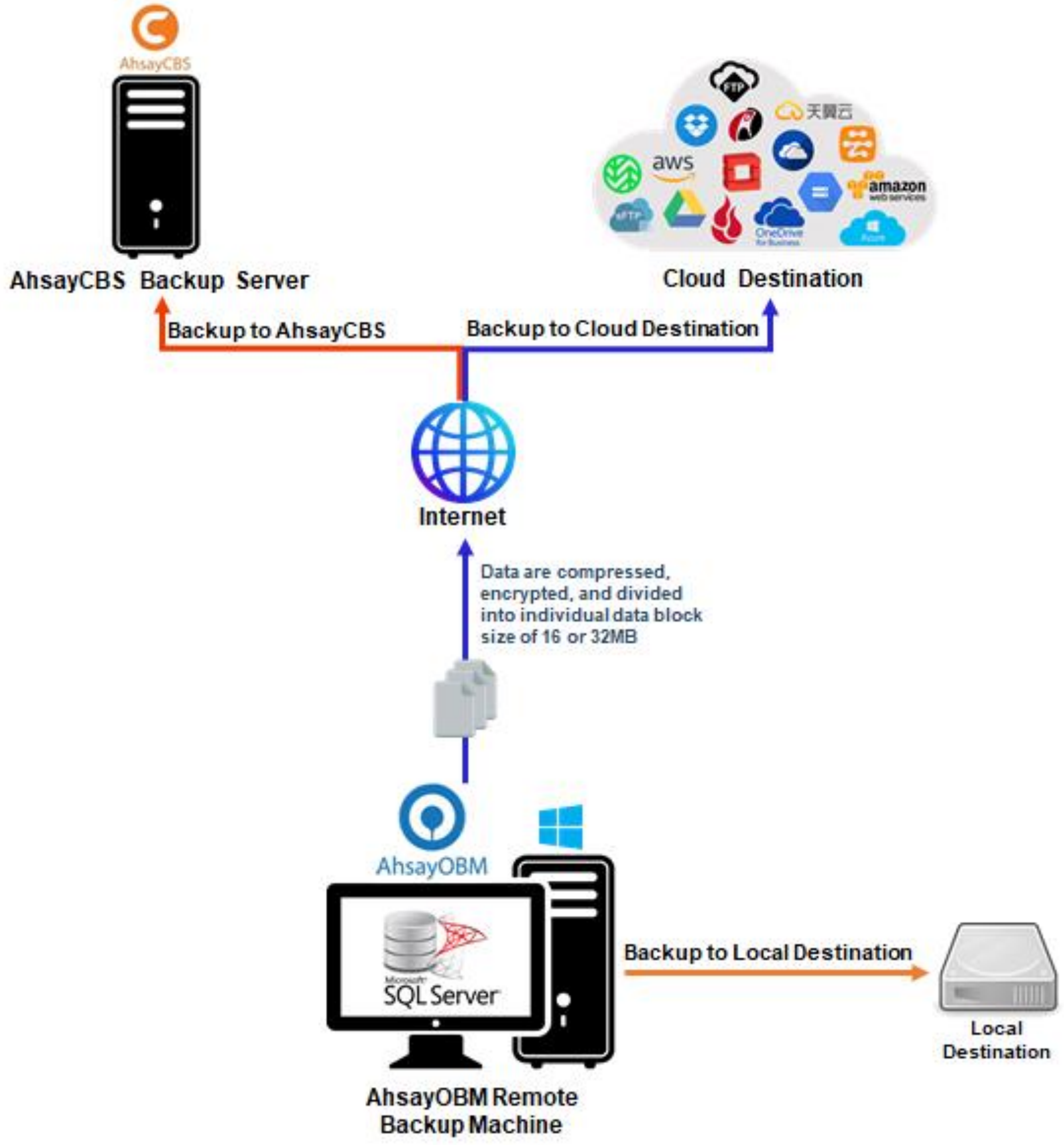
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a comprehensive backup solution for your MS SQL Server. The MS SQL Server module of AhsayOBM provides you with a set of tools to protect your MS SQL Server, whether in VSS backup mode or ODBC backup mode.

1.2 System Architecture

Below is the system architecture diagram illustrating the major elements involved in the backup process among the MS SQL server, AhsayOBM and AhsayCBS.

In this user guide, we will focus on the software installation, as well as the end-to-end backup and restore process using the AhsayOBM as a client backup software.


AhsayCBS
AhsayCBS Backup Server
Cloud Destination
Backup to AhsayCBS
Backup to Cloud Destination
Internet
Data are compressed, encrypted, and divided into individual data block size of 16 or 32MB
AhsayOBM
SQL Server
Backup to Local Destination
Local Destination
AhsayOBM Remote Backup Machine

2 Requirements

You are strongly recommended to configure or check all the requirements below before you proceed with the MS SQL server backup and restoration.

2.1 Hardware Requirement

Refer to the following article for the list of hardware requirements for AhsayOBM:
FAQ: Ahsay Hardware Requirement List (HRL) for version 8.1 or above

2.2 Software Requirement

Refer to the following article for the list of compatible operating systems and application versions: FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

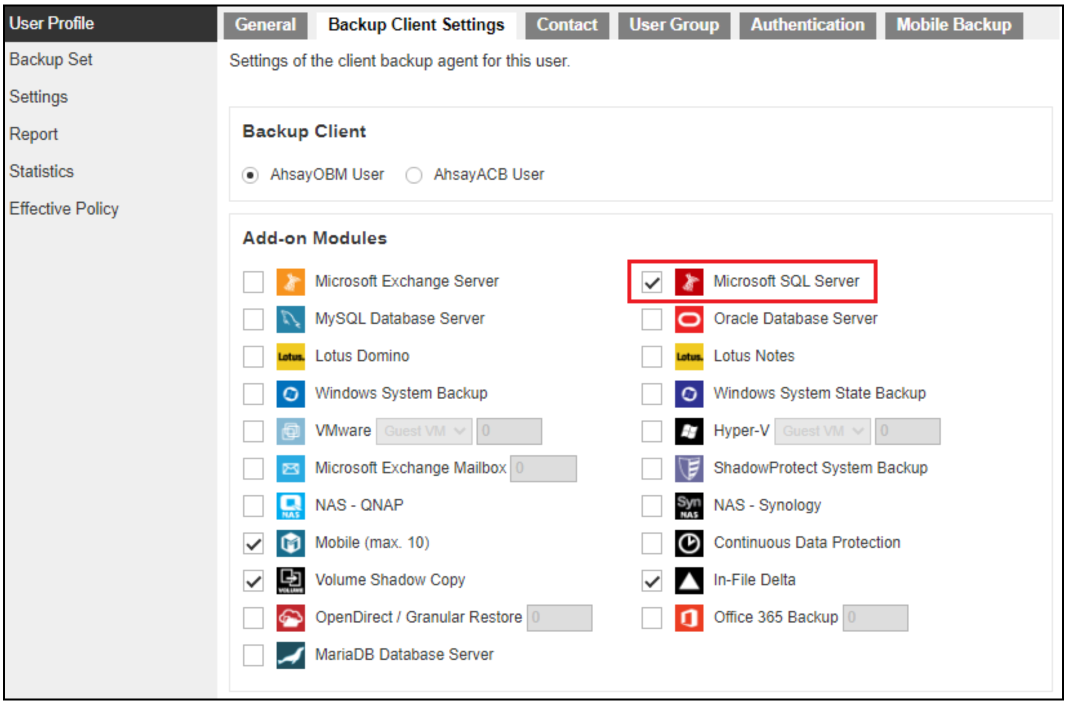
2.3 AhsayOBM Installation

Make sure the latest version of AhsayOBM is installed directly on the machine where the MS SQL Server database(s) are hosted.

NOTE
Backup and restore of MS SQL Server database(s) running on a remote machine is not supported.

2.4 AhsayOBM Add-On Module Configuration

Make sure the Microsoft SQL Server feature has been enabled as an add-on module in your AhsayOBM user account. Contact your backup service provider for more details.



Settings of the client backup agent for this user.

Backup Client

● AhsayOBM User ○ AhsayACB User

Add-on Modules

- □ Microsoft Exchange Server
- □ MySQL Database Server
- □ Lotus Domino
- □ Windows System Backup
- □ VMware Guest VM 0
- □ Microsoft Exchange Mailbox 0
- □ NAS - QNAP
- ☑ Mobile (max. 10)
- ☑ Volume Shadow Copy
- □ OpenDirect / Granular Restore 0
- □ MariaDB Database Server
- ☑ Microsoft SQL Server
- □ Oracle Database Server
- □ Lotus Notes
- □ Windows System State Backup
- □ Hyper-V Guest VM 0
- □ ShadowProtect System Backup
- □ NAS - Synology
- □ Continuous Data Protection
- ☑ In-File Delta
- □ Office 365 Backup 0

2.5 Backup Quota Requirement

Make sure that your AhsayOBM user account has sufficient storage quota assigned to accommodate the storage of MS SQL Server backup set and retention policy.

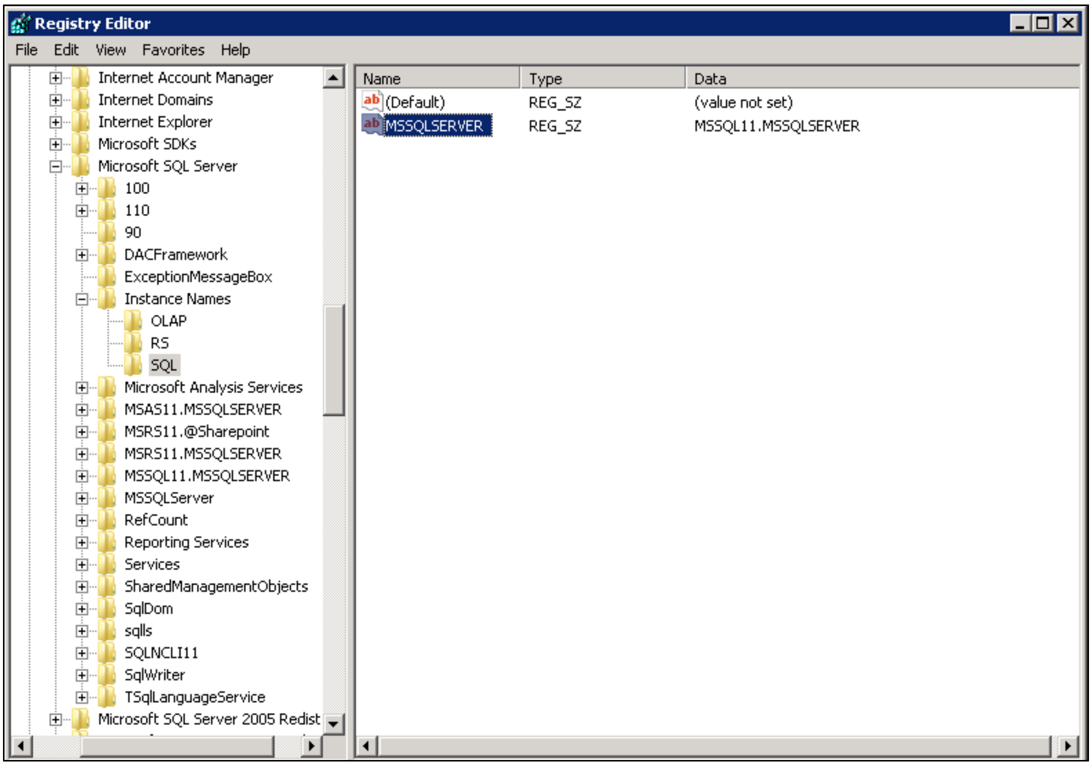
2.6 Java Heap Size

The default Java heap size setting on AhsayOBM is 2048MB. For MS SQL Server backup it is highly recommended to increase the Java heap size setting to be at least 4096MB to improve backup and restore performance. The actual heap size is dependent on the amount of free memory available on your MS SQL server.

2.7 MS SQL Server Registry

Make sure the MS SQL entry is present in the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names\SQL".

To access this path, type “regedit” in the command prompt to launch the Registry Editor.



Name	Type	Data
(Default)	REG_SZ	(value not set)
MSSQLSERVER	REG_SZ	MSSQL11.MSSQLSERVER

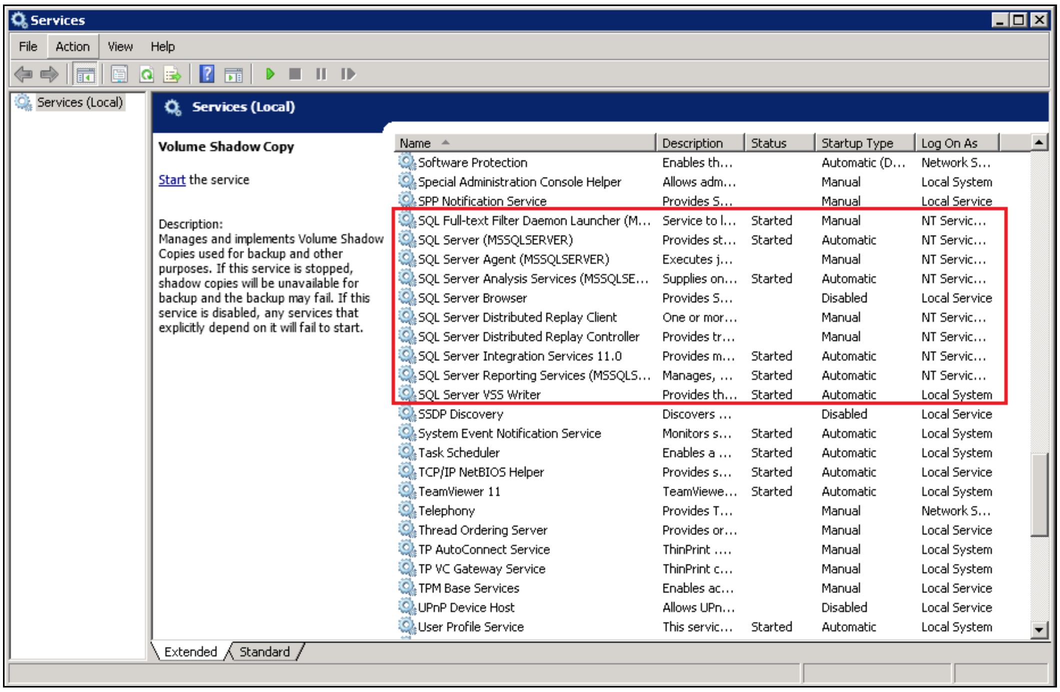
NOTE

Pay extra attention when you are checking configuration in Registry Editor. Any unauthorized changes could cause interruption to the Windows operation.

2.8 SQL Server Services

Ensure that the following SQL Server Services have been enabled in the Windows Services menu.

Launch **Services** in Windows by clicking **Start** then typing “Services” in the search box. All MS SQL server related services should be started by default. If in case it is not, turn it on by right clicking the item then selecting **Start**.



Volume Shadow Copy

Start the service

Description:
Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Software Protection	Enables th...		Automatic (D...	Network S...
Special Administration Console Helper	Allows adm...		Manual	Local System
SPP Notification Service	Provides S...		Manual	Local Service
SQL Full-text Filter Daemon Launcher (M...	Service to l...	Started	Manual	NT Servic...
SQL Server (MSSQLSERVER)	Provides st...	Started	Automatic	NT Servic...
SQL Server Agent (MSSQLSERVER)	Executes j...		Manual	NT Servic...
SQL Server Analysis Services (MSSQLSE...	Supplies on...	Started	Automatic	NT Servic...
SQL Server Browser	Provides S...		Disabled	Local Service
SQL Server Distributed Replay Client	One or mor...		Manual	NT Servic...
SQL Server Distributed Replay Controller	Provides tr...		Manual	NT Servic...
SQL Server Integration Services 11.0	Provides m...	Started	Automatic	NT Servic...
SQL Server Reporting Services (MSSQLS...	Manages, ...	Started	Automatic	NT Servic...
SQL Server VSS Writer	Provides th...	Started	Automatic	Local System
SSDP Discovery	Discovers ...		Disabled	Local Service
System Event Notification Service	Monitors s...	Started	Automatic	Local System
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Provides s...	Started	Automatic	Local Service
TeamViewer 11	TeamViewe...	Started	Automatic	Local System
Telephony	Provides T...		Manual	Network S...
Thread Ordering Server	Provides or...		Manual	Local Service
TP AutoConnect Service	ThinPrint		Manual	Local System
TP VC Gateway Service	ThinPrint c...		Manual	Local System
TPM Base Services	Enables ac...		Manual	Local Service
UPnP Device Host	Allows UPn...		Disabled	Local Service
User Profile Service	This servic...	Started	Automatic	Local System

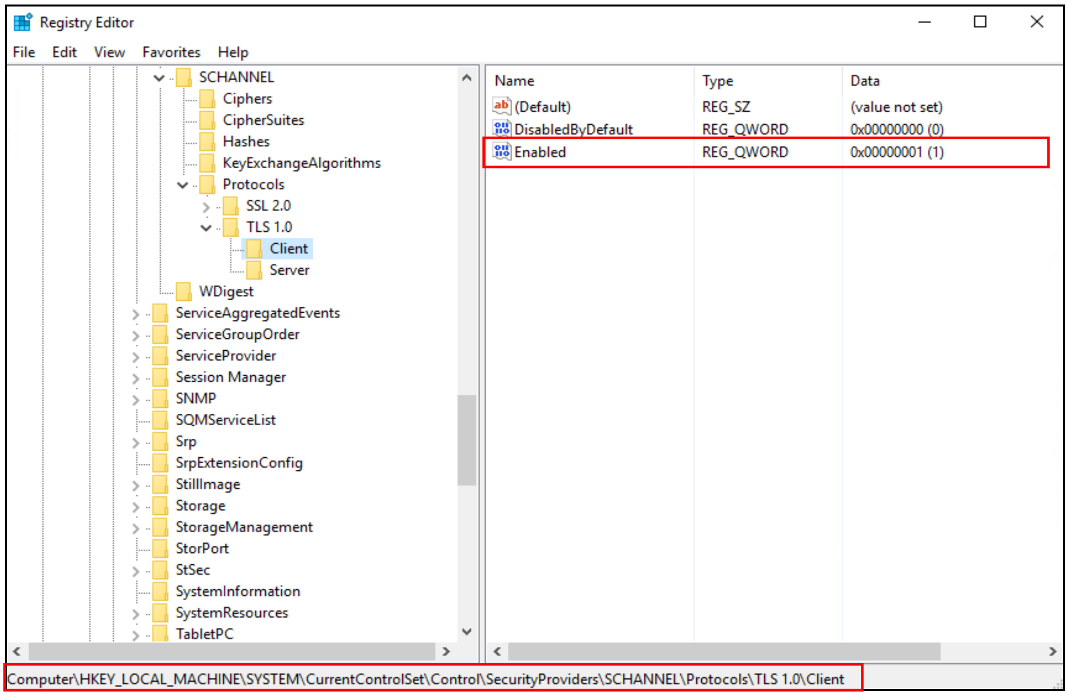
2.9 Transport Layer Security (TLS)

For MS SQL Server 2005, 2008, 2012, and 2014 VSS and ODBC backup modes, TLS version 1.0 must be enabled as only TLS version 1.0 is supported.

To check if TLS 1.0 is enabled on the MS SQL machine, launch the registry editor and locate the following path:

“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client”

The value of registry key should be “1” to indicate that TLS 1.0 is enabled.



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_QWORD	0x00000000 (0)
Enabled	REG_QWORD	0x00000001 (1)

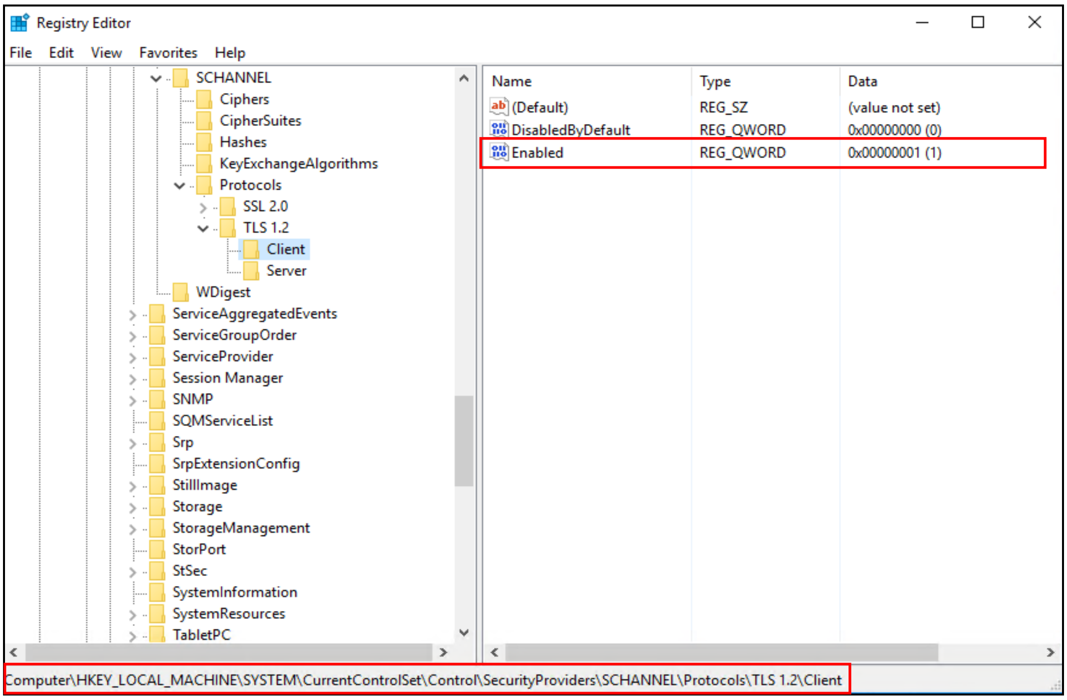
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client

Meanwhile, for MS SQL Server 2016, 2017 and 2019 VSS and ODBC backup modes, TLS version 1.2 must be enabled as only TLS version 1.2 is supported.

To check if TLS 1.2 is enabled on the MS SQL machine, launch the registry editor and locate the following path:

“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client”

The value of registry key should be “1” to indicate that TLS 1.2 is enabled.

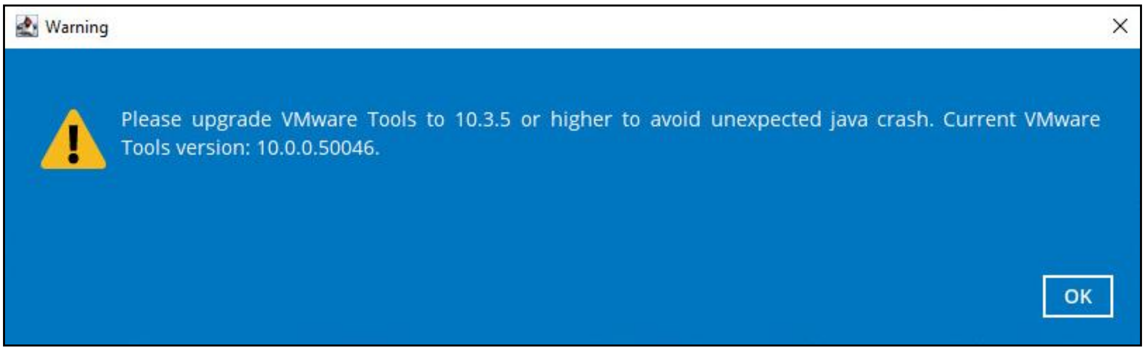


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_QWORD	0x00000000 (0)
Enabled	REG_QWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client

2.10 Upgrade VMware Tools Requirement

To avoid unexpected java crash, if the Windows machine is a guest VM hosted on a VMware Host then it is highly recommended that the VMware tools version installed on the guest VM must be 10.0.5 or above. Below is the warning message that will be displayed if the version of the VMware Tools is less than 10.0.5.



Please upgrade VMware Tools to 10.3.5 or higher to avoid unexpected java crash. Current VMware Tools version: 10.0.0.50046.

NOTE

For more information about the upgrade of VMware Tools, refer to the following article: http://wiki.ahsay.com/doku.php?id=public:5288_ahsayobc_crash_on_vm_with_vmware_tools_pre-10.0.5.

AhsayOBM supports two backup modes when creating a backup set for MS SQL server: VSS mode and ODBC mode.

2.11 VSS Backup Mode

The VSS-based backup utilizing the Microsoft SQL Server VSS Writer to obtain a consistent snapshot of the MS SQL databases, no spooling / staging of database file(s) is required during the backup process.

2.11.1 User Account Privileges

Make sure the operating system account that performs the backup and restore has sufficient permission to access both SQL server and VSS.

2.11.2 Temporary Directory Folder

- The temporary directory folder is used by AhsayOBM for storing backup set index files and incremental/differential delta files. To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder to be set to a local drive. The temporary folder should not be located on Windows system partition or the database partition to minimize any potential performance impact on Windows or database.

- It is recommended that the temporary directory folder should have at least free disk space of 50% of the total database size because the default Delta ratio is 50%. The actual free disk space required depends on various factors including the size of the database, number of backup destinations, backup frequency, in-file delta settings etc.

- The SQL Windows service must have read and write permission to the temporary directory.

2.11.3 SQL Server VSS Writer

Make sure the **SqlServerWriter** has been installed and running on the SQL server, and the writer state is **Stable**. This can be verified by running the "**vssadmin list writers"** command in the Windows Command Prompt.

If you do not find the SqlServerWriter in the result, make sure the SQL Server VSS Writer has been started by following the instructions in Windows Services section below.

Example:

```
C:\Users\Administrator>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-
line tool
(C) Copyright 2001-2013 Microsoft Corp.

Writer name: 'Task Scheduler Writer'
   Writer Id: {d61d61c8-d73a-4eee-8cdd-f6f9786b7124}
   Writer Instance Id: {1bddd48e-5052-49db-9b07-b96f96727e6b}
   State: [1] Stable
   Last error: No error

Writer name: 'VSS Metadata Store Writer'
   Writer Id: {75dfb225-e2e4-4d39-9ac9-ffaff65ddf06}
   Writer Instance Id: {088e7a7d-09a8-4cc6-a609-ad90e75ddc93}
   State: [1] Stable
   Last error: No error

Writer name: 'Performance Counters Writer'
   Writer Id: {0bada1de-01a9-4625-8278-69e735f39dd2}
   Writer Instance Id: {f0086dda-9efc-47c5-8eb6-a944c3d09381}
   State: [1] Stable
   Last error: No error

Writer name: 'SqlServerWriter'
   Writer Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}
   Writer Instance Id: {3de4f842-4d57-4198-9949-3b3f8c2629dc}
   State: [1] Stable
   Last error: No error

Writer name: 'System Writer'
   Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
   Writer Instance Id: {32d2fccc-624f-4baa-beb3-17b27fcae9ee}
   State: [1] Stable
   Last error: No error

Writer name: 'ASR Writer'
   Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
   Writer Instance Id: {e8580fb0-b51f-40ab-91bf-4eff5107c4d1}
   State: [1] Stable
   Last error: No error

Writer name: 'WMI Writer'
   Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}
   Writer Instance Id: {de1b6322-1d96-4f85-adbf-05cb517322ea}
   State: [1] Stable
   Last error: No error

Writer name: 'BITS Writer'
   Writer Id: {4969d978-be47-48b0-b100-f328f07ac1e0}
   Writer Instance Id: {a623b49f-a3d4-42d2-af9a-4e924fb31262}
   State: [1] Stable
   Last error: No error

Writer name: 'Registry Writer'
   Writer Id: {afbab4a2-367d-4d15-a586-71dbb18f8485}
   Writer Instance Id: {cc6b42f1-ebd0-429f-b3d3-e860905d40d3}
   State: [1] Stable
   Last error: No error

Writer name: 'Shadow Copy Optimization Writer'
   Writer Id: {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
   Writer Instance Id: {957ff981-d54f-4a1f-8798-bd9bd76396bd}
   State: [1] Stable
   Last error: No error

Writer name: 'COM+ REGDB Writer'
   Writer Id: {542da469-d3e1-473c-9f4f-7847f01fc64f}
   Writer Instance Id: {801fea63-6bfc-406d-9a40-4ad5af484773}
   State: [1] Stable
   Last error: No error
```

2.11.4 MS SQL Server Volumes

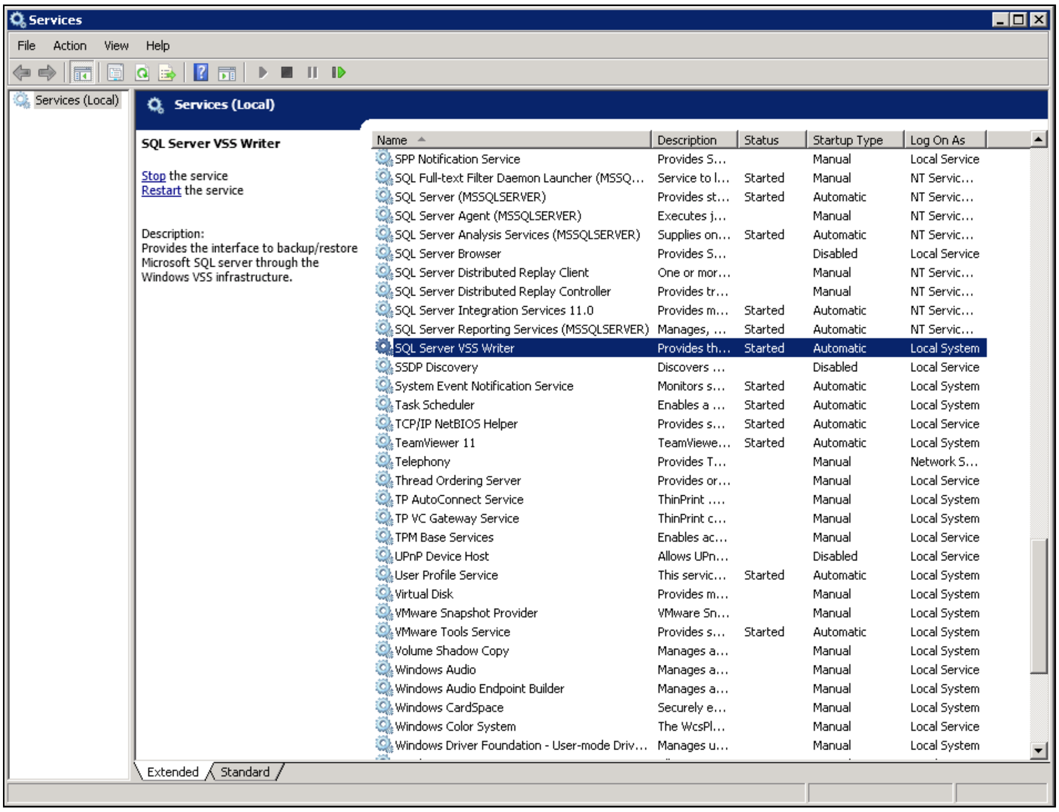
MS SQL Server volumes must use a file system which supports the use of VSS snapshot, for example NTFS.

2.11.5 Windows Services

Ensure that the following services have been enabled in the Windows Services menu.

Launch **Services** in Windows by clicking **Start** then typing “Services” in the search box. All MS SQL server related services should be started by default, in case if it is not, turn it on by right clicking the item then selecting **Start**.

1. **SQL Server VSS Writer**



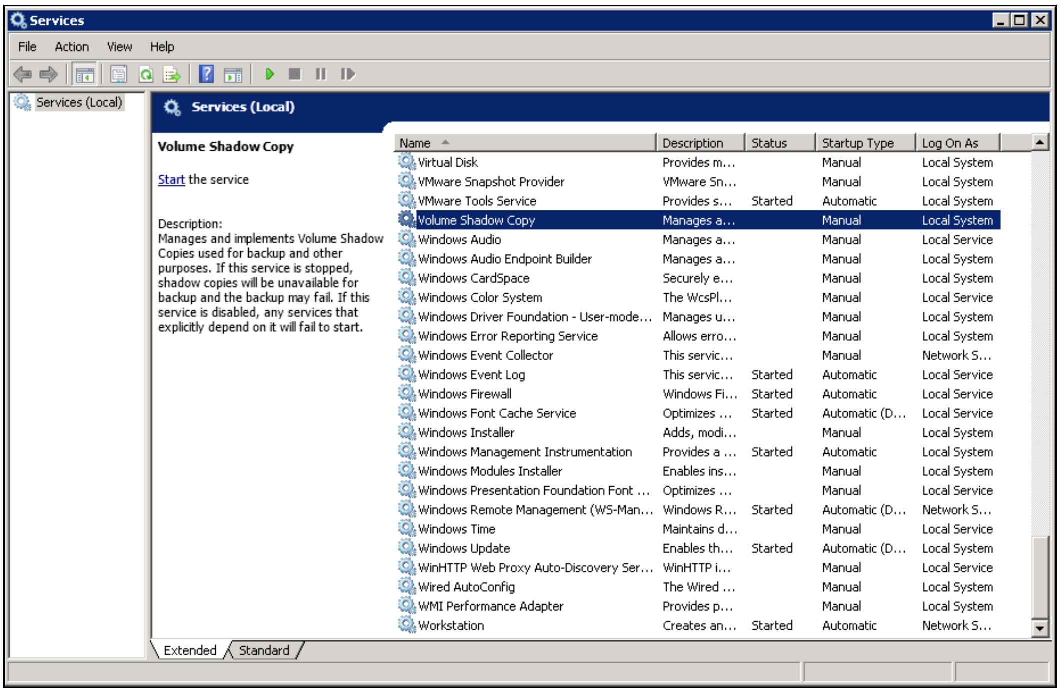
SQL Server VSS Writer

Stop the service
Restart the service

Description:
Provides the interface to backup/restore Microsoft SQL server through the Windows VSS infrastructure.

Name	Description	Status	Startup Type	Log On As
SPP Notification Service	Provides S…		Manual	Local Service
SQL Full-text Filter Daemon Launcher (MSSQ…	Service to l…	Started	Manual	NT Servic…
SQL Server (MSSQLSERVER)	Provides st…	Started	Automatic	NT Servic…
SQL Server Agent (MSSQLSERVER)	Executes j…		Manual	NT Servic…
SQL Server Analysis Services (MSSQLSERVER)	Supplies on…	Started	Automatic	NT Servic…
SQL Server Browser	Provides S…		Disabled	Local Service
SQL Server Distributed Replay Client	One or mor…		Manual	NT Servic…
SQL Server Distributed Replay Controller	Provides tr…		Manual	NT Servic…
SQL Server Integration Services 11.0	Provides m…	Started	Automatic	NT Servic…
SQL Server Reporting Services (MSSQLSERVER)	Manages, …	Started	Automatic	NT Servic…
SQL Server VSS Writer	Provides th…	Started	Automatic	Local System
SSDP Discovery	Discovers …		Disabled	Local Service
System Event Notification Service	Monitors s…	Started	Automatic	Local System
Task Scheduler	Enables a …	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Provides s…	Started	Automatic	Local Service
TeamViewer 11	TeamViewe…	Started	Automatic	Local System
Telephony	Provides T…		Manual	Network S…
Thread Ordering Server	Provides or…		Manual	Local Service
TP AutoConnect Service	ThinPrint ….		Manual	Local System
TP VC Gateway Service	ThinPrint c…		Manual	Local System
TPM Base Services	Enables ac…		Manual	Local Service
UPnP Device Host	Allows UPn…		Disabled	Local Service
User Profile Service	This servic…	Started	Automatic	Local System
Virtual Disk	Provides m…		Manual	Local System
VMware Snapshot Provider	VMware Sn…		Manual	Local System
VMware Tools Service	Provides s…	Started	Automatic	Local System
Volume Shadow Copy	Manages a…		Manual	Local System
Windows Audio	Manages a…		Manual	Local Service
Windows Audio Endpoint Builder	Manages a…		Manual	Local System
Windows CardSpace	Securely e…		Manual	Local System
Windows Color System	The WcsPl…		Manual	Local Service
Windows Driver Foundation - User-mode Driv…	Manages u…		Manual	Local System

2. **Volume Shadow Copy**



Volume Shadow Copy

Start the service

Description:
Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Virtual Disk	Provides m…		Manual	Local System
VMware Snapshot Provider	VMware Sn…		Manual	Local System
VMware Tools Service	Provides s…	Started	Automatic	Local System
Volume Shadow Copy	Manages a…		Manual	Local System
Windows Audio	Manages a…		Manual	Local Service
Windows Audio Endpoint Builder	Manages a…		Manual	Local System
Windows CardSpace	Securely e…		Manual	Local System
Windows Color System	The WcsPl…		Manual	Local Service
Windows Driver Foundation - User-mode …	Manages u…		Manual	Local System
Windows Error Reporting Service	Allows erro…		Manual	Local System
Windows Event Collector	This servic…		Manual	Network S…
Windows Event Log	This servic…	Started	Automatic	Local Service
Windows Firewall	Windows Fi…	Started	Automatic	Local Service
Windows Font Cache Service	Optimizes …	Started	Automatic (D…	Local Service
Windows Installer	Adds, modi…		Manual	Local System
Windows Management Instrumentation	Provides a …	Started	Automatic	Local System
Windows Modules Installer	Enables ins…		Manual	Local System
Windows Presentation Foundation Font …	Optimizes …		Manual	Local Service
Windows Remote Management (WS-Man…	Windows R…	Started	Automatic (D…	Network S…
Windows Time	Maintains d…		Manual	Local Service
Windows Update	Enables th…	Started	Automatic (D…	Local System
WinHTTP Web Proxy Auto-Discovery Ser…	WinHTTP i…		Manual	Local Service
Wired AutoConfig	The Wired …		Manual	Local System
WMI Performance Adapter	Provides p…		Manual	Local System
Workstation	Creates an…	Started	Automatic	Network S…

2.11.6 MS SQL Recovery Model

VSS backup mode does not support backup of transaction log files, but for databases configured in either Full or Bulk-logging recovery model, this may eventually result in transaction logs filling up the available disk space on the volume of the MS SQL Server.

https://technet.microsoft.com/en-us/library/cc966520.aspx

To prevent this from occurring, you can modify the recovery model of database selected for backup to Simple.

Alternatively, to truncate the transaction log files, you can perform a transaction log backup manually (with the instruction provided in Appendix B) or create an additional MS SQL database backup set in ODBC backup mode to perform a transaction log backup.

Please refer to ODBC Backup Mode for further details.

2.12 ODBC Backup Mode

2.12.1 Temporary Directory Folder

- The temporary directory folder is used by AhsayOBM for storing the database files, incremental/differential delta files and backup set index files. To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive.

- The temporary folder should not be located on Windows system partition or the database partition to minimize any potential performance impact on Windows or database. If the temporary directory folder is located on a network drive, make sure the login account has sufficient permission to access the network resources.

- Please refer to the following URL for more details:

  https://support.microsoft.com/en-us/help/2926557/sql-server-vdi-backup-and-restore-operations-require-sysadmin-privileg

  https://technet.microsoft.com/en-us/library/cc966520.aspx

- It is recommended that the temporary directory folder should have at least free disk space of 150% of the total database size. The actual free disk space required depends on various factors including the size of the database, number of backup destinations, backup frequency, in-file delta settings etc.

  NOTE

  To determine if the drive for temporary folder has enough disk space to accommodate the spooling of the database(s) in ODBC backup mode, please refer to Appendix E.

- The SQL Windows service must have read and write permission to the temporary directory.

2.12.2 Maximum Worker Thread

For SQL instance with large number of database (more than 500 databases), consider increasing the “Maximum Worker Thread” setting. Refer to the article below for further details.
https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-max-worker-threads-server-configuration-option

2.12.3 MS SQL Recovery Model

ODBC backup mode supports transaction log backup for database with Full recovery model.

- For database with Simple recovery mode, only full database and differential database backups can be performed.

  https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server

- To perform a transaction log backup, please change the recovery model of corresponding databases from Simple to Full.

  https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/view-or-change-the-recovery-model-of-a-database-sql-server

2.12.4 ODBC Mode Authentication Methods

ODBC backup mode supports two types authentication method:

- Trusted Authentication

  This is the default authentication method in the MS SQL Server. When using this method, MS SQL Server uses the Windows login account to authenticate the login to the MS SQL Server.

- MS SQL Authentication

  When using this method, the username and password are created and stored in the MS SQL Server.

For details on how to verify if the login credentials you intend to use to authenticate the MS SQL Server backup job on AhsayOBM has the correct permissions, and to determine if the drive for temporary folder has enough disk space to accommodate the spooling of the database(s), please refer to Appendix E.

NOTE

It is recommended to use the Trusted Authentication method wherever possible as this type of method is tightly integrated with Windows which has an integrated security. MS SQL Server trusts the credentials provided by Windows as Windows authentication uses a series of encrypted messages to authenticate users in the MS SQL Server.

However, when MS SQL Server logins are used, MS SQL Server login names and encrypted passwords are passed across the network, which makes them less secure.

3 Best Practice and Recommendation

3.1 Considerations for Backing up and Restore of System Databases

Refer to the following tables for considerations for backup and restoration of system databases.

3.1.1 For backup of system databases

SQL server maintains a set of system level database which are essential for the operation of the server instance.

Several of the system databases must be backed up after every significant update, they include:

1. **master**
2. **model**
3. **msdb**
4. **distribution** (for SQL database with replication enabled only)

This table summarizes all of the system databases.

System	Description	Backup	Suggestion
master	The database that records all of the system level information of a SQL server system.	Yes	To back up any database, the instance of SQL server must be running. Startup of an instance of SQL server requires that the master database is accessible and at least partly usable. Back up the master database as often as necessary to protect the data sufficiently for your business needs. Microsoft recommends a regular backup schedule, which you can supplement with manual backup after any substantial update.
model	The template for all databases that are created on the instance of SQL server.	Yes	Backup the model database only when necessary, for example, after customizing its database options. Microsoft recommends that you create only full database backups of model, as required. Because model is small and rarely changes, backing up the log is unnecessary.
msdb	The msdb database is used by SQL Server Agent for	Yes	Back up the msdb whenever it is updated.

	scheduling alerts and jobs, and for recording operators. It also contains history tables (e.g. backup / restore history table).		
tempdb	A workspace for holding temporary or intermediate result sets. This database is recreated every time an instance of SQL server is started.	No	The tempdb system database cannot be backed up.
distribution	The distribution database exists only if the server is configured as a replication distributor. It stores metadata and history data for all types of replication, and transactions for transactional replication.	Yes	Replicated databases and their associated system databases should be backed up regularly.

3.1.2 For restore of system databases

System database	Restoration suggestion
master	To restore any database, the instance of SQL server must be running. Startup of an instance of SQL server requires that the master database is accessible and at least partly usable. Restore or rebuild the master database completely if master becomes unusable.
model	Restore the model database if: ➢ The master database has been rebuilt. ➢ The model database has been damaged, for example due to media failure. ➢ The model database has been modified, in this case, it is necessary to restore model from a backup when you rebuild master, because the Rebuild Master utility deletes and recreates model.
msdb	Restore the msdb database if the master database has been rebuilt.
distribution	For restore strategies of distribution database, please refer to the following online document from Microsoft for more details: http://msdn.microsoft.com/enus/library/ms152560.aspx

3.2 Best Practices and Recommendations

The following are some best practices and recommendations we strongly recommend you follow before you start any MS SQL Server backup and restore.

1. For VSS backup mode, it is suggested to set the backup schedule to a time when system activity is low to achieve the best possible performance.

2. It is recommended to use ODBC backup mode for backup of database with a high volume of transaction, since such setup may require frequent backups. Transaction log backup (which is only supported by ODBC backup mode) can be performed periodically and is less resource intensive than VSS based backup.

3. For maximum data protection and restore options, it is recommended to configure:

   i. At least one offsite or cloud destination

   ii. At least one local destination for fast recovery

4. Perform test restores periodically to ensure your backup is set up and performed properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan. It is important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

5. The Restore Raw File option is for advanced MS SQL Server administrator and should only be used if you have in-depth knowledge and understanding of your MS SQL Server, otherwise, it is not recommended to use this option as there are additional MS SQL techniques required to perform the manual restore.

6. To ensure an optimal backup/restoration performance, it is highly recommended to set the temporary directory folder to a location with sufficient free disk space. It must be on another location other than Drive C: (e.g. Drive E:).

7. The periodic backup schedule should be reviewed regularly to ensure that the interval is sufficient to handle the data volume on the machine. Over time, data usage pattern may change on a production server, i.e. the number of new files created, the number of files which are updated/deleted, and new users may be added etc.

   Consider the following key points to efficiently handle backup sets with periodic backup schedule.

   - Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,

     - so that the data is always backed up within the periodic backup interval

     - so that the backup frequency does not affect the performance of the production server

   - Network – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.

- Retention Policy - also make sure to consider the retention policy settings and retention area storage management which can grow because of the changes in the backup data for each backup job.

NOTE

Make sure that the latest version of AhsayOBM is installed directly on the MS SQL server as the backup of MS SQL server databases running on a remote machine is not supported.

4 Limitation

4.1 Standalone Environment Only

AhsayOBM does not support backup of MS SQL server in cluster environment, only standalone environment is supported.

4.2 VSS Backup Mode

1. Only support backup of database on local drive. Database on network drive is not supported. For backup of database on a network drive, it is recommended to use ODBC backup mode instead.

2. VSS backup mode does not support transaction log backup, therefore, transaction log backup will have to be done manually. Or you can choose ODBC backup mode for transaction log backup.

3. In order to truncate transaction logs, you have to perform a manual log truncation, which could be time consuming.

4.3 File System for Database Snapshot

You cannot create database snapshots on FAT32 file system or RAW partitions. The sparse files used by database snapshots are provided by the NTFS file system.

4.4 SQL Server Version

1. **Automated Restore Option**
   If you have chosen the automated restoration to the Original SQL server or Alternate SQL server of your selection, the restoration can only be done in a SQL server version that is the same as the one used for performing the backup.

2. **Manual Raw file Restore Option**
   If you have chosen to restore the raw file, the raw database file(s) can be manually restored to the same or newer SQL server version that you used to perform the backup.

4.5 Restoration to Other SQL Server

1. If you would like to restore database to an alternate SQL server, you can only choose to restore one database to restore at a time.

2. If you would like to restore database to an alternate SQL server, make sure you choose to restore raw file by enabling the checkbox **Restore raw file**.

4.6 Remote Machine Backup

MS SQL server databases backup running on a remote machine is not supported. Ensure that the latest version of AhsayOBM is installed directly on the MS SQL server.

5 Backup Mode

You can choose from one of the two backup modes when creating a backup set for MS SQL server. The information below provides you with more details on each backup mode.

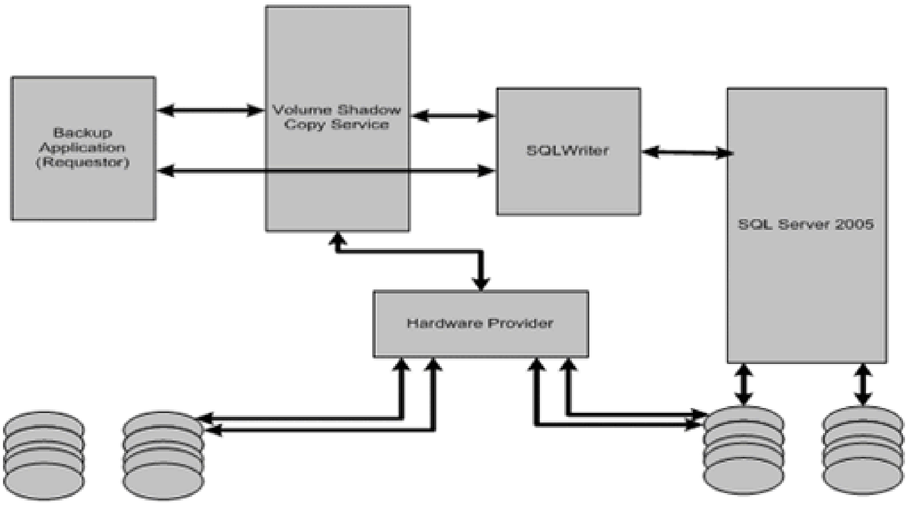
NOTE

For MS SQL server backup sets which are upgraded from v6, the default backup mode will be ODBC.

VSS Mode

Introduction

VSS-based backup utilizing the Microsoft SQL Server VSS Writer to obtain a consistent snapshot of the MS SQL databases, no spooling / staging of database file(s) is required during the backup process.



(Diagram from Microsoft)

Temporary Folder Requirement

- **<u>Location for temporary folder</u>**

  The temporary directory folder is used by AhsayOBM for storing backup set index files and incremental/differential delta files. To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive. The temporary folder should not be located on Windows system partition or the database partition to minimize any potential performance impact on Windows and or database.

- **<u>Temporary folder capacity</u>**

  With VSS-based backup, the disk space of the temporary folder required for storing the VSS image is significantly smaller than using the ODBC spooling backup method. As the extra space is not required to hold the full database.

  It is recommended that the temporary directory should have at least free disk space of 50% of the total database size. The rationale behind this recommended free disk space is the default in-file delta ratio settings is 50%, therefore AhsayOBM could generate incremental or differential delta file(s) of up to 50% of the total database size. The actual free disk space required depends on various factors including the size of the database, number of backup destinations, backup frequency, in-file delta settings etc.

Pros

- **Fast and minimal interruption**
  The database snapshot capture process is fast and can take place on a running server, as you may continue to work when the snapshot capturing is taking place, there may be another process that holds your input in some memory section until the snapshot capture is completed. That said, the whole snapshot capture is fast, so there is no need for you to stop working and it causes minimal interruption to your business operation.

- **Significantly lesser disk burden**
  VSS Snapshot typically requires much less additional disk space than clones which is the traditional backup method by spooling database into the temporary folder. Oftentimes, the capacity of the database to back up is huge and therefore the temporary folder would overload with the equal or even larger disk space if traditional backup method is used. By utilizing the VSS technology, it helps your system greatly reduce disk capacity burden and promote optimized performance.

Cons

- **No Transaction Log Backup**
  MS SQL does not support transaction log backup when VSS is used, therefore, transaction log backup will have to be done manually.

- **Workaround is time consuming**
  In order to truncate the transaction logs, you have to either change the Recovery model to Simple or perform a manual log truncation, which could be time consuming.

Transaction Log Handling

VSS based backup no longer requires backup of the transaction log files, however for databases configured in either full or bulk-logging recovery model, this may eventually result in transaction logs filling up the available disk space on the volume of the MS SQL Server. https://technet.microsoft.com/en-us/library/cc966520.aspx.

To prevent this from occurring, it is recommended to change the recovery model of database selected for backup to simple recovery model.

Refer to the following steps for details:

1. In SQL Server Management Studio, expand **Databases**, select a user database, or expand **System Databases** and select a system database.
2. Right-click the corresponding database, then click **Properties** to open the **Database Properties** dialog box.
3. In the **Select a page** pane, click **Options**.
4. The current recovery model is displayed in the **Recovery model** list box. Modify the recovery model by selecting **Simple** from the model list.

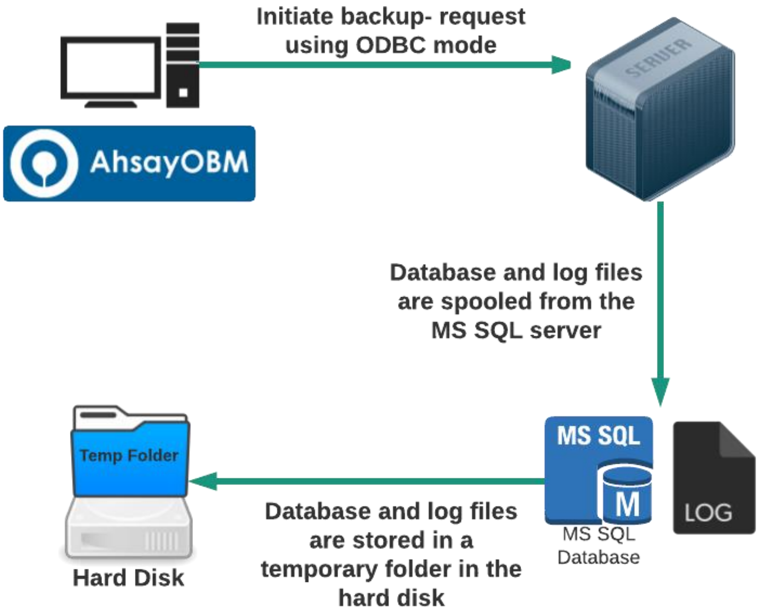
Important: Only modify the recovery model of a live database during low activities hour. It is also recommended to perform a full backup before changing the recovery model.

For MS SQL Server setups where you cannot modify the recovery model of the database, please refer to Appendix B for details on how to truncate transaction log (e.g. perform a transaction log backup manually).

ODBC Mode

Introduction

By using the ODBC mode for MS SQL backup, database files are spooled to a temporary directory before being uploaded to the backup destination.


Initiate backup- request using ODBC mode
AhsayOBM
SERVER
Database and log files are spooled from the MS SQL server
MS SQL
M
MS SQL Database
LOG
Temp Folder
Hard Disk
Database and log files are stored in a temporary folder in the hard disk

Temporary Folder Requirement

- **Location for temporary folder**

  The temporary directory folder is used by AhsayOBM for storing; the database files, incremental/differential delta files, and backup set index files. To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive. The temporary folder should not be located on Windows system partition or the database partition to minimize any potential performance impact on Windows and or database.

- **Temporary folder capacity**

  ODBC backup requires a significantly larger disk space of temporary folder as it need to store the database files spooled during the backup process.

  It is recommended that the temporary directory have disk space of at least 150% of the total database size. For each database backup, AhsayOBM will spool the database files to the temporary directory before they are uploaded to the backup destination. Also, additional space is required for in-file delta generation the default in-file delta ratio settings is 50%, therefore AhsayOBM could generate incremental or differential delta file(s) of up to 50% of the total database size. The actual disk space required depends on various factors, including the size of the database, number of backup destinations, backup frequency, in-file delta settings etc.

Pros

➢ **Support Automated Transaction Logs Backup**
Schedule backup of transaction log can be configured so that the transaction logs can be backed up periodically and the transaction logs are truncated automatically after each backup job.

- **Support Point in Time Recovery**

  The ability to restore to a point in time for all of your transaction log backups.

- **Support Backup of High Transaction Databases**

  For databases which supports a high number of transaction which may require frequent backups. Transaction log backups at regular intervals are more suitable and less resource intensive than VSS based backups, i.e. transaction log backup every 60 minutes, 30 minutes, 15 minutes etc. depending on the database transaction volume.

Cons

- **Large disk space required**
  Since the database files will be spooled to a temporary folder before uploading to backup destination, investment on hard disk could be high if your MS SQL database size is large.

- **Slower backup process**
  By utilizing the conventional spooling method, it could take a long time to back up the database and the speed is subject to various factors, including database size, network transfer speed, backup frequency, etc.

Comparison between VSS Backup Mode and ODBC Backup Mode

Description	VSS Backup Mode	ODBC Backup Mode
Support database backup using VSS snapshot	✓	✗
Requires larger temporary folder capacity for storing spooled databases and log files	✗	✓
Requires spooling / staging of database file(s) for backup	✗	✓
Support Transaction log backup	✗	✓
Support backup of databases located on a network drive	✗	✓

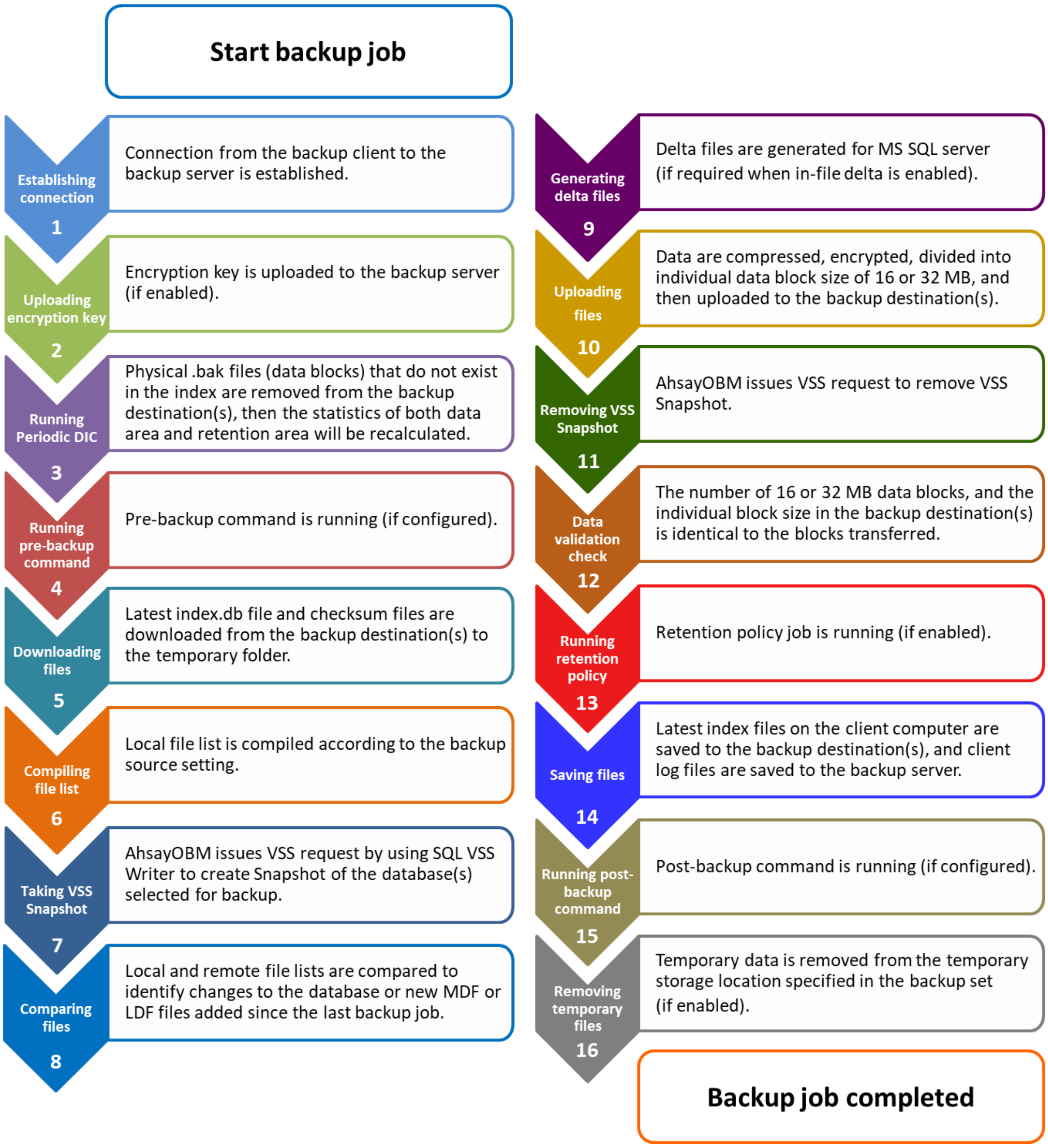
6 Overview on the Backup Process

The following steps are performed during a MS SQL Server backup job in VSS and ODBC Backup Modes.

6.1 VSS Backup Mode

For an overview of the detailed process for Steps **3**, **5**, **12**, and **14**, refer to the following chapters:

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
    - Start Backup Job **(Step 5)**
    - Completed Backup Job **(Step 14)**
- Data Validation Check **(Step 12)**



Start backup job

Establishing connection 1: Connection from the backup client to the backup server is established.

Uploading encryption key 2: Encryption key is uploaded to the backup server (if enabled).

Running Periodic DIC 3: Physical .bak files (data blocks) that do not exist in the index are removed from the backup destination(s), then the statistics of both data area and retention area will be recalculated.

Running pre-backup command 4: Pre-backup command is running (if configured).

Downloading files 5: Latest index.db file and checksum files are downloaded from the backup destination(s) to the temporary folder.

Compiling file list 6: Local file list is compiled according to the backup source setting.

Taking VSS Snapshot 7: AhsayOBM issues VSS request by using SQL VSS Writer to create Snapshot of the database(s) selected for backup.

Comparing files 8: Local and remote file lists are compared to identify changes to the database or new MDF or LDF files added since the last backup job.

Generating delta files 9: Delta files are generated for MS SQL server (if required when in-file delta is enabled).

Uploading files 10: Data are compressed, encrypted, divided into individual data block size of 16 or 32 MB, and then uploaded to the backup destination(s).

Removing VSS Snapshot 11: AhsayOBM issues VSS request to remove VSS Snapshot.

Data validation check 12: The number of 16 or 32 MB data blocks, and the individual block size in the backup destination(s) is identical to the blocks transferred.

Running retention policy 13: Retention policy job is running (if enabled).

Saving files 14: Latest index files on the client computer are saved to the backup destination(s), and client log files are saved to the backup server.

Running post-backup command 15: Post-backup command is running (if configured).

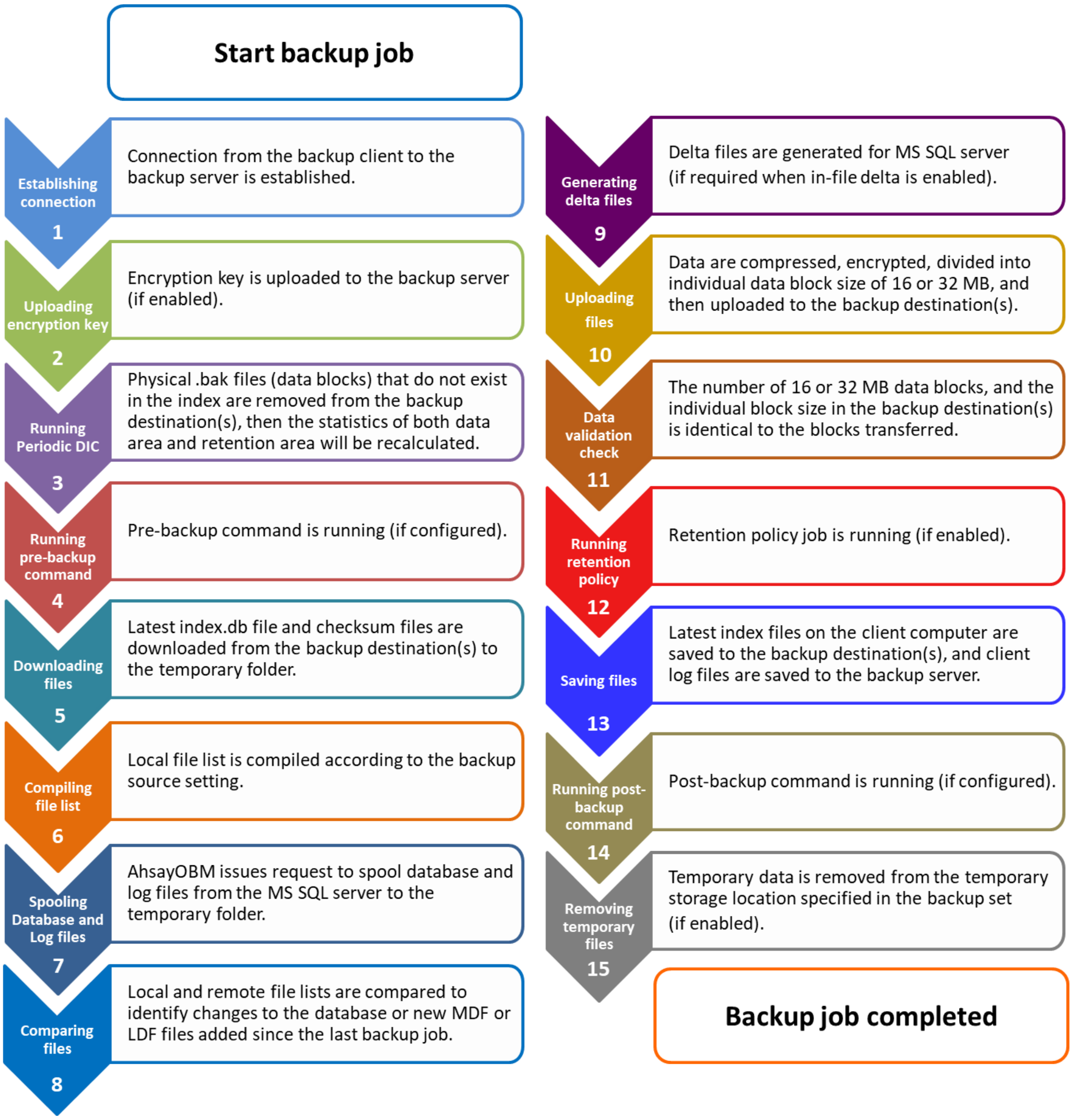
Removing temporary files 16: Temporary data is removed from the temporary storage location specified in the backup set (if enabled).

Backup job completed

6.2 ODBC Backup Mode

For an overview of the detailed process for Steps **3**, **5**, **11**, and **13**, refer to the following chapters:

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 5)**
  - Completed Backup Job **(Step 13)**
- Data Validation Check **(Step 11)**



Start backup job

1 Establishing connection: Connection from the backup client to the backup server is established.

2 Uploading encryption key: Encryption key is uploaded to the backup server (if enabled).

3 Running Periodic DIC: Physical .bak files (data blocks) that do not exist in the index are removed from the backup destination(s), then the statistics of both data area and retention area will be recalculated.

4 Running pre-backup command: Pre-backup command is running (if configured).

5 Downloading files: Latest index.db file and checksum files are downloaded from the backup destination(s) to the temporary folder.

6 Compiling file list: Local file list is compiled according to the backup source setting.

7 Spooling Database and Log files: AhsayOBM issues request to spool database and log files from the MS SQL server to the temporary folder.

8 Comparing files: Local and remote file lists are compared to identify changes to the database or new MDF or LDF files added since the last backup job.

9 Generating delta files: Delta files are generated for MS SQL server (if required when in-file delta is enabled).

10 Uploading files: Data are compressed, encrypted, divided into individual data block size of 16 or 32 MB, and then uploaded to the backup destination(s).

11 Data validation check: The number of 16 or 32 MB data blocks, and the individual block size in the backup destination(s) is identical to the blocks transferred.

12 Running retention policy: Retention policy job is running (if enabled).

13 Saving files: Latest index files on the client computer are saved to the backup destination(s), and client log files are saved to the backup server.

14 Running post-backup command: Post-backup command is running (if configured).

15 Removing temporary files: Temporary data is removed from the temporary storage location specified in the backup set (if enabled).

Backup job completed

6.3 Periodic Data Integrity Check (PDIC) Process

For AhsayOBM v8.3.6.0 (or above), the PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

To minimize the impact of the potential load of large number of PDIC jobs running at the same time on the AhsayCBS server, the schedule of a PDIC job for each backup set is automatically determined by the result of the following formula:

> ***PDIC schedule*** = ***%BackupSetID% modulo 5***
>
> or
>
> ***%BackupSetID% mod 5***

The calculated **result** will map to the corresponding day of the week (i.e., from Monday to Friday).

0	**Monday**
1	**Tuesday**
2	**Wednesday**
3	**Thursday**
4	**Friday**

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation*:* 1594627447932 *mod 5* = ***2***

2	**Wednesday**

In this example:

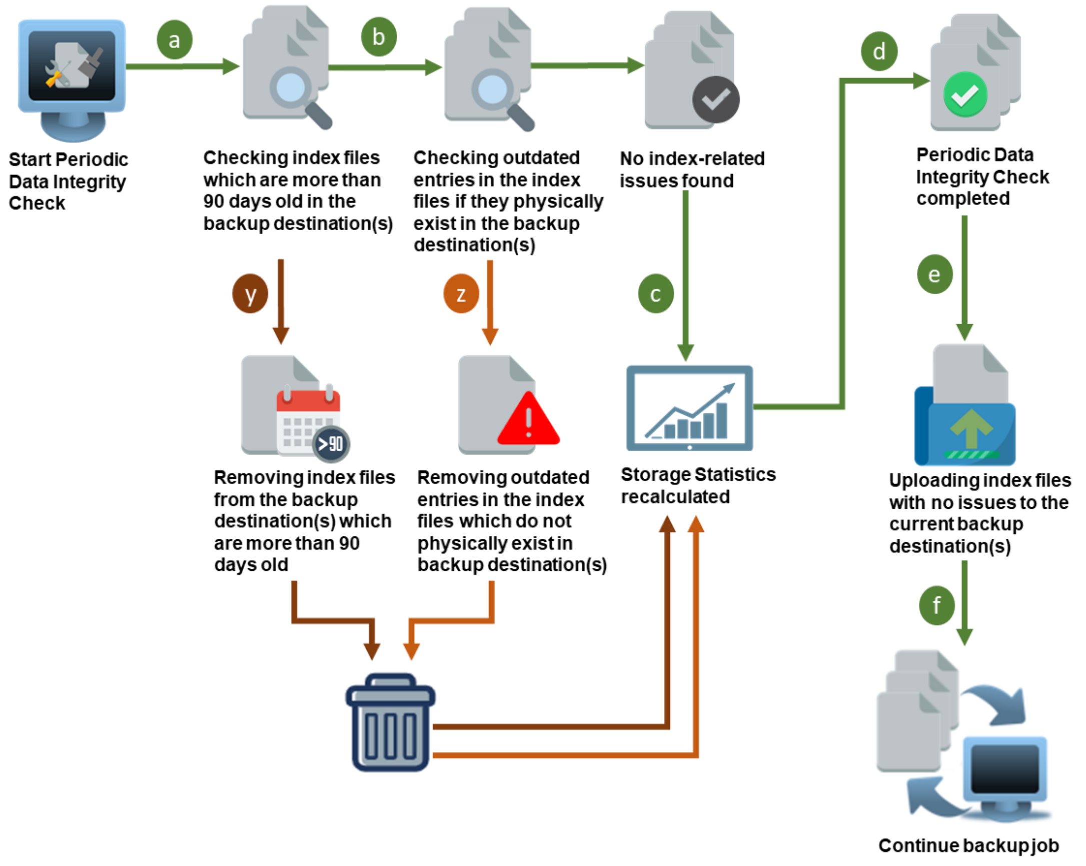
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

Although according to the PDIC formula for determining the schedule is ***%BackupSetID% mod 5***, this schedule only applies if the previous PDIC job was actually run more than 7 days prior.

Under certain conditions, the PDIC may not run strictly according to this formula. For example:

1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.


a
b
d
Start Periodic Data Integrity Check
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
No index-related issues found
Periodic Data Integrity Check completed
y
z
c
e
>90
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Storage Statistics recalculated
Uploading index files with no issues to the current backup destination(s)
f
Continue backup job

a Check the index files in the backup destination(s) to determine if they were more than 90 days old.

➔ If **YES**, proceed to y

➔ If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).

➔ If **YES**, proceed to c

➔ If **NO**, proceed to z

c Storage Statistics for Data area and Retention area usage will be recalculated.

d Periodic Data Integrity check is completed.

e Index files with no issues will be uploaded to the current backup destination(s).

f The backup job process will continue.

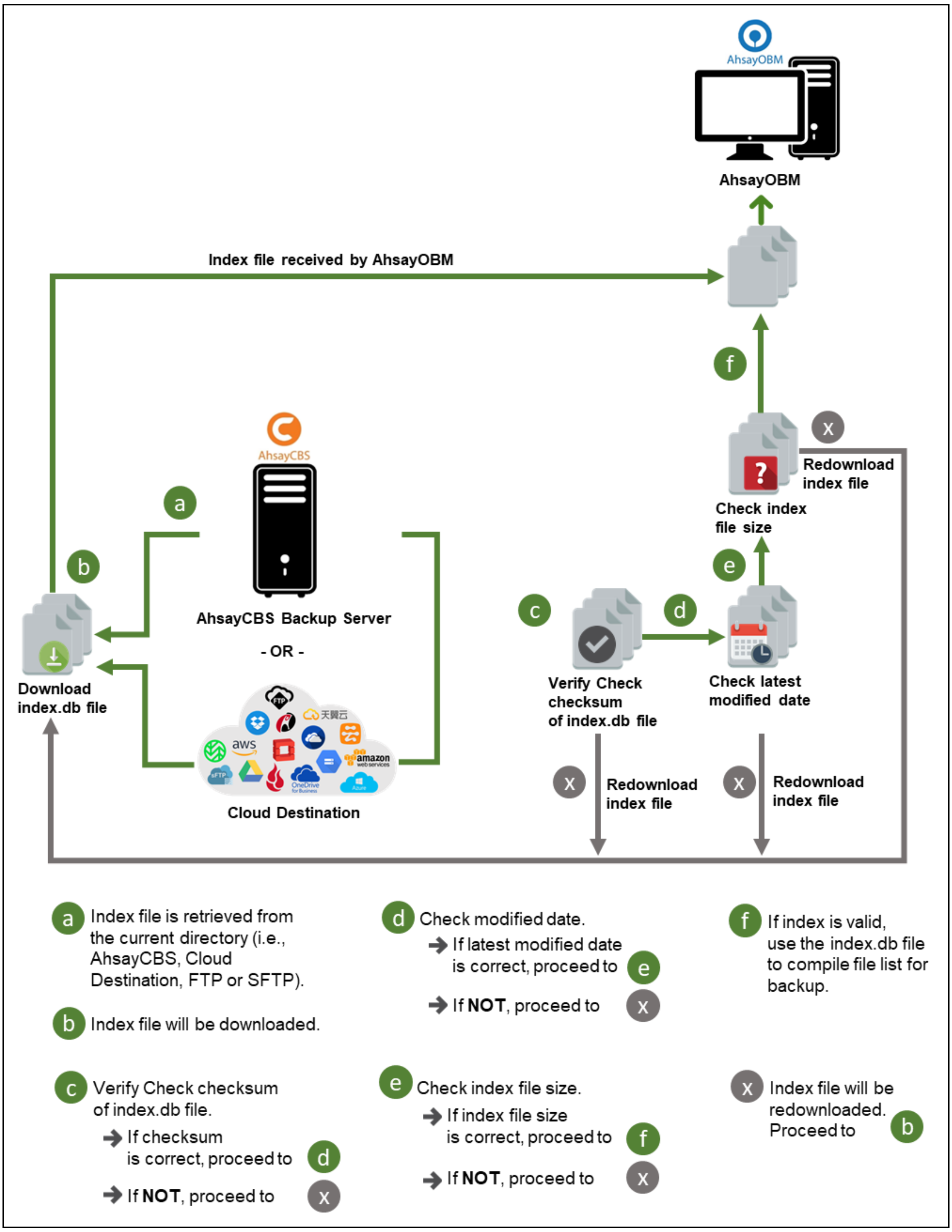
y Index files which are more than 90 days old will be removed from the backup destination(s).

z Outdated entries in the index files for files and/or folders which do not physically exist in backup destination(s) will be removed.

6.4 Backup Set Index Handling Process

To minimize the possibility of index related issues affecting backups, each time index files are downloaded from and uploaded to backup destination(s); the file size, last modified date, and checksum is verified to ensure index file integrity.

6.4.1 Start Backup Job



a Index file is retrieved from the current directory (i.e., AhsayCBS, Cloud Destination, FTP or SFTP).

b Index file will be downloaded.

c Verify Check checksum of index.db file.
→ If checksum is correct, proceed to d
→ If **NOT**, proceed to x

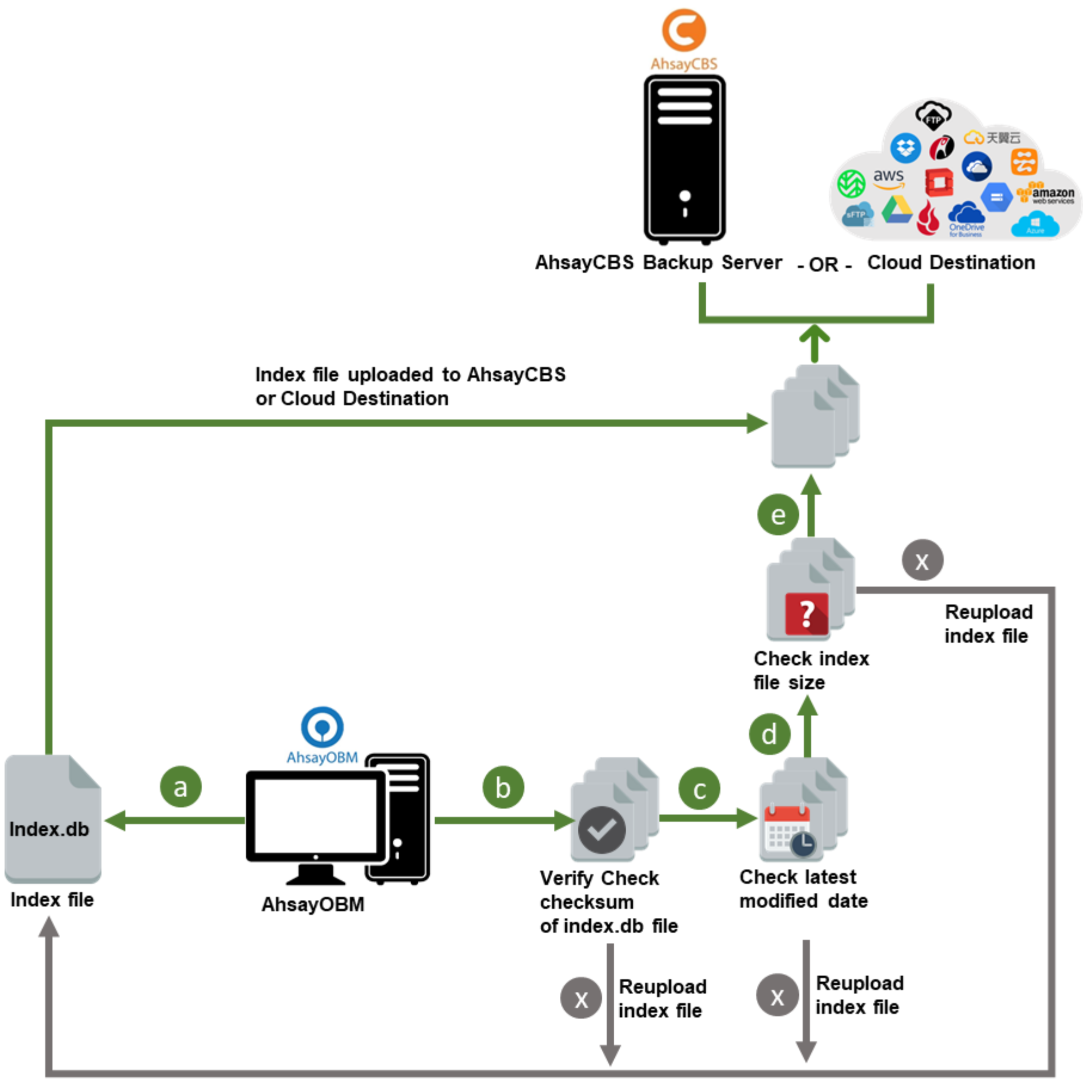
d Check modified date.
→ If latest modified date is correct, proceed to e
→ If **NOT**, proceed to x

e Check index file size.
→ If index file size is correct, proceed to f
→ If **NOT**, proceed to x

f If index is valid, use the index.db file to compile file list for backup.

x Index file will be redownloaded. Proceed to b

6.4.2 Completed Backup Job



a Index file from AhsayOBM is uploaded to AhsayCBS, Cloud Destination, FTP or SFTP.

b Verify Check checksum of index.db file.

- ➔ If checksum is correct, proceed to c
- ➔ If **NOT**, proceed to x

c Check modified date.

- ➔ If latest modified date is correct, proceed to d
- ➔ If **NOT**, proceed to x

d Check index file size.

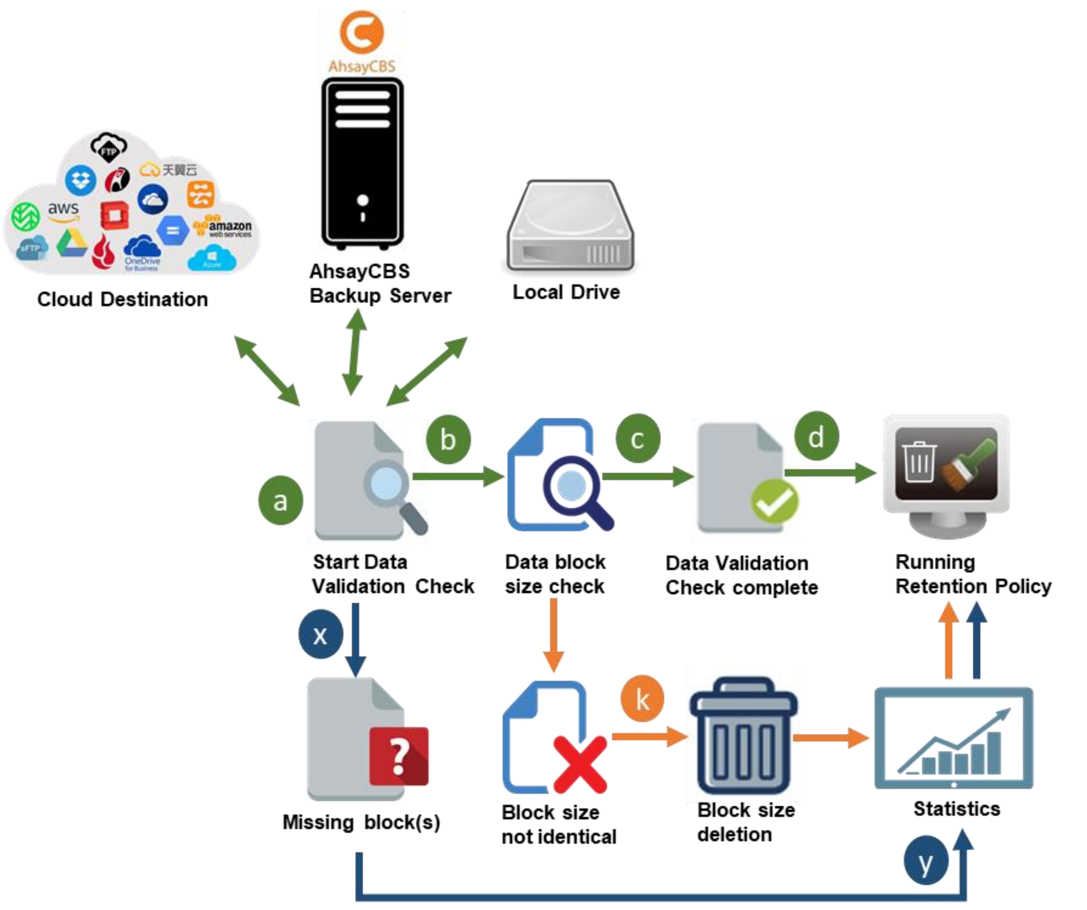
- ➔ If index file size is correct, proceed to e
- ➔ If **NOT**, proceed to x

e Index file is uploaded correctly to AhsayCBS or Cloud Destination.

x Index file will be reuploaded. Proceed to a

6.5 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.



a Check the number of 16 or 32 MB data blocks in the backup destination(s) is identical to the number of blocks transferred.

→ If YES, proceed to b

→ If NO, proceed to x

b Check the individual sizes of each data block in the backup destination(s) is identical to the sizes of each block transferred.

→ If YES, proceed to c

→ If NO, proceed to k

c Data validation check is complete.

d Retention policy will run (if enabled).

x Files in the missing block(s) will be removed from the index.db file.

y Statistics will be updated according to the files removed.

Proceed to d

k Block size that are not identical will be removed from the backup destination(s).

Proceed to y then

Proceed to d

7 Logging in to AhsayOBM

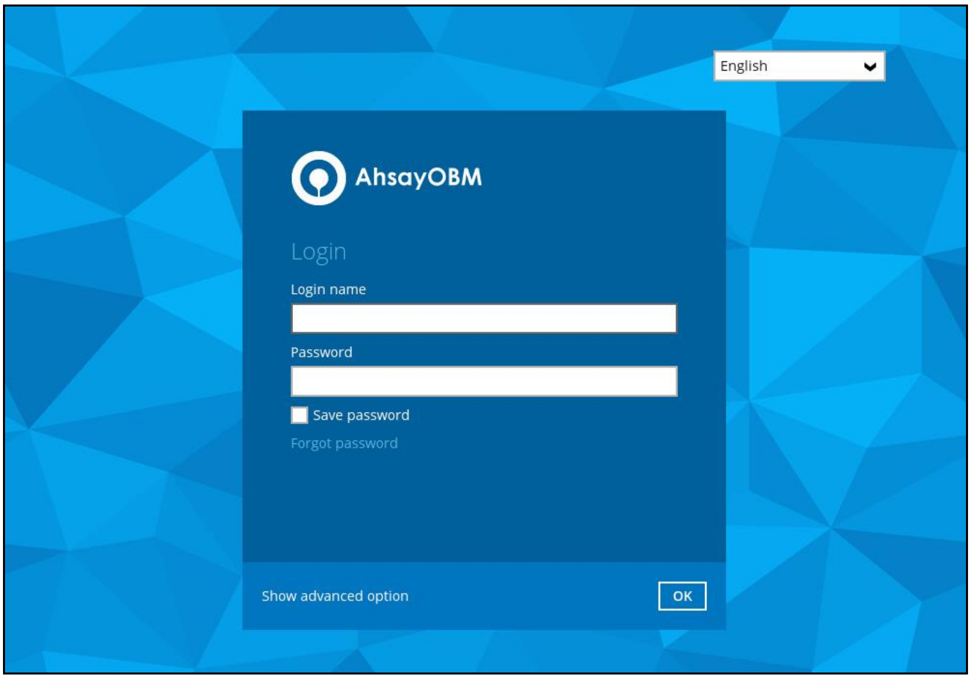
Starting with AhsayOBM v8.5.0.0 there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

- Login without 2FA
- Login with 2FA using authenticator app
- Login with 2FA using Twilio

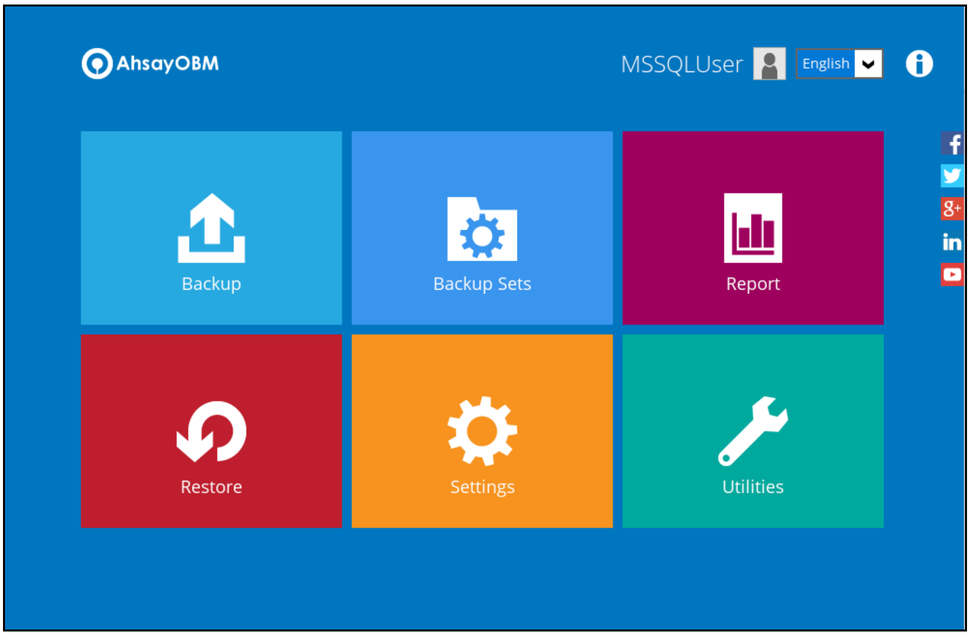
7.1 Login to AhsayOBM without 2FA

1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account provided by your backup service provider, then click **OK** to login.



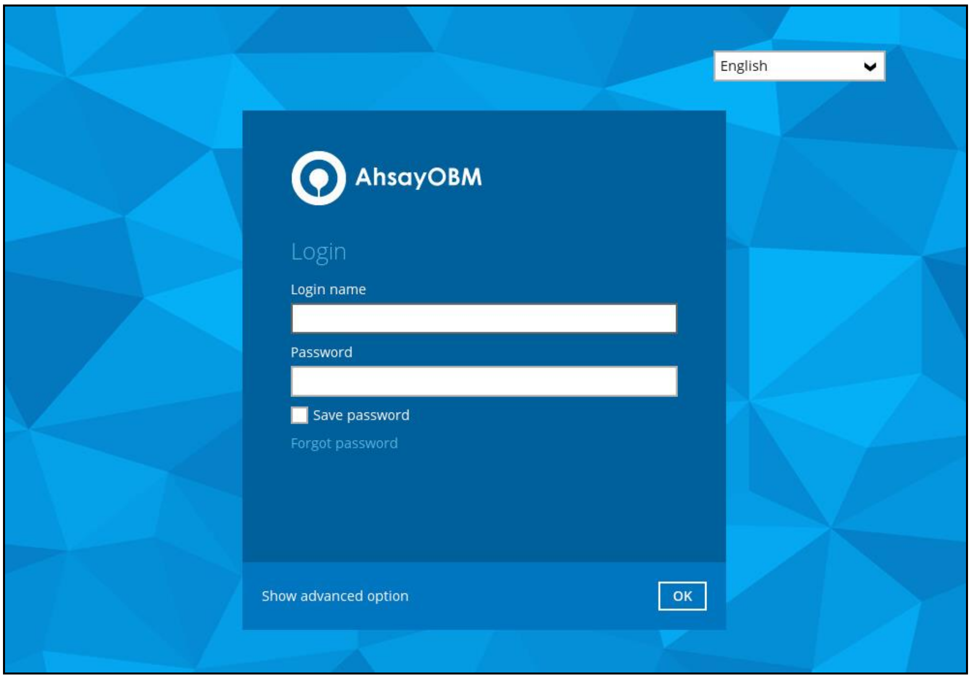
3. After successful login, the following screen will appear.



7.2 Login to AhsayOBM with 2FA using authenticator app

1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account provided by your backup service provider, then click **OK** to login.

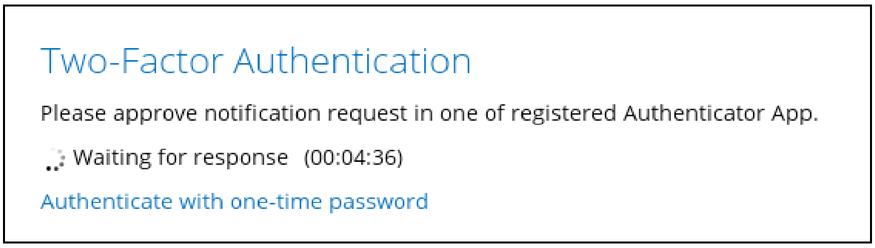


3. One of the two authentication methods will be displayed to continue with the login:

- [Push Notification and TOTP when using Ahsay Mobile app]
- [TOTP only]

- If **Ahsay Mobile app** was configured to use Push Notification and TOTP then there are two 2FA modes that can be used:
  - Push Notification (default)

    Push notification is the default 2FA mode. Accept the login request on Ahsay Mobile to complete the login.



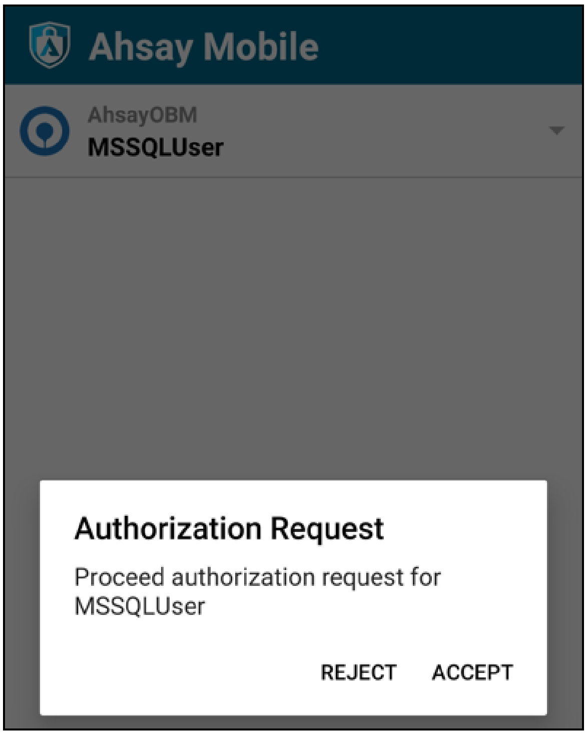
Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

Waiting for response (00:04:36)

Authenticate with one-time password

Example of the login request sent to the Ahsay Mobile app.



Ahsay Mobile

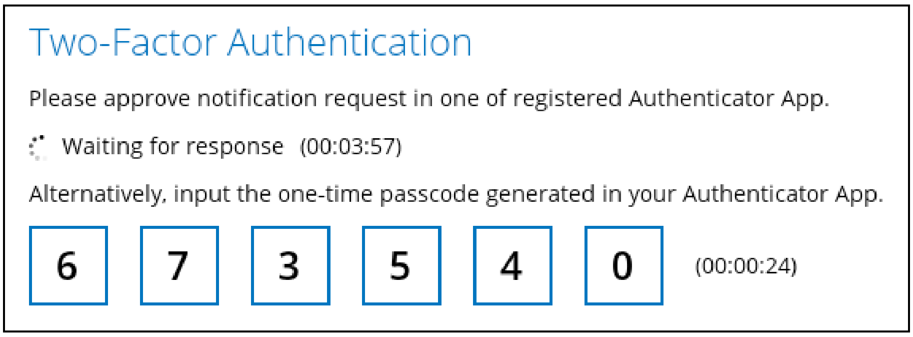
AhsayOBM
MSSQLUser

Authorization Request

Proceed authorization request for MSSQLUser

- TOTP

However, if push notification is not working or you prefer to use one-time passcode, click the Authenticate with one-time password link, then input the one-time passcode generated by Ahsay Mobile to complete the login.



Two-Factor Authentication

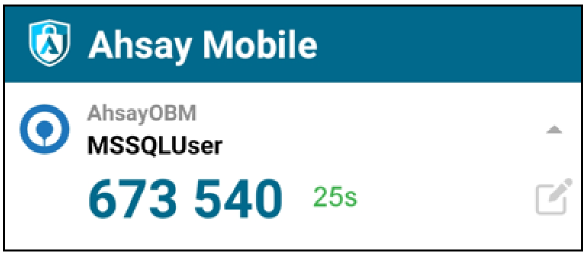
Please approve notification request in one of registered Authenticator App.

Waiting for response (00:03:57)

Alternatively, input the one-time passcode generated in your Authenticator App.

6 7 3 5 4 0 (00:00:24)

Example of the one-time passcode generated in Ahsay Mobile.

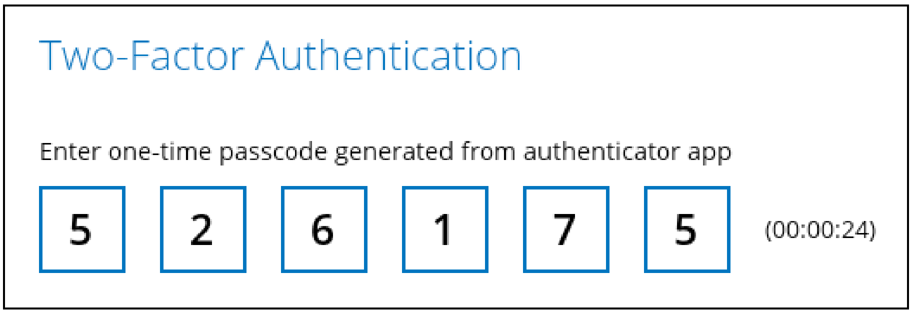


Ahsay Mobile

AhsayOBM
MSSQLUser
673 540 25s

◉ TOTP only

Enter the one-time passcode generated by the authenticator app to complete the login.

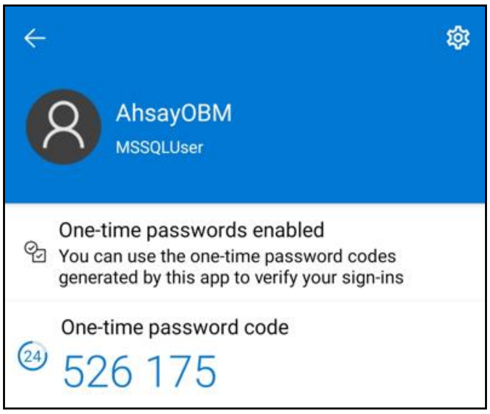


Two-Factor Authentication

Enter one-time passcode generated from authenticator app

5 2 6 1 7 5 (00:00:24)

Example of the one-time passcode generated in the third party authenticator app Microsoft Authenticator.

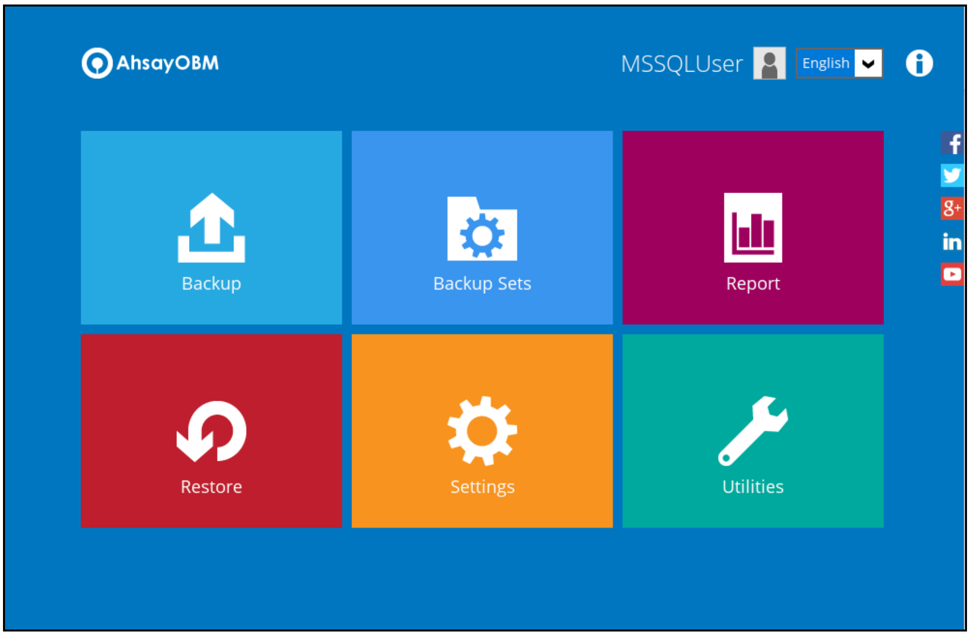


AhsayOBM
MSSQLUser

One-time passwords enabled
You can use the one-time password codes generated by this app to verify your sign-ins

One-time password code
24
526 175

4. After successful login, the following screen will appear.



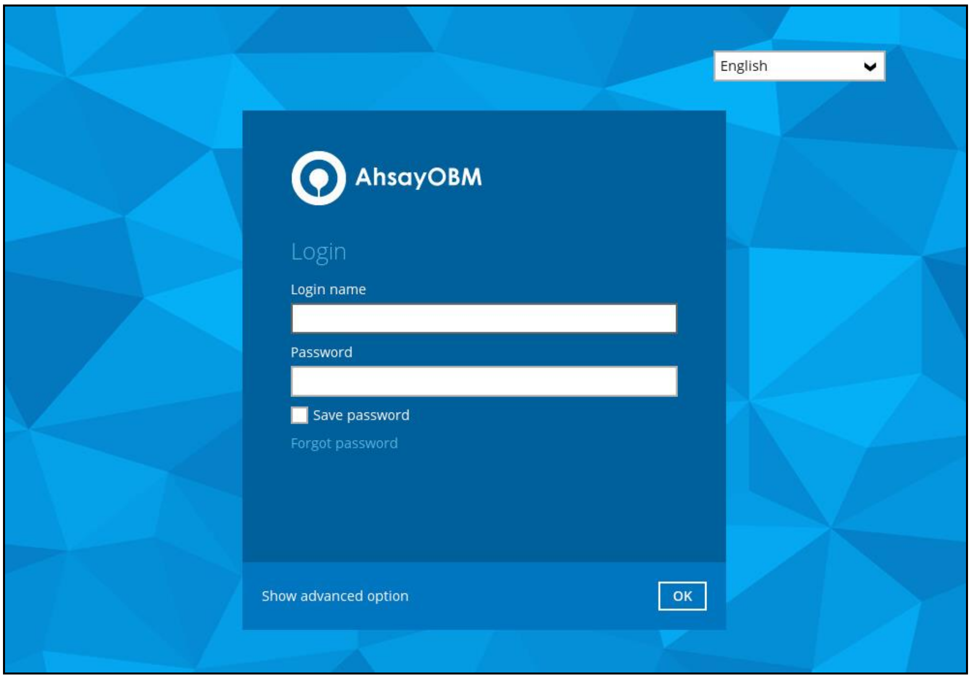
NOTE

If you have trouble logging in using the authenticator app please refer to Chapter 9 of the AhsayOBM Quick Start Guide for Windows for more information.

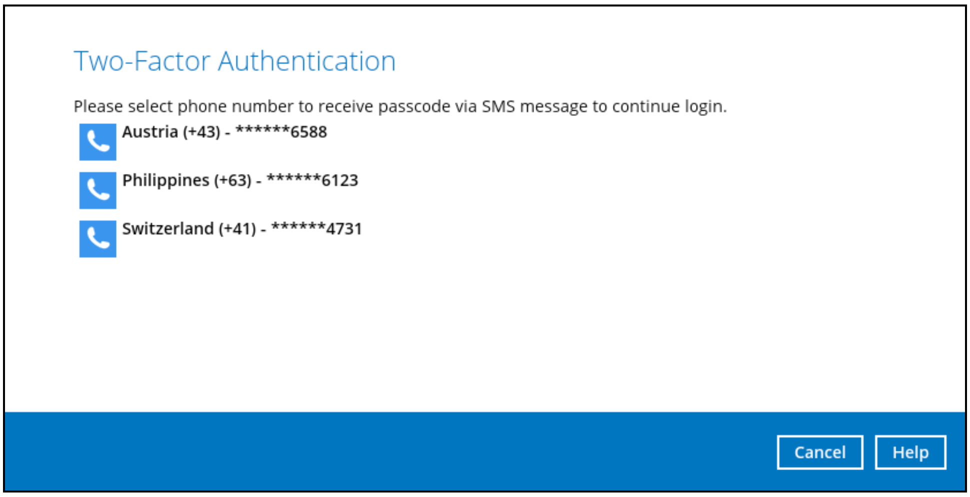
7.3 Login to AhsayOBM with 2FA using Twilio

1. A shortcut icon of AhsayOBM should have been created on your Windows desktop after installation. Double click the icon to launch the application.

2. Enter the **Login name** and **Password** of your AhsayOBM account provided by your backup service provider, then click **OK** to login.



3. Select your phone number.



Two-Factor Authentication

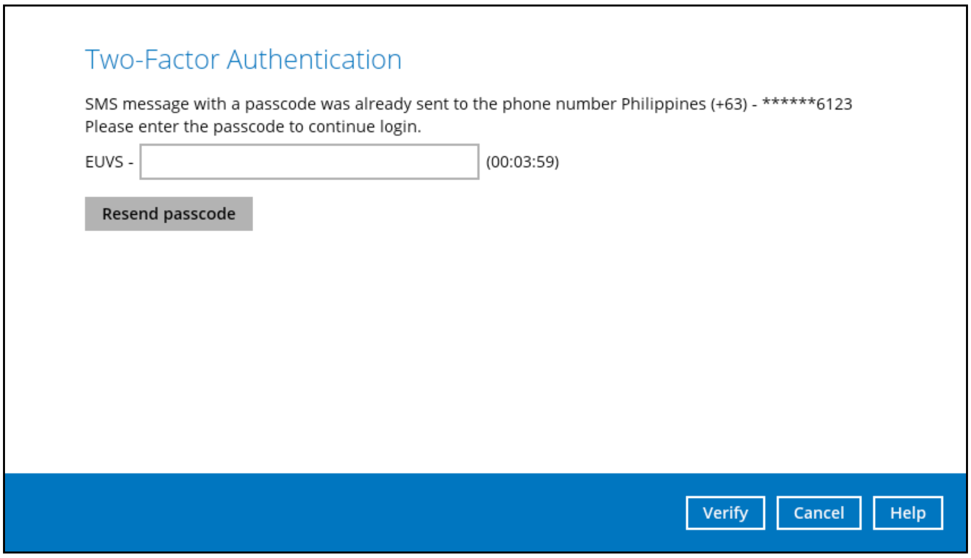
Please select phone number to receive passcode via SMS message to continue login.

☎ Austria (+43) - ******6588

☎ Philippines (+63) - ******6123

☎ Switzerland (+41) - ******4731

4. Enter the passcode and click **Verify** to login.

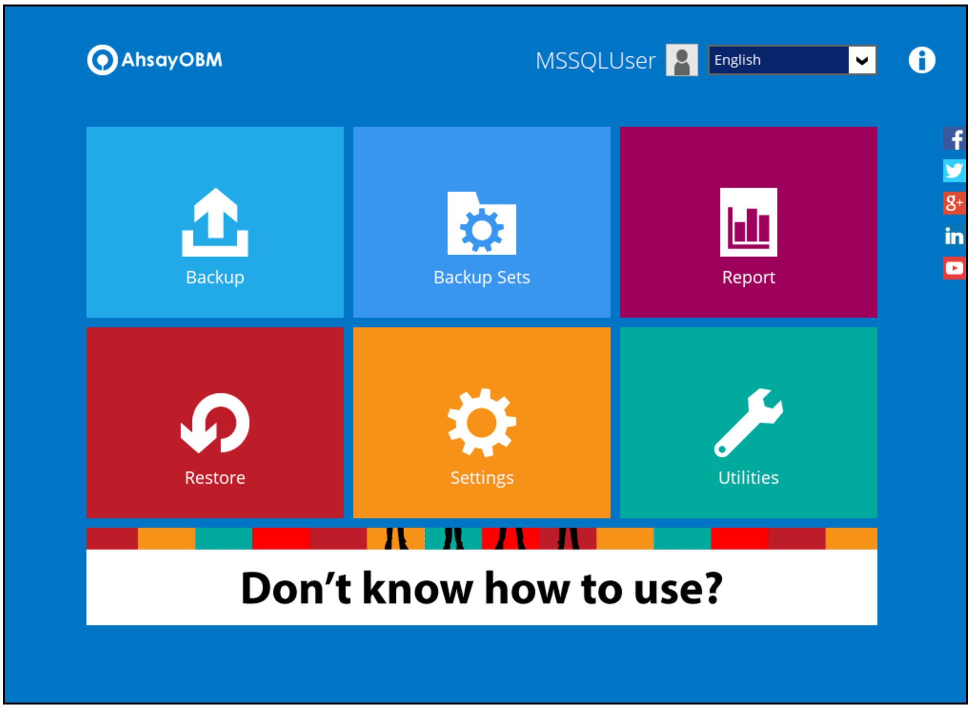


Two-Factor Authentication

SMS message with a passcode was already sent to the phone number Philippines (+63) - ******6123
Please enter the passcode to continue login.

EUVS - (00:03:59)

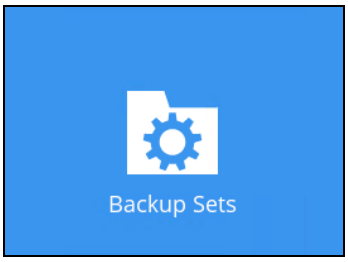
5. After successful login, the following screen will appear.



8 Performing Backup for Microsoft SQL Server

8.1 Creating Backup Set for Microsoft SQL Server

1. Click the **Backup Sets** icon on the main interface of AhsayOBM.

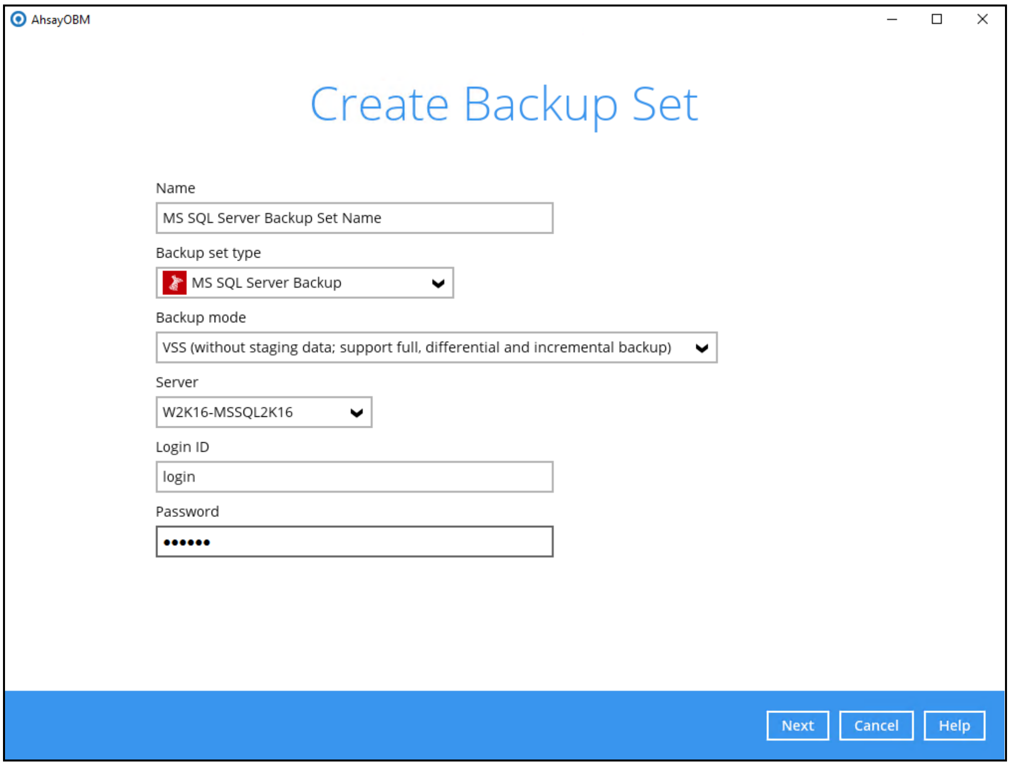


2. Create a new backup set by clicking the "**+**" icon next to **Add new backup set**.

3. Select the Backup set type as **MS SQL Server Backup**.

   - **Name –** enter a meaningful backup set name
   - **Backup mode –** choose between VSS mode and ODBC mode. Refer to the Backup Mode section for details on the differences between the two modes.
   - **Server -** AhsayOBM supports backup of multiple SQL instance in one backup set. In this Server drop-down menu, you can choose to back up multiple SQL instances or a specific instance of your choice.
   - **Login -** Enter the login ID for the chosen instance.
   - **Password –** Enter the password for the chosen instance.

Click **Next** to proceed when you are done with the settings.



Create Backup Set

Name
MS SQL Server Backup Set Name

Backup set type
MS SQL Server Backup

Backup mode
VSS (without staging data; support full, differential and incremental backup)

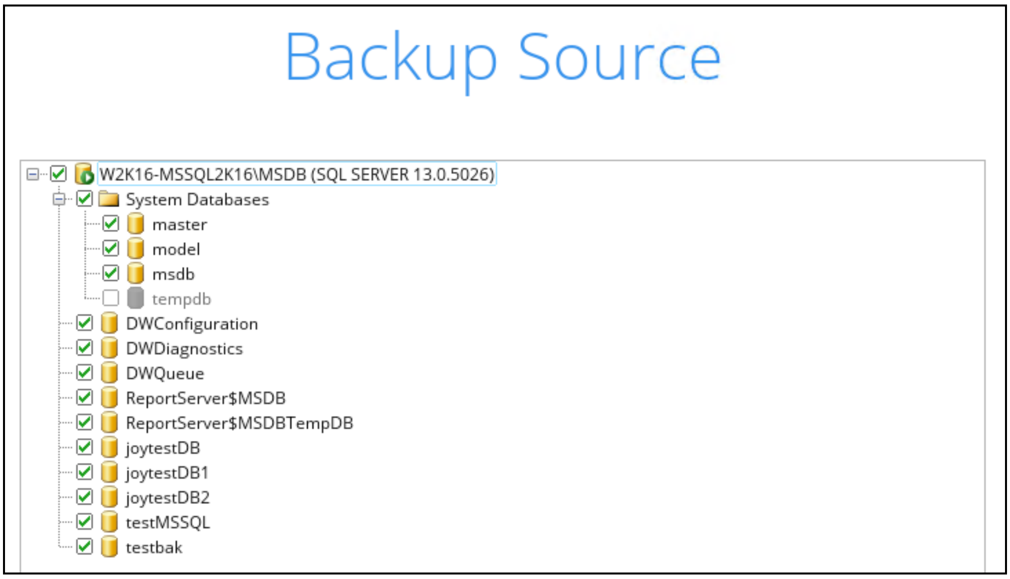
Server
W2K16-MSSQL2K16

Login ID
login

Password
••••••

4. In the **Backup Source** menu, select the database you would like to back up, then click **Next** to proceed.

If you have chosen to back up multiple SQL instances in the previous step, databases in all the chosen instances will be shown here.



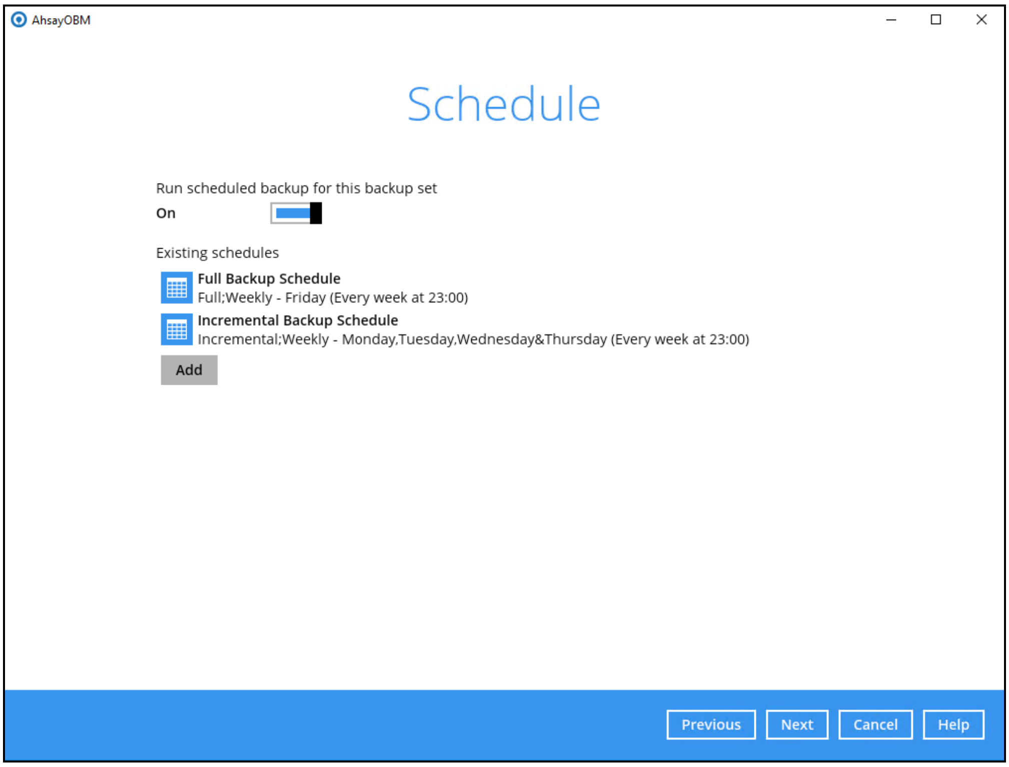
Backup Source

- ☑ W2K16-MSSQL2K16\MSDB (SQL SERVER 13.0.5026)
  - ☑ System Databases
    - ☑ master
    - ☑ model
    - ☑ msdb
    - □ tempdb
  - ☑ DWConfiguration
  - ☑ DWDiagnostics
  - ☑ DWQueue
  - ☑ ReportServer$MSDB
  - ☑ ReportServer$MSDBTempDB
  - ☑ joytestDB
  - ☑ joytestDB1
  - ☑ joytestDB2
  - ☑ testMSSQL
  - ☑ testbak

5. In the Schedule menu, you can configure a backup schedule for backup job to run automatically at your specified time interval. Click **Add** to add a new schedule, then click **Next** to proceed when you are done with the settings.

	VSS Mode	**ODBC Mode**
Name	Name of the Backup Schedule	
Backup set type	➢ Full ➢ Differential ➢ Incremental	➢ Full ➢ Differential ➢ Transaction Log
	Refer to Appendix A for details on the differences of the backup set type.	
Type	Choose frequency for this backup schedule to occur	
Start backup at	Choose a time for this backup schedule to start	
Run Retention Policy after backup	Check this box if you wish to enable the Retention Policy setting	
Default setting	➢ **Full Backup Schedule** Full Backup / Every Friday at 23:00 ➢ **Incremental Backup Schedule** Incremental Backup Type	➢ **Full Backup Schedule** Full Backup / Every Friday at 23:00 ➢ **Transaction Log Backup Schedule** Transaction Log Backup

	/ Mon-Thu every week at 23:00	Type / Mon-Thu every week at 23:00



Run scheduled backup for this backup set

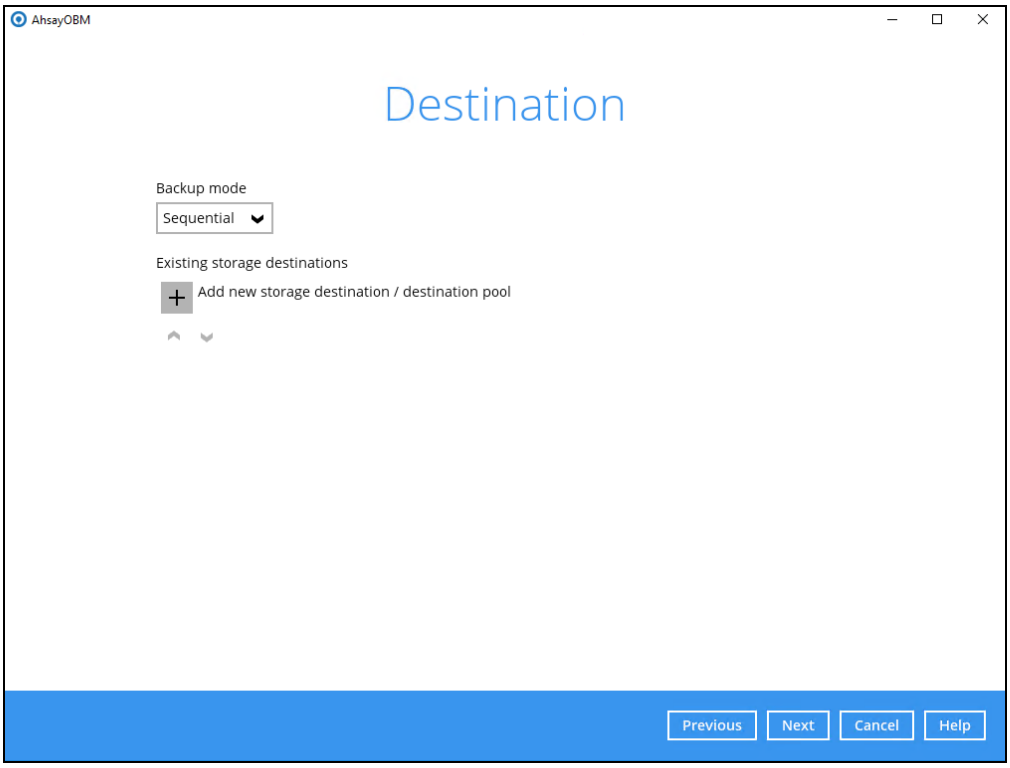
On

Existing schedules

Full Backup Schedule
Full;Weekly - Friday (Every week at 23:00)

Incremental Backup Schedule
Incremental;Weekly - Monday,Tuesday,Wednesday&Thursday (Every week at 23:00)

6. In the Destination menu, select a backup destination where the backup database will be stored. Click the “**+**” icon next to **Add new storage destination / destination pool**.



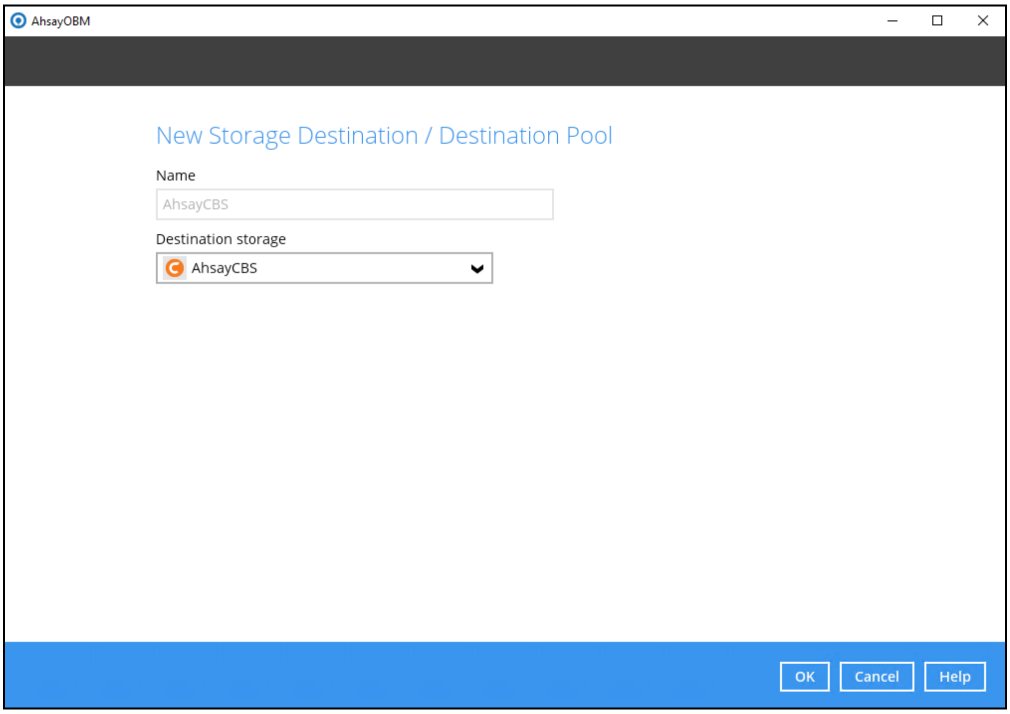
Backup mode

Sequential

Existing storage destinations

Add new storage destination / destination pool

7. Select the destination storage, then click **OK** to proceed.



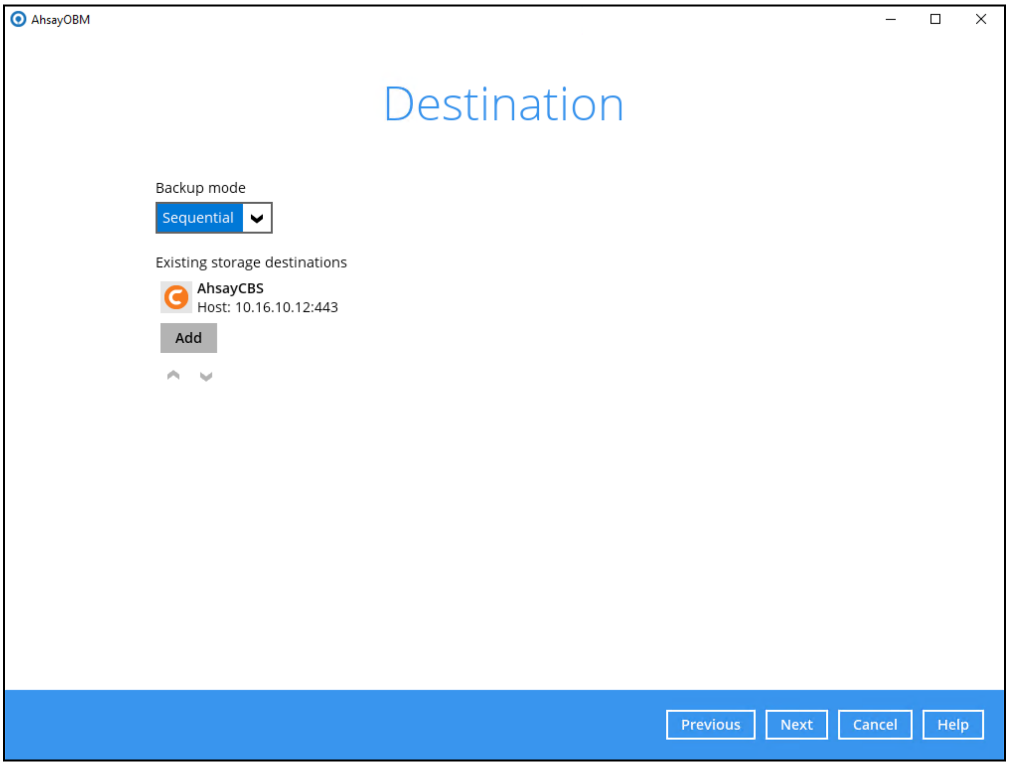
New Storage Destination / Destination Pool

Name: AhsayCBS

Destination storage: AhsayCBS

For more information regarding backing up to cloud storage destination, refer to Appendix C Cloud Storage as Backup Destination.

8. Click **Next** on the Destination menu page to proceed.



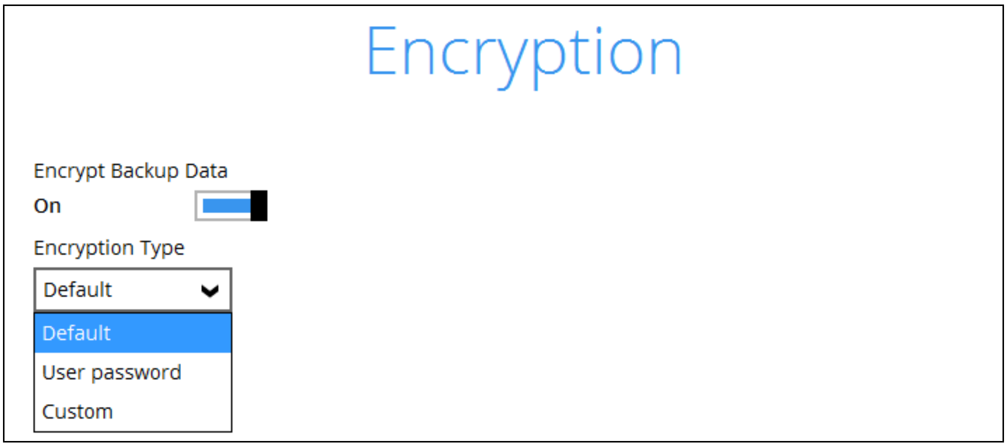
Destination

Backup mode: Sequential

Existing storage destinations

AhsayCBS
Host: 10.16.10.12:443

9. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



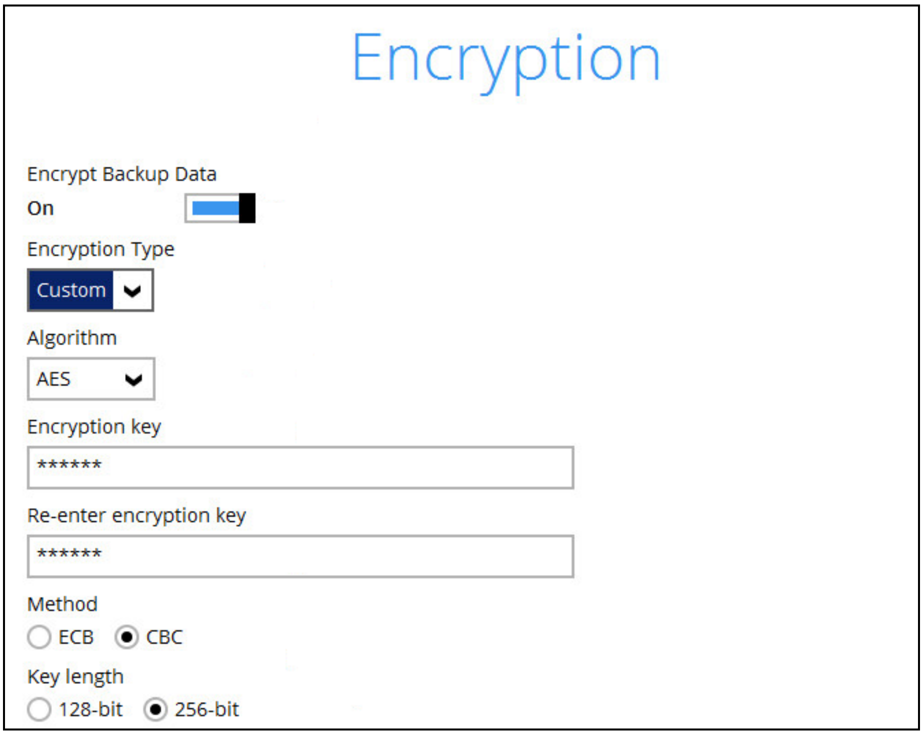
Encryption

Encrypt Backup Data
On

Encryption Type
Default

You can choose from one of the following three Encryption Type options:

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.



Encryption

Encrypt Backup Data
On

Encryption Type
Custom

Algorithm
AES

Encryption key
******

Re-enter encryption key
******

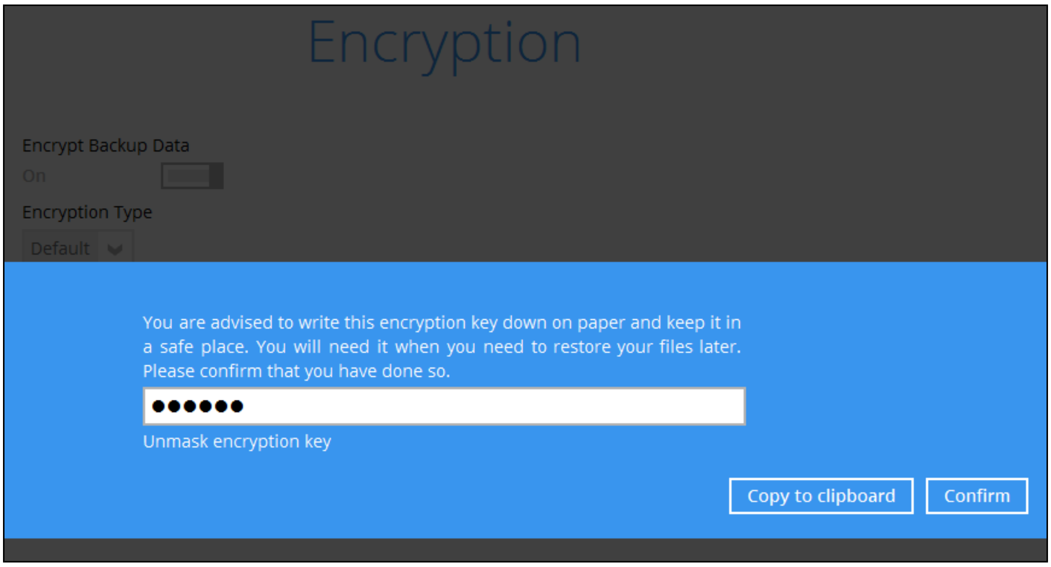
Method
○ ECB ● CBC

Key length
○ 128-bit ● 256-bit

NOTE: *For best practice on managing your encryption key, refer to the following KB article.*
http://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key

Click **Next** when you are done setting.

10. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption key you have selected.

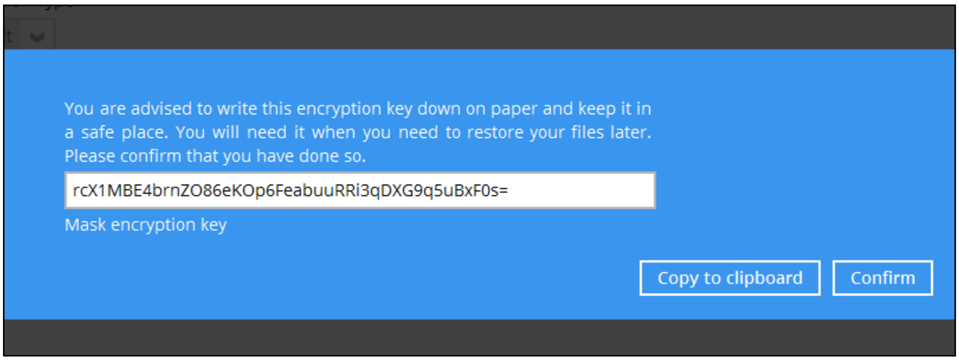


You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

●●●●●●

The pop-up window has the following three options to choose from:

- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

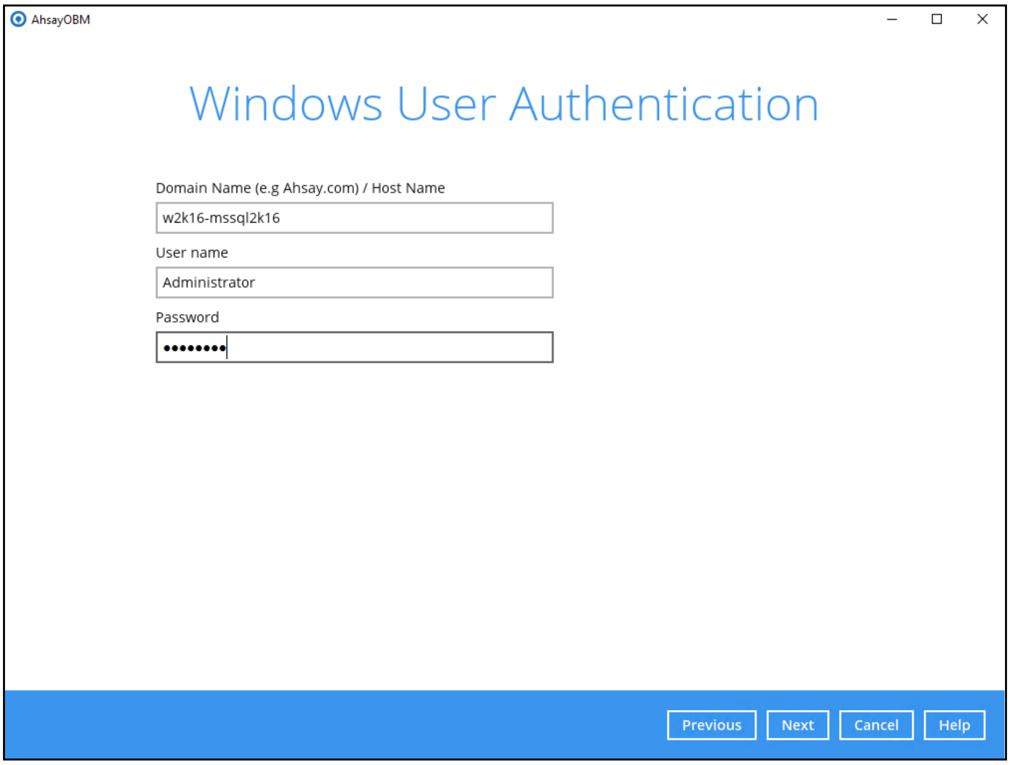
rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

- **Confirm** – Click to exit this pop-up window and proceed to the next step.

11. Enter the Windows login credentials for user authentication. Click **Next** to proceed.

NOTE: *This screen shows only if you have configured scheduled backup.*



Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name

w2k16-mssql2k16

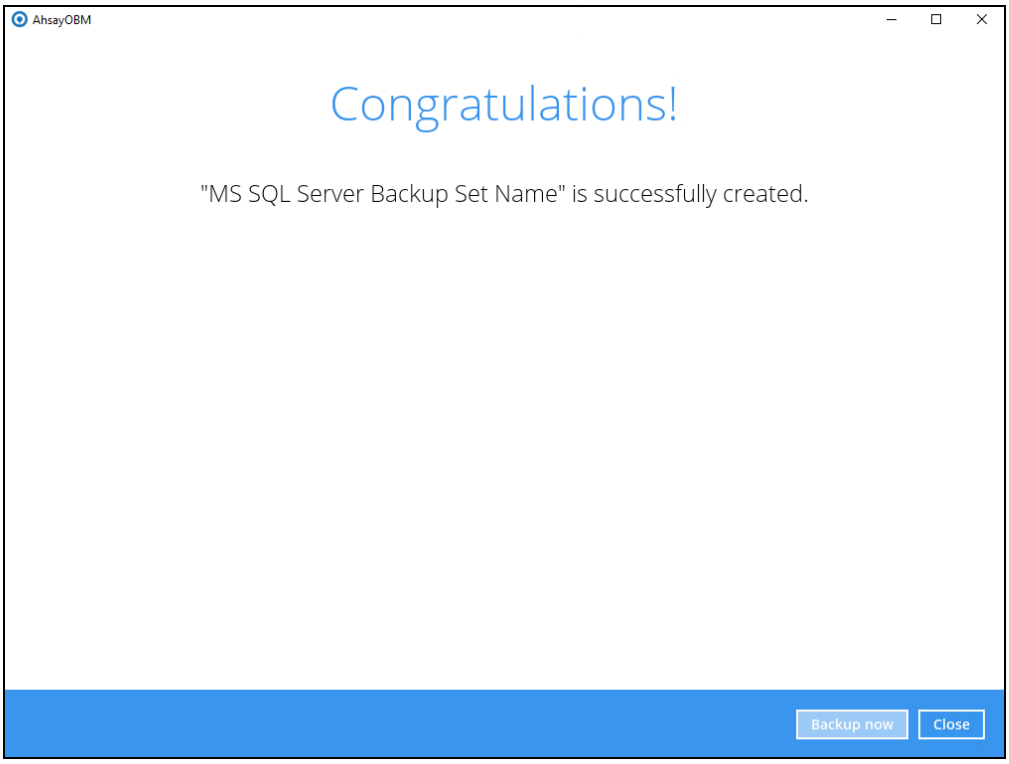
User name

Administrator

Password

••••••••

12. The following screen shows when the new backup set is created successfully.

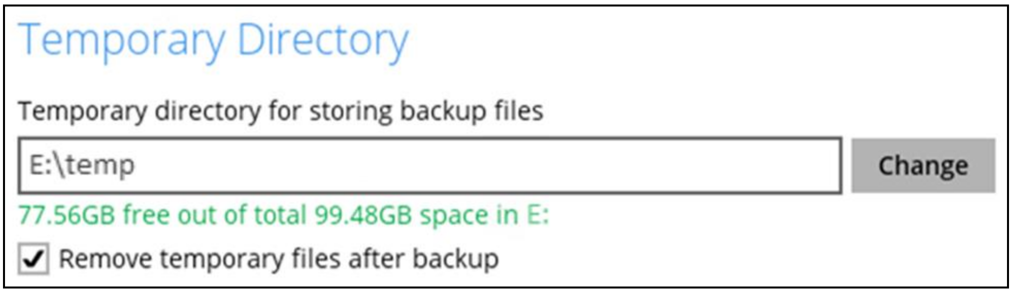


Congratulations!

"MS SQL Server Backup Set Name" is successfully created.

13. Click **Backup now** to start a backup immediately, or you can run a backup job later by following the instructions in Running Backup Job for Microsoft SQL Server.

14. Based on the Best Practices and Recommendations, it is highly recommended to set the **temporary directory** to another location other than Drive C: (e.g. Drive E:). To do this, go to **Backup Sets > Others > Temporary Directory** and click the **Change** button to browse for another location.



Temporary Directory

Temporary directory for storing backup files

E:\temp

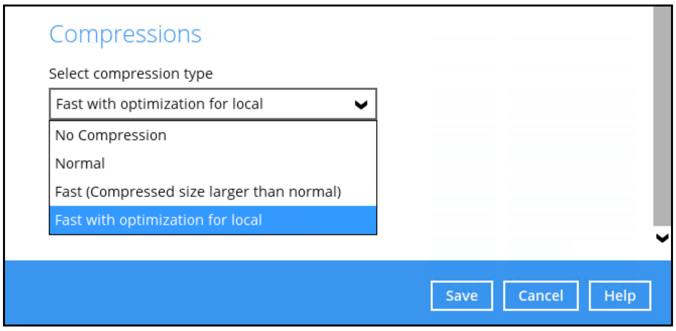
77.56GB free out of total 99.48GB space in E:

☑ Remove temporary files after backup

15. Optional: Select your preferred **Compression** type. By default, the compression type is Fast with optimization for local.

Go to **Others > Compressions**, then select from the following:

- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local



Compressions

Select compression type

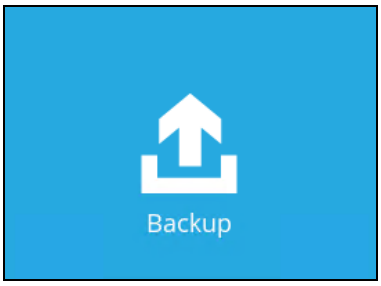
Fast with optimization for local

No Compression
Normal
Fast (Compressed size larger than normal)
Fast with optimization for local
Save
Cancel
Help

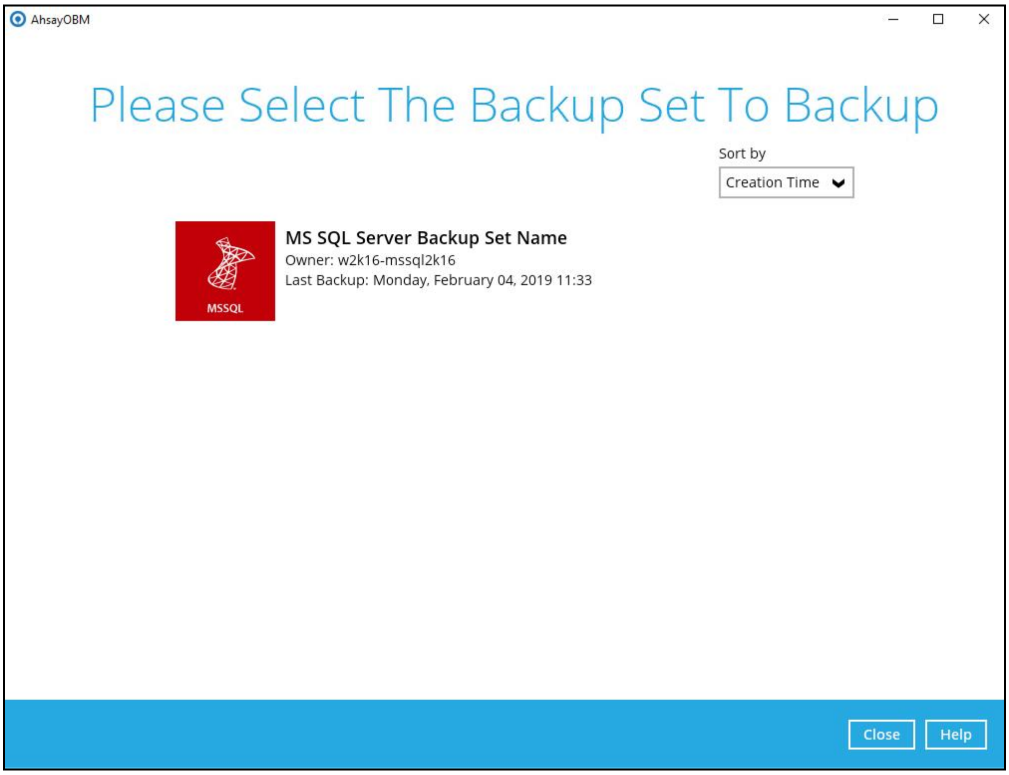
8.2 Running Backup Job for Microsoft SQL Server

1. Log in to AhsayOBM.

2. Click the Backup icon on the main interface of AhsayOBM.



3. Select the backup set which you would like to start a backup for.



AhsayOBM

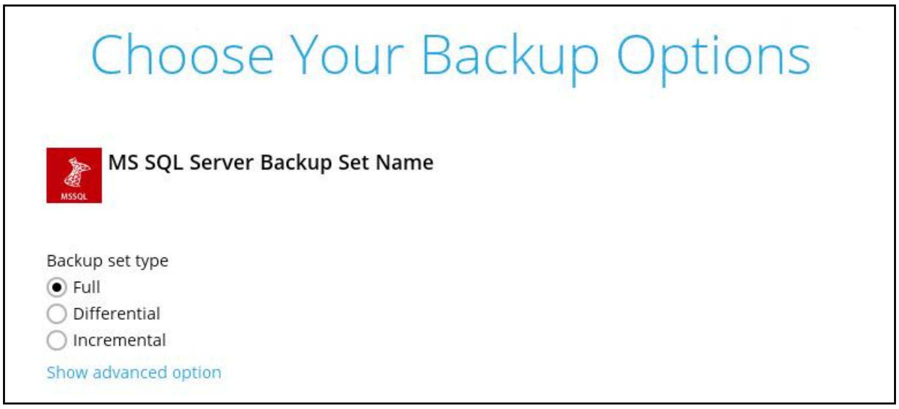
Please Select The Backup Set To Backup

Sort by: Creation Time

MS SQL Server Backup Set Name
Owner: w2k16-mssql2k16
Last Backup: Monday, February 04, 2019 11:33

4. Select the Backup set type. For more details regarding the Backup set type & In-file delta type, refer to Appendix A Backup Set Type .

For VSS Backup Mode

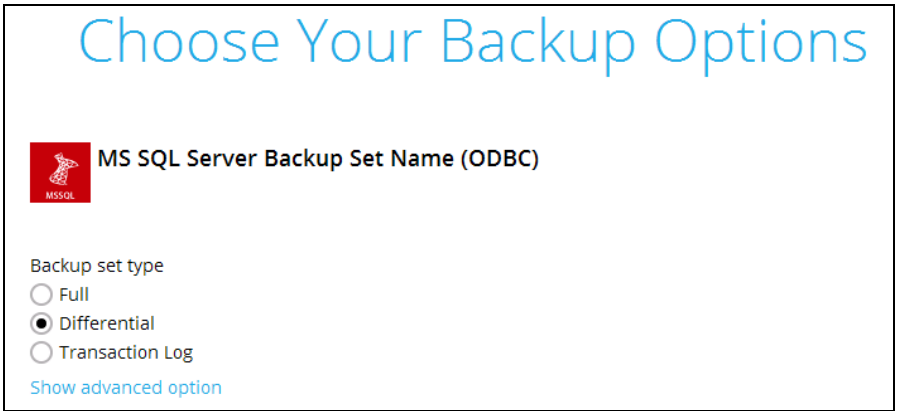


Choose Your Backup Options

MS SQL Server Backup Set Name

Backup set type
● Full
○ Differential
○ Incremental

For ODBC Backup Mode



Choose Your Backup Options

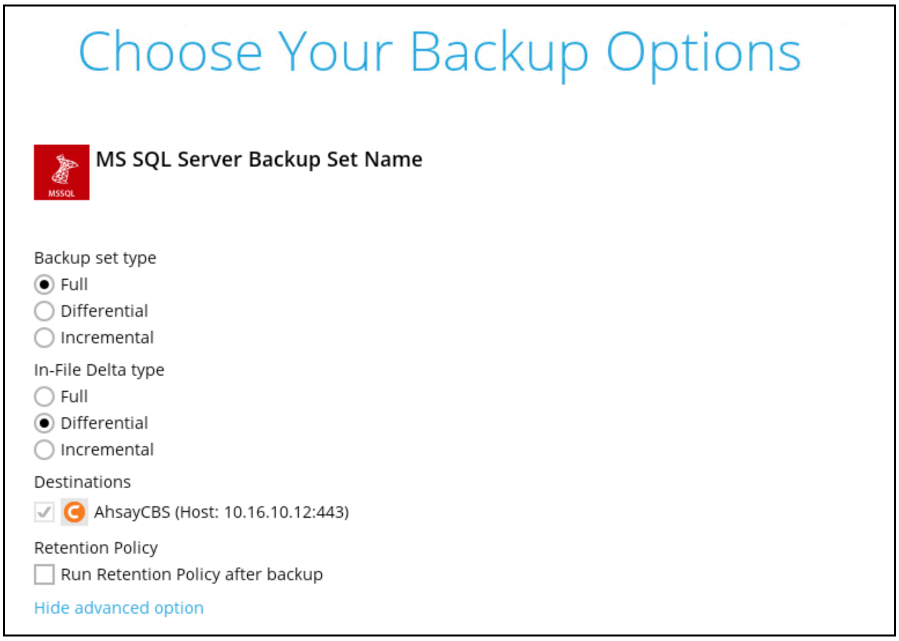
MS SQL Server Backup Set Name (ODBC)

Backup set type
○ Full
● Differential
○ Transaction Log

IMPORTANT

Upon upgrade to AhsayCBS v8 from AhsayOBS v6, when attempting to run a transaction log backup for backup sets created on v6 for the **FIRST TIME**, a full backup will be performed instead. As the disk space required for running a full backup set may significantly be larger than running a transaction log backup, make sure the backup destination has enough quota to accommodate the full backup.

If you would like to modify the In-File Delta type (for Full backup set type only), Destinations and Retention Policy settings, click **Show advanced option**.



Choose Your Backup Options

MS SQL Server Backup Set Name

Backup set type
● Full
○ Differential
○ Incremental

In-File Delta type
○ Full
● Differential
○ Incremental

Destinations
☑ AhsayCBS (Host: 10.16.10.12:443)

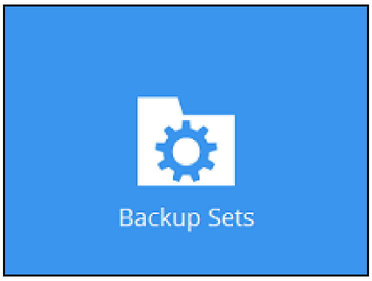
Retention Policy
□ Run Retention Policy after backup

Hide advanced option

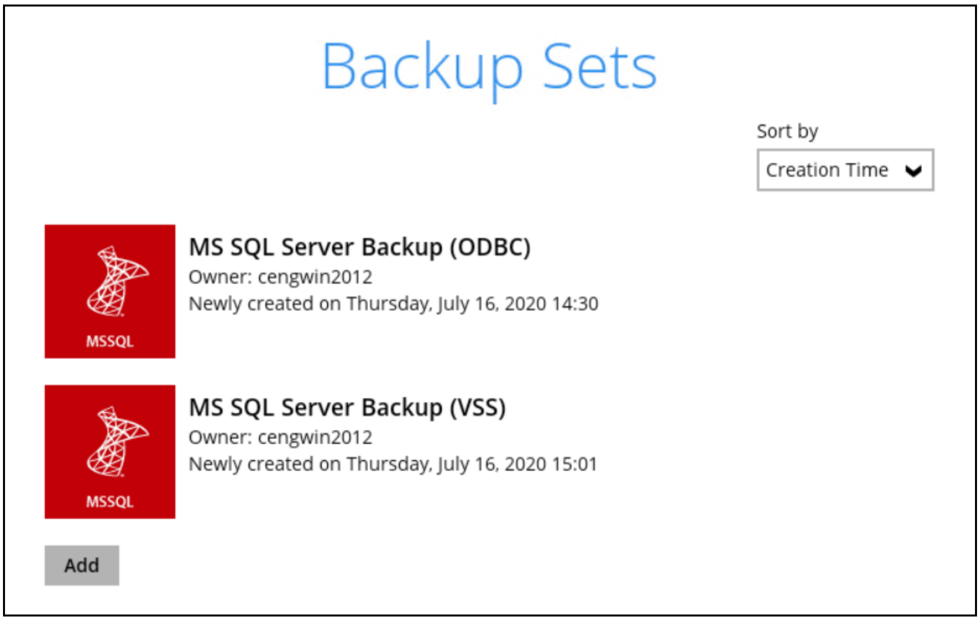
5. Click **Backup** to start the backup job.

8.3 Configuring Backup Schedule for Automated Backup

1. Click the **Backup Sets** icon on the AhsayOBM main interface.



2. Select the backup set which you would like to create a backup schedule for.



Backup Sets

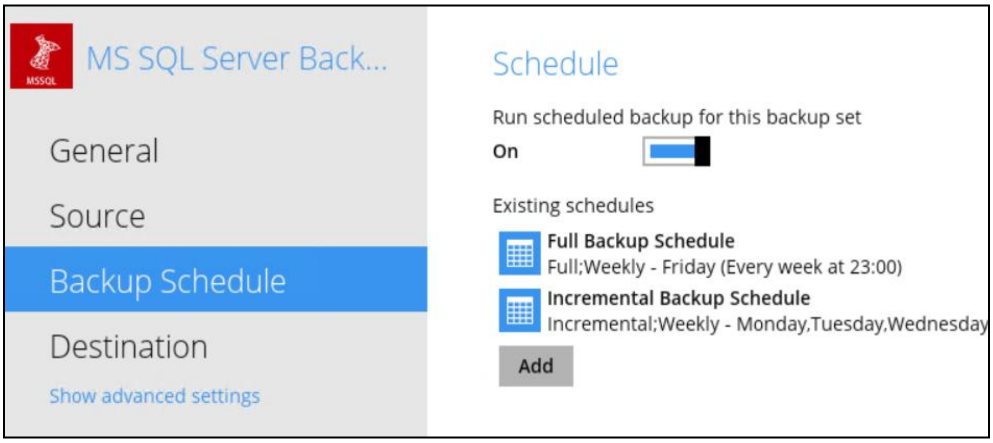
Sort by
Creation Time

MS SQL Server Backup (ODBC)
Owner: cengwin2012
Newly created on Thursday, July 16, 2020 14:30

MS SQL Server Backup (VSS)
Owner: cengwin2012
Newly created on Thursday, July 16, 2020 15:01

3. Go to the **Backup Schedule** tab. If the **Run scheduled backup for this backup set** option is off, switch it **On**. Existing schedules will be listed by default.

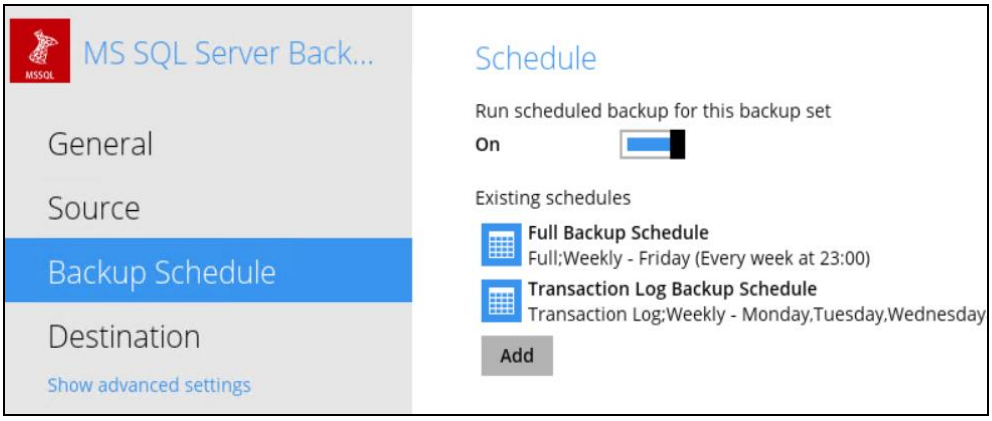
For **VSS Backup Mode**:



Run scheduled backup for this backup set
On

Existing schedules
Full Backup Schedule
Full;Weekly - Friday (Every week at 23:00)
Incremental Backup Schedule
Incremental;Weekly - Monday,Tuesday,Wednesday

For **ODBC Backup Mode**:



Run scheduled backup for this backup set
On

Existing schedules
Full Backup Schedule
Full;Weekly - Friday (Every week at 23:00)
Transaction Log Backup Schedule
Transaction Log;Weekly - Monday,Tuesday,Wednesday

4. Click the **Add** button to add a new backup schedule. The New Backup Schedule window will appear.

5. In the New Backup Schedule window, configure the following backup schedule settings.

   - **Name** – the name of the backup schedule.
   - **Backup set type** – the type of backup set. VSS and ODBC backup modes have different backup set types:

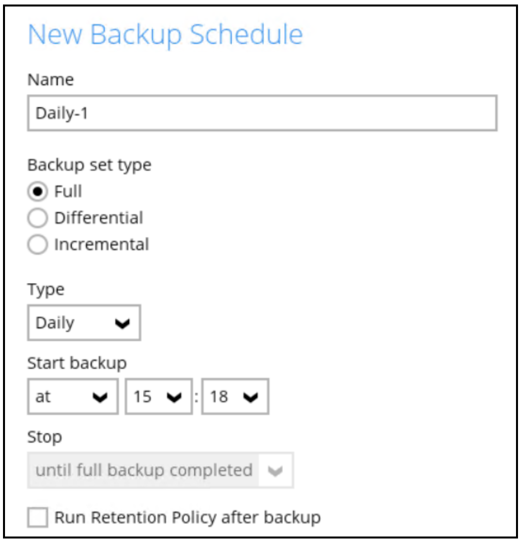
     VSS Backup Mode – has Full, Differential and Incremental backup set types

     ODBC Back Mode – has Full, Differential and Transaction Log backup set types

     For more information, refer to Appendix A Backup Set Type.

- **Type** – the type of backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.
  - **Daily** – the time of the day or interval in minutes/hours which the backup job will run.

VSS Backup Mode



New Backup Schedule

Name: Daily-1

Backup set type
● Full
○ Differential
○ Incremental

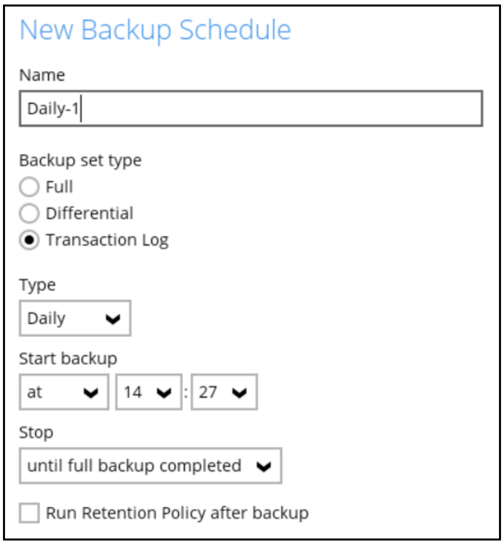
Type: Daily

Start backup: at 15 : 18

Stop: until full backup completed

□ Run Retention Policy after backup

ODBC Backup Mode



New Backup Schedule

Name: Daily-1

Backup set type
○ Full
○ Differential
● Transaction Log

Type: Daily

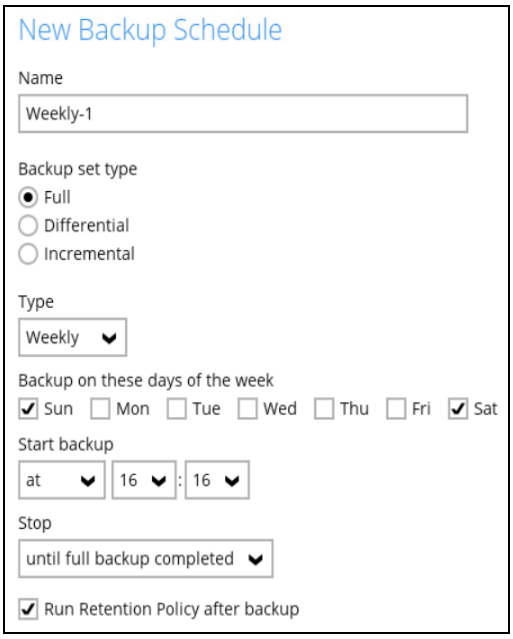
Start backup: at 14 : 27

Stop: until full backup completed

□ Run Retention Policy after backup

  - **Weekly** – the day of the week and the time of the day or interval in minutes/hours which the backup job will run.

VSS Backup Mode



New Backup Schedule

Name: Weekly-1

Backup set type
● Full
○ Differential
○ Incremental

Type: Weekly

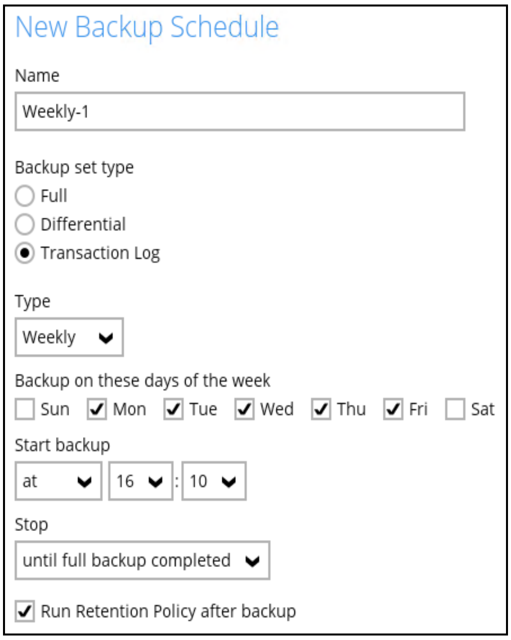
Backup on these days of the week
☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

Start backup: at 16 : 16

Stop: until full backup completed

☑ Run Retention Policy after backup

ODBC Backup Mode



New Backup Schedule

Name: Weekly-1

Backup set type
○ Full
○ Differential
● Transaction Log

Type: Weekly

Backup on these days of the week
□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

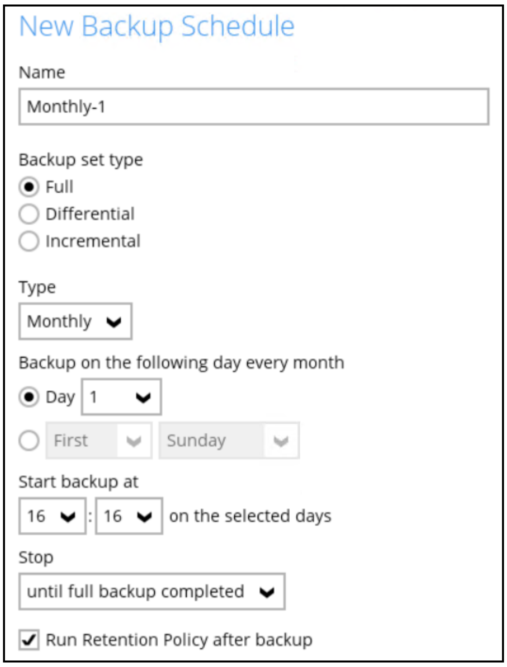
Start backup: at 16 : 10

Stop: until full backup completed

☑ Run Retention Policy after backup

- **Monthly** – the day of the month and the time of that day which the backup job will run.

VSS Backup Mode



New Backup Schedule

Name: Monthly-1

Backup set type
● Full
○ Differential
○ Incremental

Type: Monthly

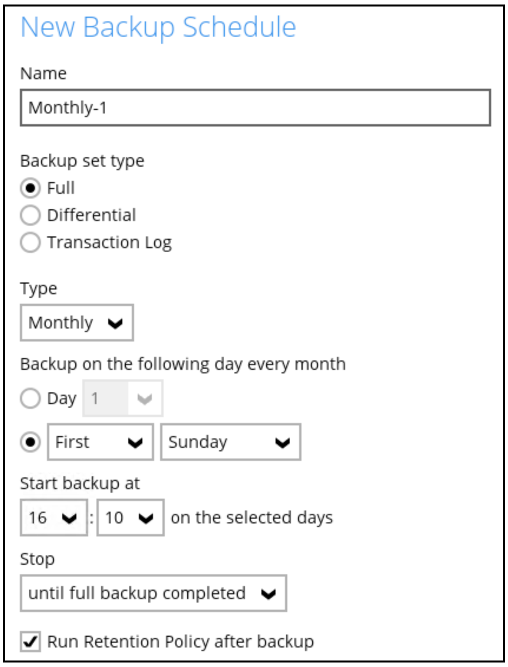
Backup on the following day every month
● Day 1
○ First Sunday

Start backup at 16 : 16 on the selected days

Stop: until full backup completed

☑ Run Retention Policy after backup

ODBC Backup Mode



New Backup Schedule

Name: Monthly-1

Backup set type
● Full
○ Differential
○ Transaction Log

Type: Monthly

Backup on the following day every month
○ Day 1
● First Sunday

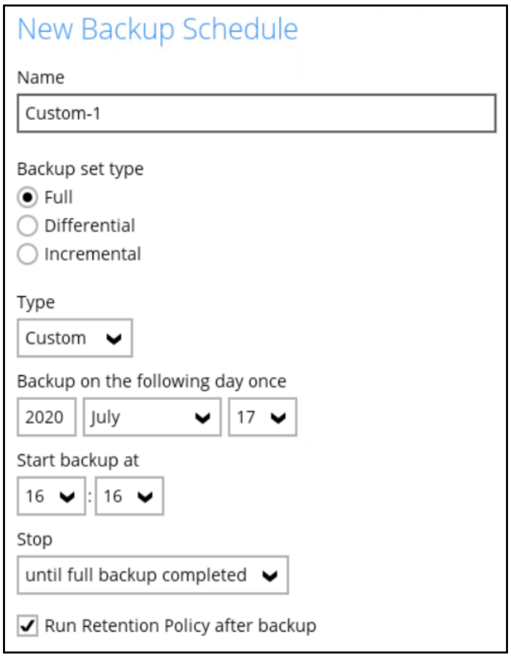
Start backup at 16 : 10 on the selected days

Stop: until full backup completed

☑ Run Retention Policy after backup

- **Custom** – a specific date and the time of that date which the backup job will run.

VSS Backup Mode



New Backup Schedule

Name: Custom-1

Backup set type
● Full
○ Differential
○ Incremental

Type: Custom

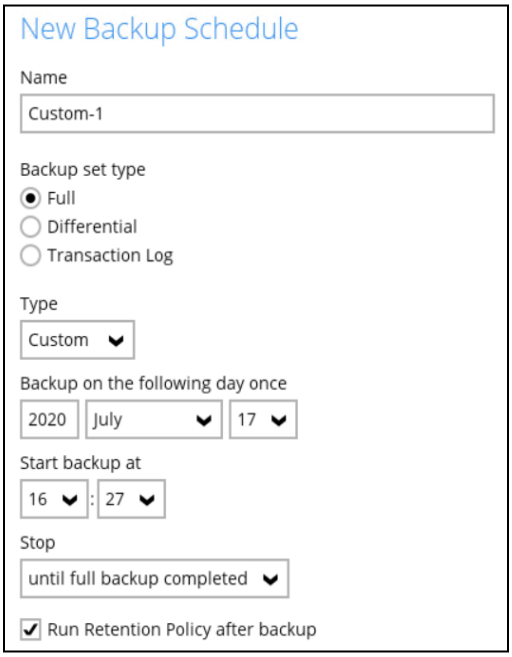
Backup on the following day once: 2020 July 17

Start backup at 16 : 16

Stop: until full backup completed

☑ Run Retention Policy after backup

ODBC Backup Mode



New Backup Schedule

Name: Custom-1

Backup set type
● Full
○ Differential
○ Transaction Log

Type: Custom

Backup on the following day once: 2020 July 17

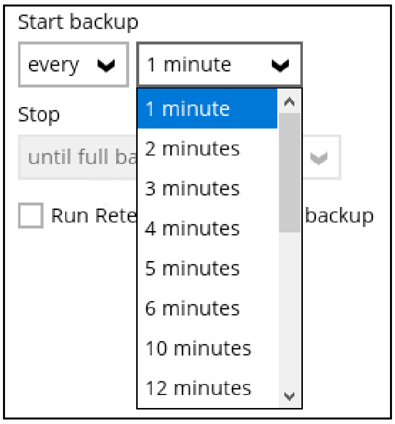
Start backup at 16 : 27

Stop: until full backup completed

☑ Run Retention Policy after backup

- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job <u>at a specific time</u>.

- **every** – this option will start a backup job <u>in intervals of minutes or hours</u>.



Start backup

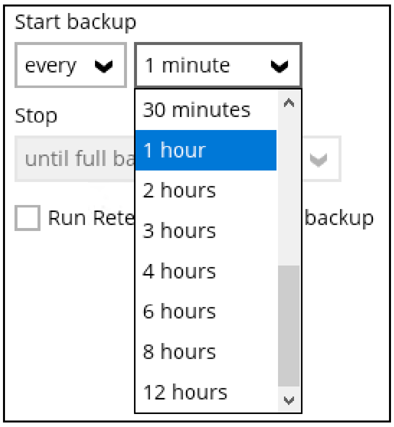
every ▾ 1 minute ▾

Stop

until full ba

□ Run Rete backup

1 minute
2 minutes
3 minutes
4 minutes
5 minutes
6 minutes
10 minutes
12 minutes



Start backup

every ▾ 1 minute ▾

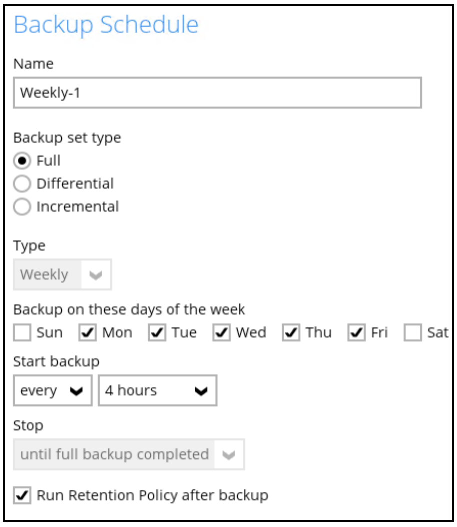
Stop

until full ba

□ Run Rete backup

30 minutes
1 hour
2 hours
3 hours
4 hours
6 hours
8 hours
12 hours

Here is an example of a backup set that has a periodic and normal backup schedule.



Backup Schedule

Name: Weekly-1

Backup set type
● Full
○ Differential
○ Incremental

Type: Weekly

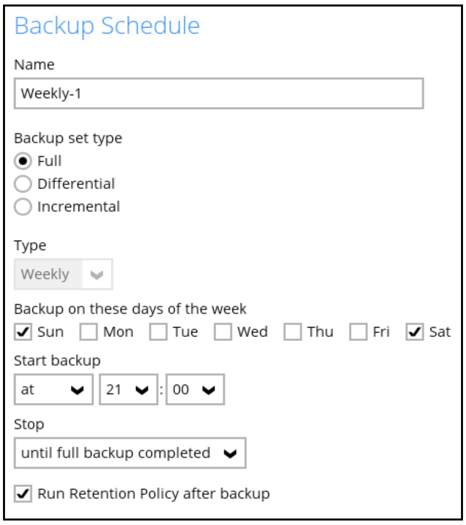
Backup on these days of the week
□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Start backup: every ▾ 4 hours ▾

Stop: until full backup completed

☑ Run Retention Policy after backup

Figure 1.1



Backup Schedule

Name: Weekly-1

Backup set type
● Full
○ Differential
○ Incremental

Type: Weekly

Backup on these days of the week
☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

Start backup: at ▾ 21 ▾ : 00 ▾

Stop: until full backup completed ▾

☑ Run Retention Policy after backup

Figure 1.2

Figure 1.1 – Periodic backup schedule runs every 4 hours from Monday – Friday during business hours

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday on weekend non-business hours

- **Stop** – the stop time of the backup job. This only applies to schedules with start backup “at” and is not supported for periodic backup schedule (start backup “every”)

  - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.

  - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

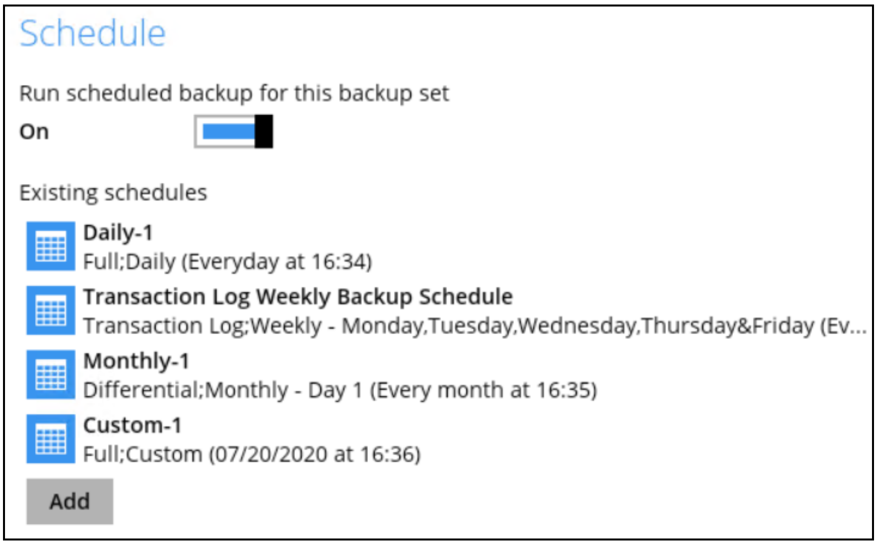
For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set the "stop" after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

The partially backed up data will have to be removed by running the data integrity check.

As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

- **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job. To save hard disk quote in the long run, it is recommended to enable this option.

As an example, the four types of backup schedule (i.e. Daily, Weekly, Monthly and Custom) may look like the following:



Schedule

Run scheduled backup for this backup set
On

Existing schedules

Daily-1
Full;Daily (Everyday at 16:34)

Transaction Log Weekly Backup Schedule
Transaction Log;Weekly - Monday,Tuesday,Wednesday,Thursday&Friday (Ev...

Monthly-1
Differential;Monthly - Day 1 (Every month at 16:35)

Custom-1
Full;Custom (07/20/2020 at 16:36)

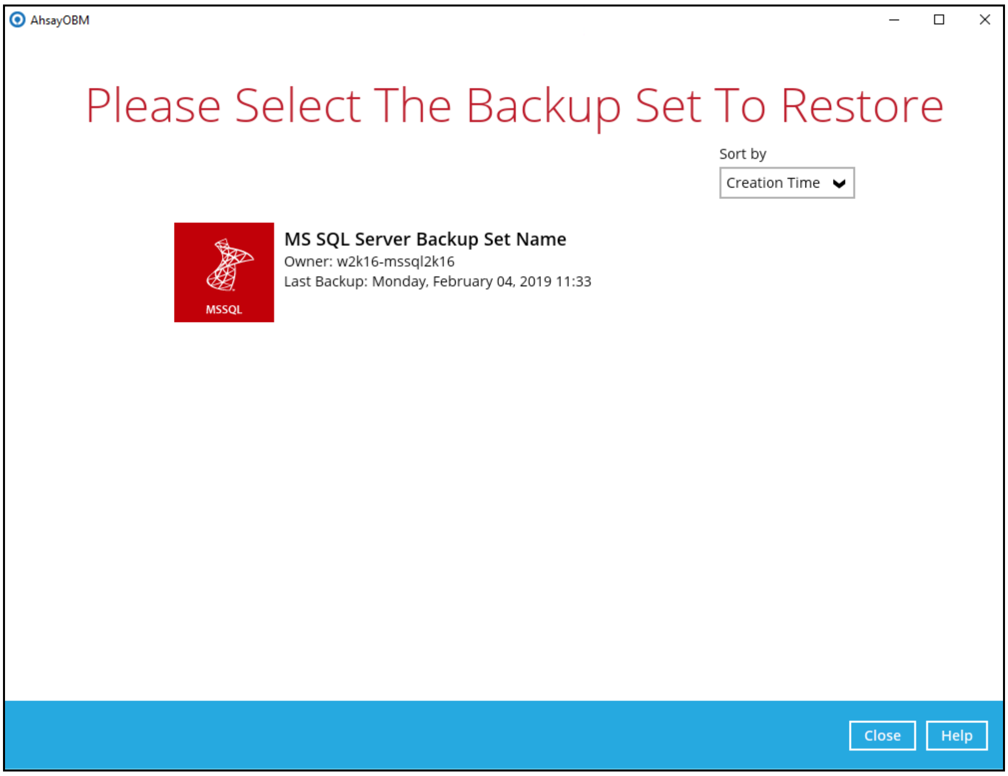
6. Click **Save** to confirm your settings once done.

9 Restoring Backup for Microsoft SQL Server

Restoring Backup for Microsoft SQL Server

1. In the AhsayOBM main interface, click the **Restore** icon.

2. Select the backup set that you would like to restore.

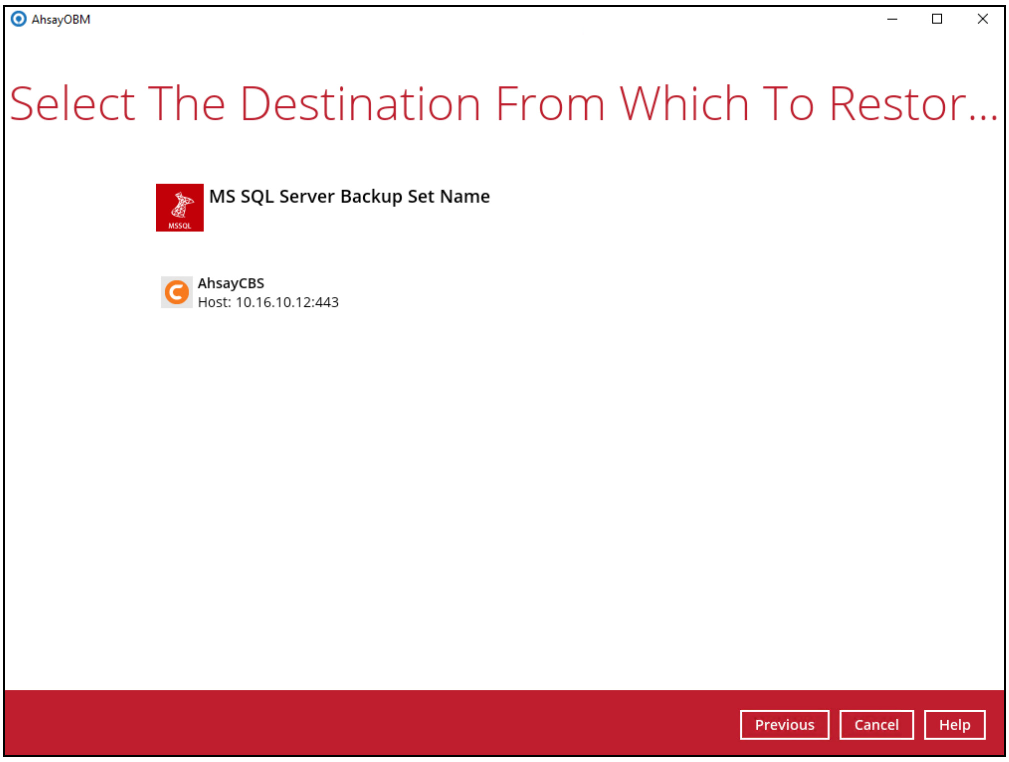


Please Select The Backup Set To Restore

Sort by: Creation Time

MS SQL Server Backup Set Name
Owner: w2k16-mssql2k16
Last Backup: Monday, February 04, 2019 11:33

3. Select the backup destination that you would like to restore data from.



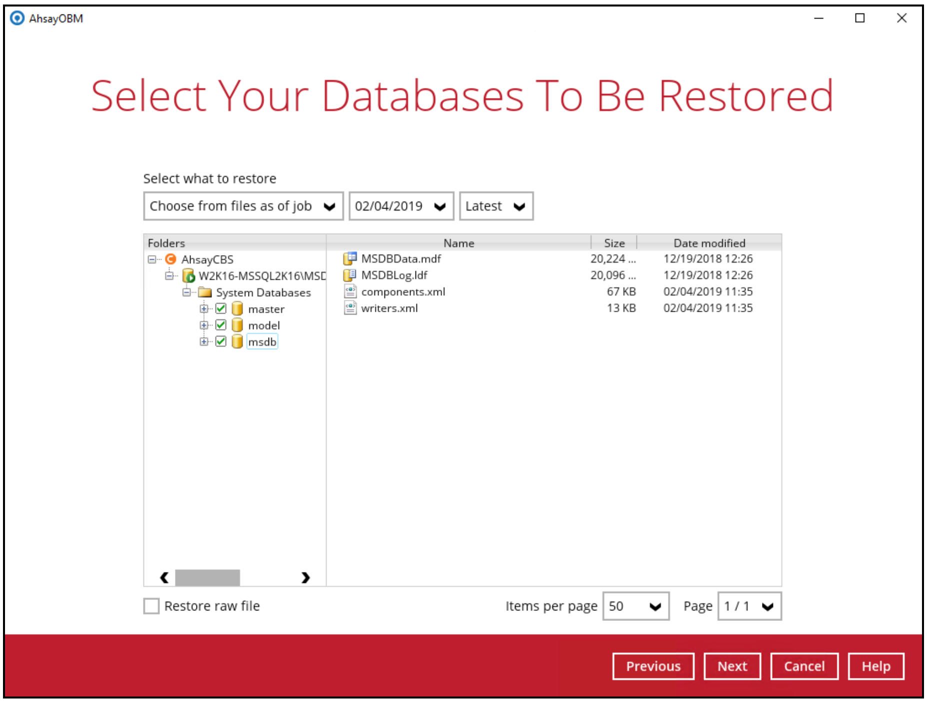
Select The Destination From Which To Restor...

MS SQL Server Backup Set Name

AhsayCBS
Host: 10.16.10.12:443

4. Select the database(s) or raw file(s) you would like to restore. You can also choose to restore backed up database or raw file from a specific backup job of your choice using the **Select what to restore** drop-down menu at the top. Click **Next** to proceed when you are done with the selection.

- **Restoring database -** expand the menu tree to select which database to restore. Follow **5a** below to select restoring to the original SQL server or an alternate SQL server.



Select Your Databases To Be Restored

Select what to restore: Choose from files as of job | 02/04/2019 | Latest

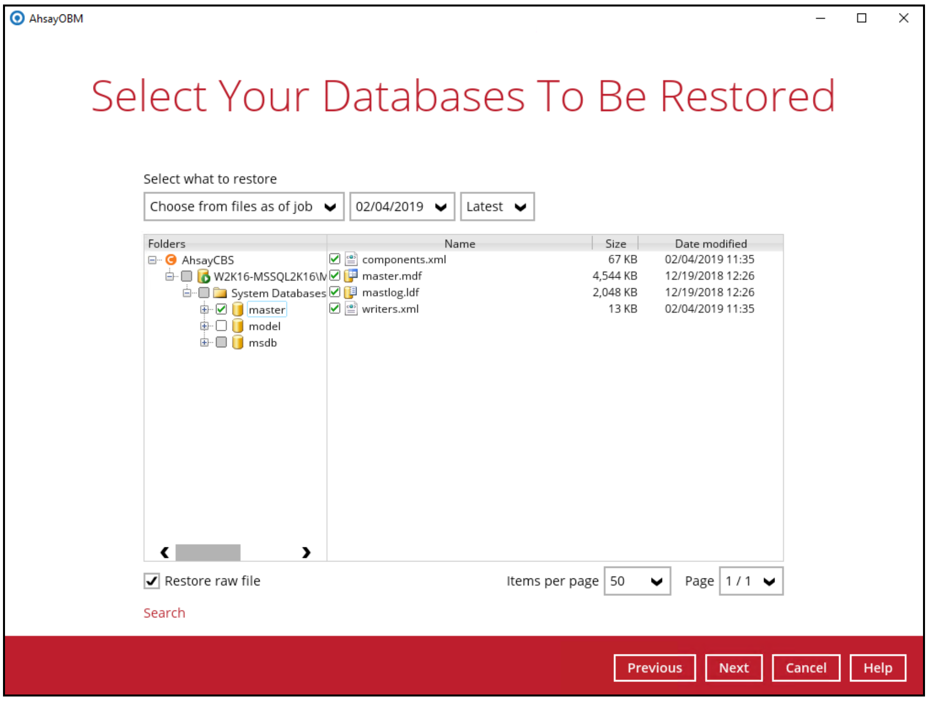
Folders:
- AhsayCBS
  - W2K16-MSSQL2K16\MSSQ
    - System Databases
      - ☑ master
      - ☑ model
      - ☑ msdb

Name	Size	Date modified
MSDBData.mdf	20,224 ...	12/19/2018 12:26
MSDBLog.ldf	20,096 ...	12/19/2018 12:26
components.xml	67 KB	02/04/2019 11:35
writers.xml	13 KB	02/04/2019 11:35

□ Restore raw file

Items per page 50   Page 1 / 1

- **Restoring raw file** - you can select individual raw database file to restore by clicking the **Restore raw file** checkbox at the left bottom corner. Follow **5b** below to select the path where you would like to restore the raw file(s) to.



AhsayOBM

Select Your Databases To Be Restored

Select what to restore

Choose from files as of job | 02/04/2019 | Latest

Folders

- AhsayCBS
  - W2K16-MSSQL2K16\M
    - System Databases
      - ☑ master
      - □ model
      - □ msdb

	Name	Size	Date modified
☑	components.xml	67 KB	02/04/2019 11:35
☑	master.mdf	4,544 KB	12/19/2018 12:26
☑	mastlog.ldf	2,048 KB	12/19/2018 12:26
☑	writers.xml	13 KB	02/04/2019 11:35

☑ Restore raw file

Items per page 50 Page 1 / 1

Search

Limitations:

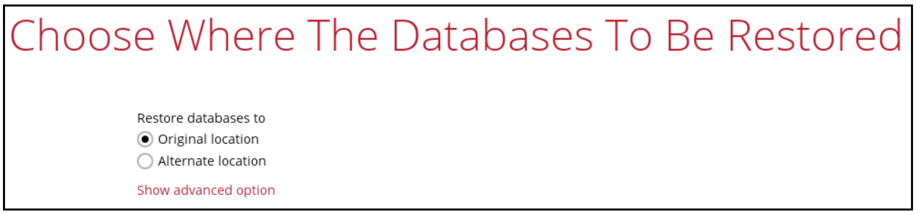
- ➢ If you would like to restore database with the Alternate location option, you can only choose to restore one database at a time.
- ➢ If you would like to restore database to an alternate SQL server with the **Restore raw file** option, make sure you have checked the **Restore raw file** option.

5. Select the destination to restore. Refer to 5a or 5b below for steps to restore the database automatically (Restore database to Original/Alternate location) or manually (Restore raw file).

5a. Select to restore the database to its Original SQL server, or to an Alternate SQL server.

- **Restore to Original SQL server**

  Select the **Original location** option, then press **Next** to proceed.



Choose Where The Databases To Be Restored

Restore databases to

● Original location

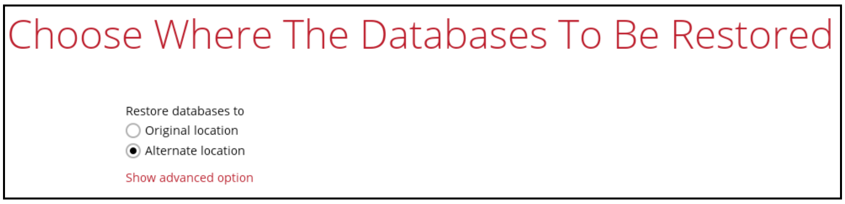
○ Alternate location

Show advanced option

If you would like to modify the Verify checksum of in-file delta files during restore setting, click **Show advanced option**.

- **Restore to Alternate SQL server (only for restoring raw file)**

i. Select the **Alternate location** option, then press **Next**.



Choose Where The Databases To Be Restored

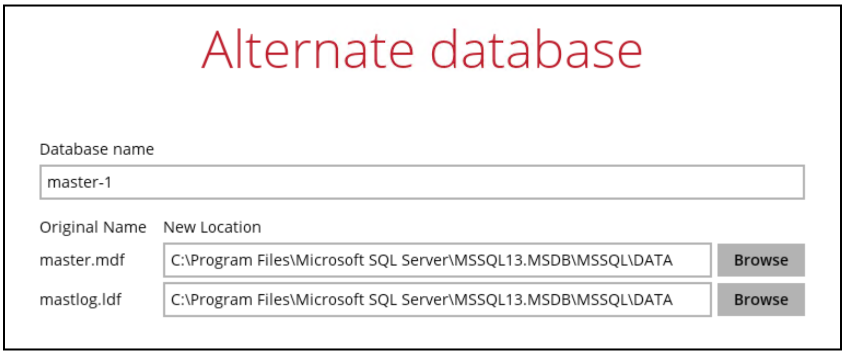
Restore databases to

○ Original location

● Alternate location

If you would like to modify the In-File Delta type (for Full backup set type only), Destinations and Retention Policy settings, click **Show advanced option**.

ii. Click **Browse** to select the locations where you would like to restore the database and log files to. Name the new database, then.



Alternate database

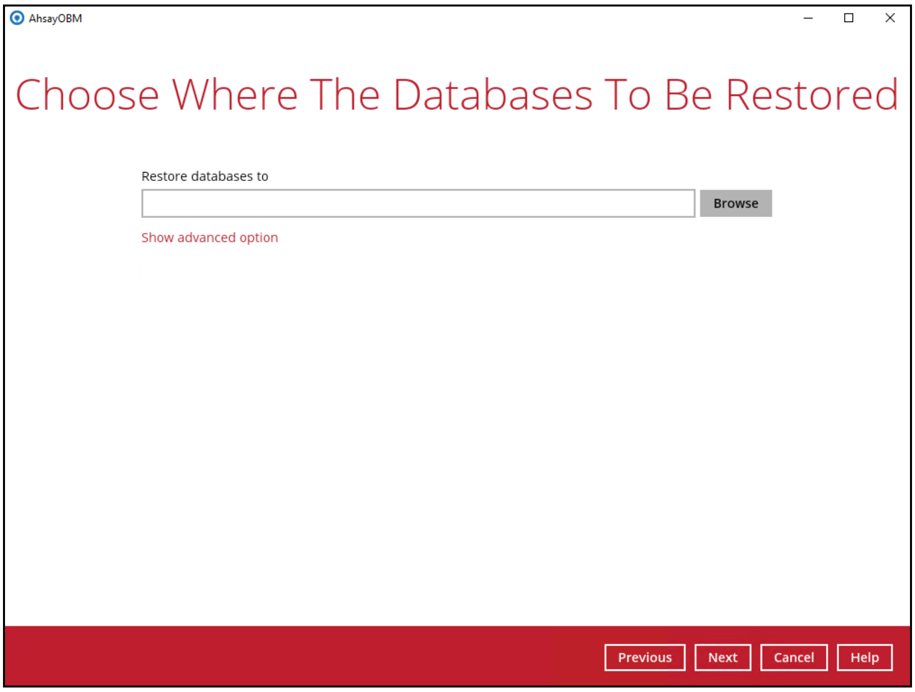
Database name

master-1

Original Name	New Location	
master.mdf	C:\Program Files\Microsoft SQL Server\MSSQL13.MSDB\MSSQL\DATA	Browse
mastlog.ldf	C:\Program Files\Microsoft SQL Server\MSSQL13.MSDB\MSSQL\DATA	Browse

iii. Click **Next** to proceed when you are done with the settings.

5b. i) If you have chosen to restore raw file, choose the location path where you would like the raw file(s) to be restored to. Click **Next** to proceed.



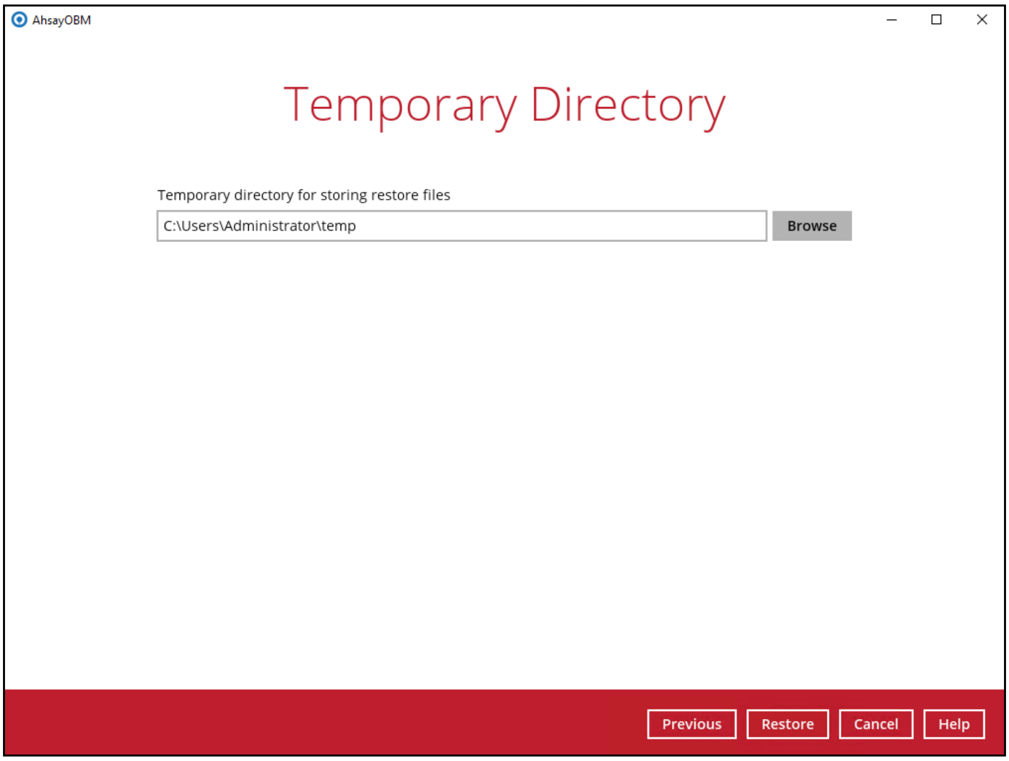
Choose Where The Databases To Be Restored

Restore databases to

If you would like to modify the In-File Delta type (for Full backup set type only), Destinations and Retention Policy settings, click **Show advanced option**.

ii) Restore the database manually with the restored database file via the SQL Server Management Studio. Refer to the MS KB article below for instructions.
https://technet.microsoft.com/en-us/library/ms177429%28v=sql.110%29.aspx

6. Select the temporary directory for storing temporary files, such as delta files when they are being merged, click **Restore** to start the restoration.

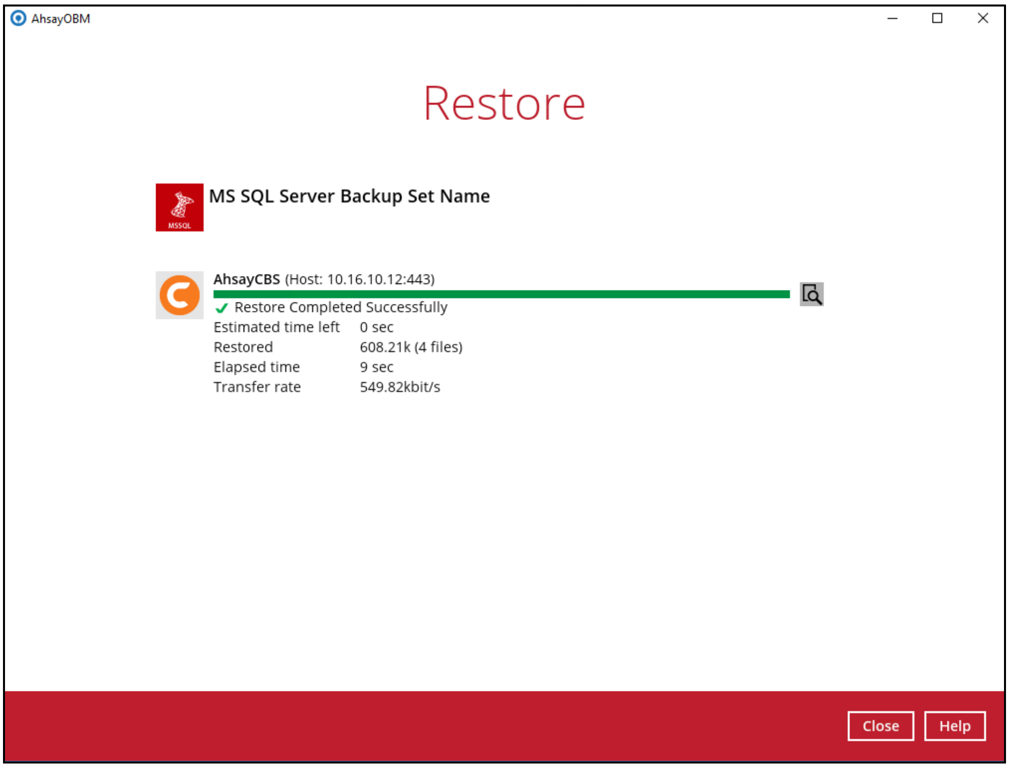


Temporary Directory

Temporary directory for storing restore files

C:\Users\Administrator\temp

7. The following screen with the text **Restore Completed Successfully** shows when the restoration is completed.



Restore

MS SQL Server Backup Set Name

AhsayCBS (Host: 10.16.10.12:443)

✓ Restore Completed Successfully

```
Estimated time left    0 sec
Restored               608.21k (4 files)
Elapsed time           9 sec
Transfer rate          549.82kbit/s
```

10 Contacting Ahsay

10.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:
https://www.ahsay.com/partners/

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
https://wiki.ahsay.com/

10.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:
https://www.ahsay.com/partners/

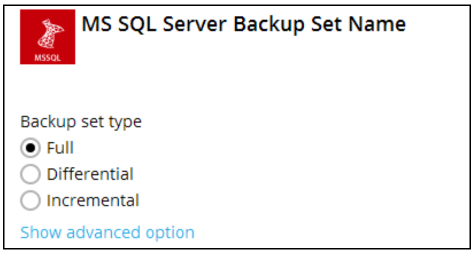
Please specify the specific document title as well as the change required/suggestion when contacting us.

Appendix

Appendix A Backup Set Type

There are three kinds of backup set type to choose from, namely full backup, differential backup and incremental backup. The information below gives you an overall idea of what each backup set type is like.

Full backup (with configurable in-file delta type)



MS SQL Server Backup Set Name

Backup set type

● Full

○ Differential

○ Incremental

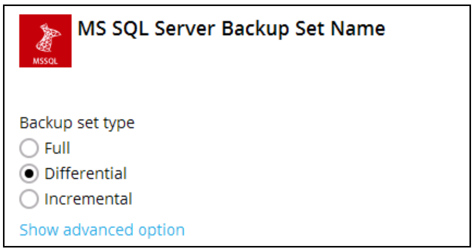
Show advanced option

To perform a full backup, AhsayOBM requests the SQL server to generate a Volume Shadow Copy Service (VSS) snapshot of the database. AhsayOBM will back up the VSS snapshot generated by the SQL server directly. A full backup is required in order to run incremental or differential backups.

You can also decide how the full backup is run by selecting the desired in-file delta type (Full, Differential or Incremental).

For further details on this topic, refer to the URL below.
https://msdn.microsoft.com/en-us/library/ms175477.aspx

Differential backup



MS SQL Server Backup Set Name

Backup set type

○ Full

● Differential

○ Incremental

Show advanced option

A differential backup of the SQL server saves changes to the database that have occurred since the last full backup. To perform a differential backup, AhsayOBM requests the SQL server to generate a differential backup file of the database since the last full backup. At the back end, the SQL server performs the following:

1. Generate a VSS snapshot of the database of the current state.
2. Compare the VSS snapshot just generated by the SQL server with the one generated from the last full backup in order to produce a differential backup file.
3. The differential backup file being sent to AhsayOBM for backup.

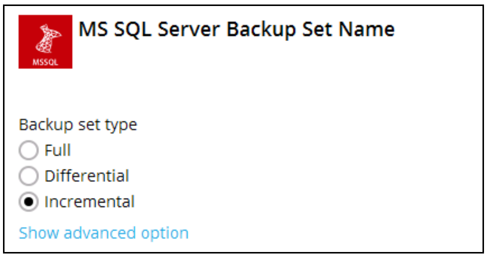
Using a differential backup file to recover a database requires the restoration of only two data sets - the last full backup and the most recent differential backup.

The disadvantage of using differential backups is that it duplicates the backed up data in each backup until a full backup is performed. If there are many differential backups taken between full backups, the storage space required can greatly exceed that required by the same number of incremental backups.

The SQL server does not allow a differential backup to occur when there has been no previous full backup to establish the starting point.

For further details on this topic, refer to the URL below.
https://msdn.microsoft.com/en-us/library/ms186289.aspx

Incremental backup


MS SQL Server Backup Set Name

Backup set type

○ Full

○ Differential

● Incremental

Show advanced option

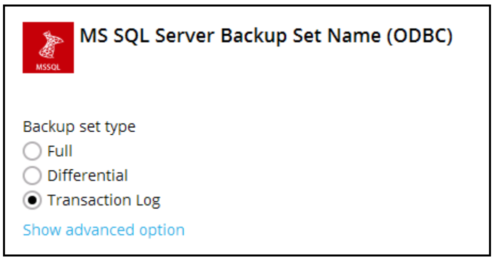
An incremental backup of the SQL server saves changes to the database that have occurred since the last full or incremental backup. To perform an incremental backup, AhsayOBM requests the SQL server to generate a differential backup file of the database since the last full backup. At the back end, the SQL server performs the following:

1. Generate a VSS snapshot of the database of the current state.
2. Compare the VSS snapshot just generated with the one generated from the last full backup in order to produce a differential backup file.
3. The differential backup file being sent to AhsayOBM.
4. AhsayOBM performs an in-file delta check between the differential backup file just received from the SQL server and the one from the last backup.
5. AhsayOBM will then be able to generate an incremental delta file which contains changes of the database files since last differential backup. Only this incremental delta file will be backed up.

Using an incremental backup to recover a database requires the restoration of at least two data sets - the last full backup and every incremental backup taken after the last Full backup. The benefit of using incremental backups is that the individual backups are much smaller than a full backup and individual incremental backups are frequently smaller than differential backups.

The disadvantage of using incremental backups is that if there are many incremental backups made between full backups, recovering the storage group may involve recovering many incremental backups. The SQL server does not allow an incremental backup to occur when there has been no previous full backup to establish the starting point.

Transaction log


MS SQL Server Backup Set Name (ODBC)

Backup set type

○ Full

○ Differential

● Transaction Log

Show advanced option

Every SQL Server database has a transaction log that records all transactions and the database modifications made by each transaction. The transaction log is a critical component of the database. If there is a system failure, you will need that log to bring your database back to a consistent state.

If you have chosen to back up in ODBC mode, you can configure schedule backup to back up the transaction log regularly at a time interval of your choice.

IMPORTANT

Upon upgrade to AhsayCBS v8 from AhsayOBS v6, when attempting to run a transaction log backup for backup sets created on v6 for the **FIRST TIME**, a full backup will be performed instead. As the disk space required for running a full backup set may significantly be larger than running a transaction log backup, make sure the backup destination has enough quota to accommodate the full backup.

Appendix B Truncating Transaction Log

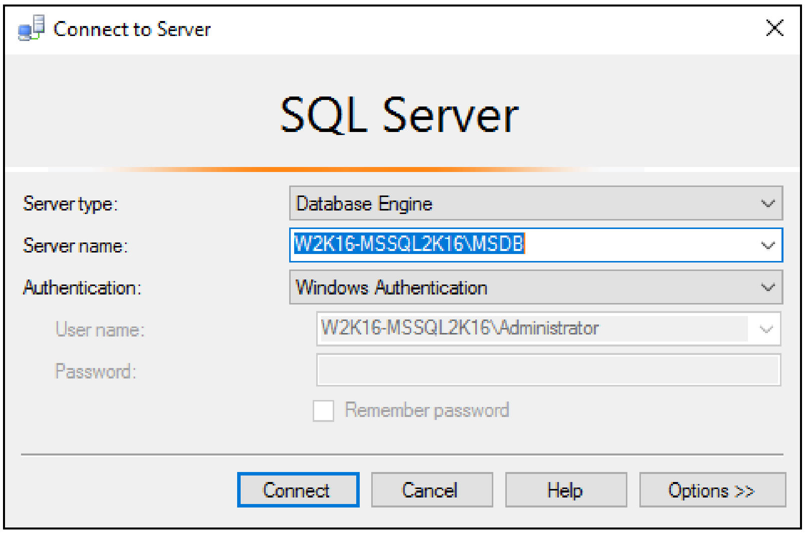
The instructions below only apply for database with full recovery model.

Since AhsayOBM v8 utilizes VSS-based backup, which does not support log backup (https://technet.microsoft.com/en-us/library/cc966520.aspx), transaction log of database in full / bulk-logging recovery model may eventually fill up all disk space available on the volume

Below are steps to perform a log backup in the SQL Server Management Studio. For further details on this topic, refer to the URL below.
https://msdn.microsoft.com/en-us/library/ms179478.aspx

1. Launch SQL Server Management Studio in Windows.

2. Select the SQL server you would like to connect to, and the corresponding authentication method, then click **Connect** to proceed.



Connect to Server

SQL Server

Server type: Database Engine

Server name: W2K16-MSSQL2K16\MSDB

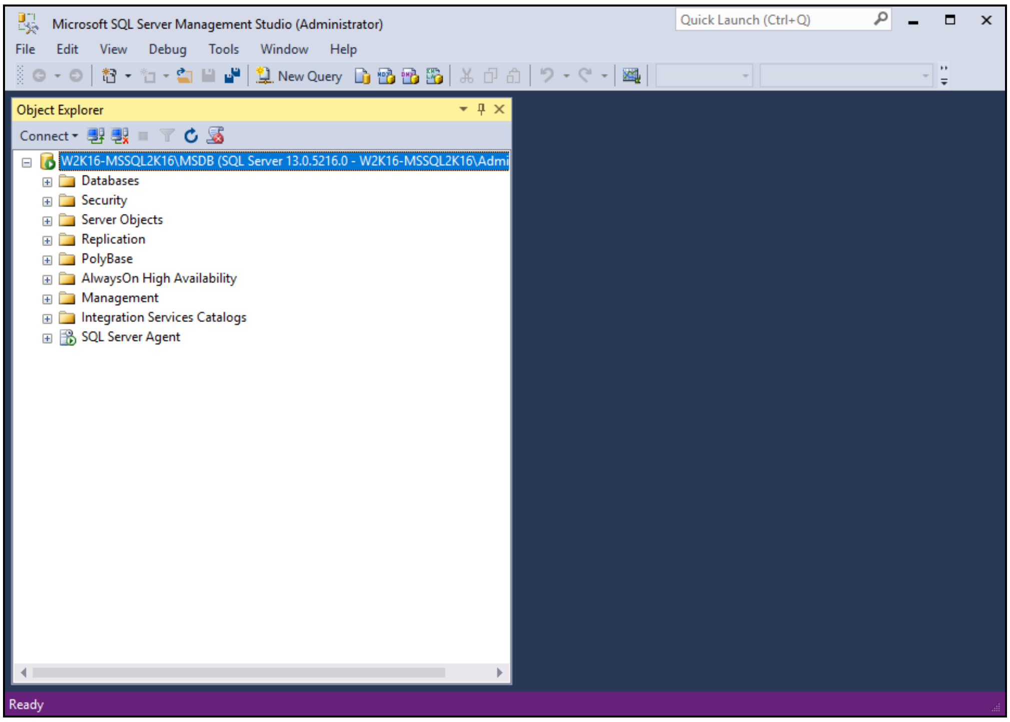
Authentication: Windows Authentication

User name: W2K16-MSSQL2K16\Administrator

Password:

□ Remember password

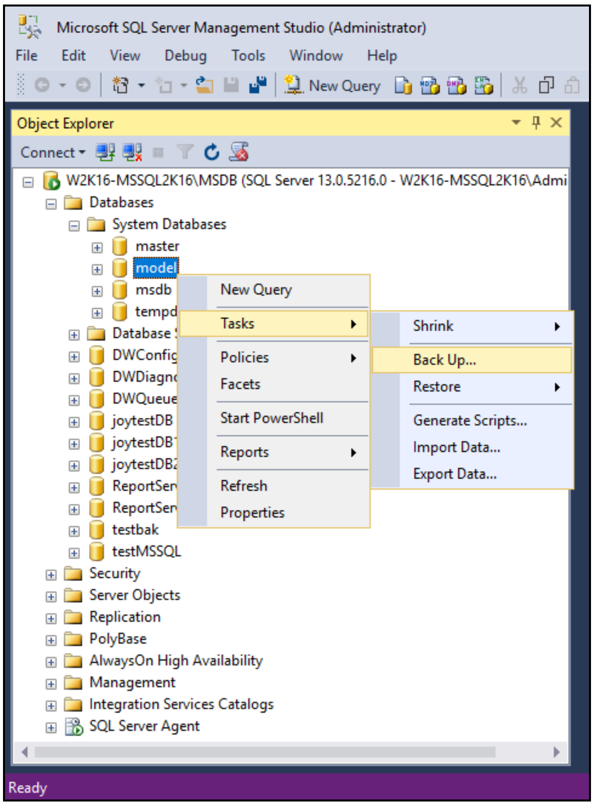
3. Expand the menu tree and select the desired database you would like to back up.



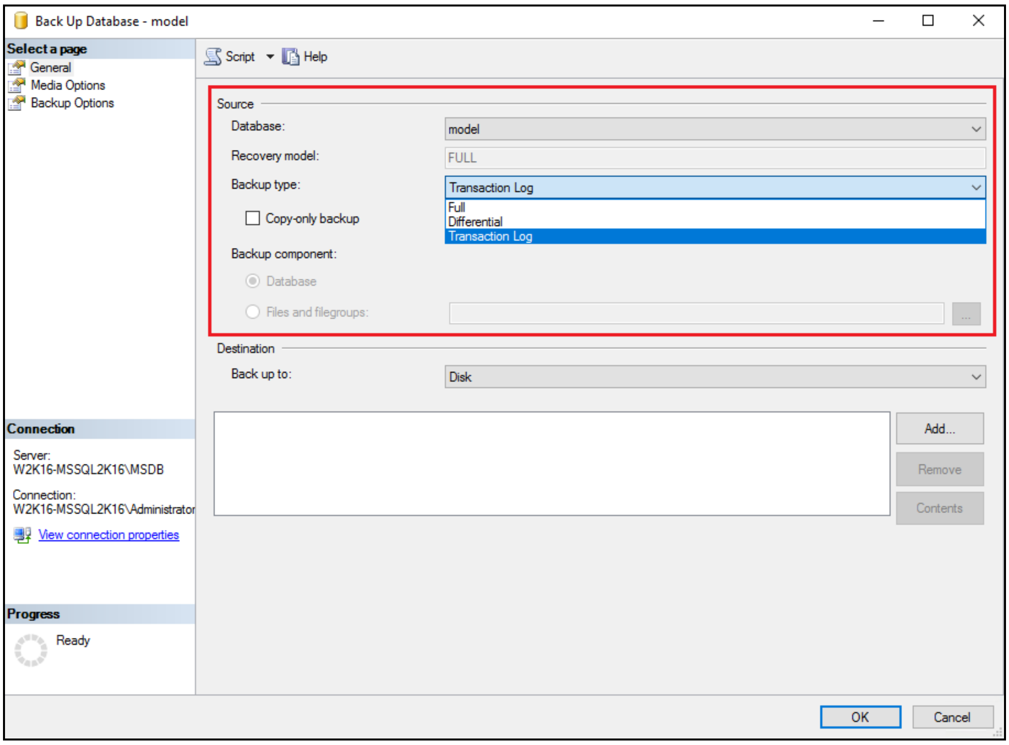
Microsoft SQL Server Management Studio (Administrator)

W2K16-MSSQL2K16\MSDB (SQL Server 13.0.5216.0 - W2K16-MSSQL2K16\Admi

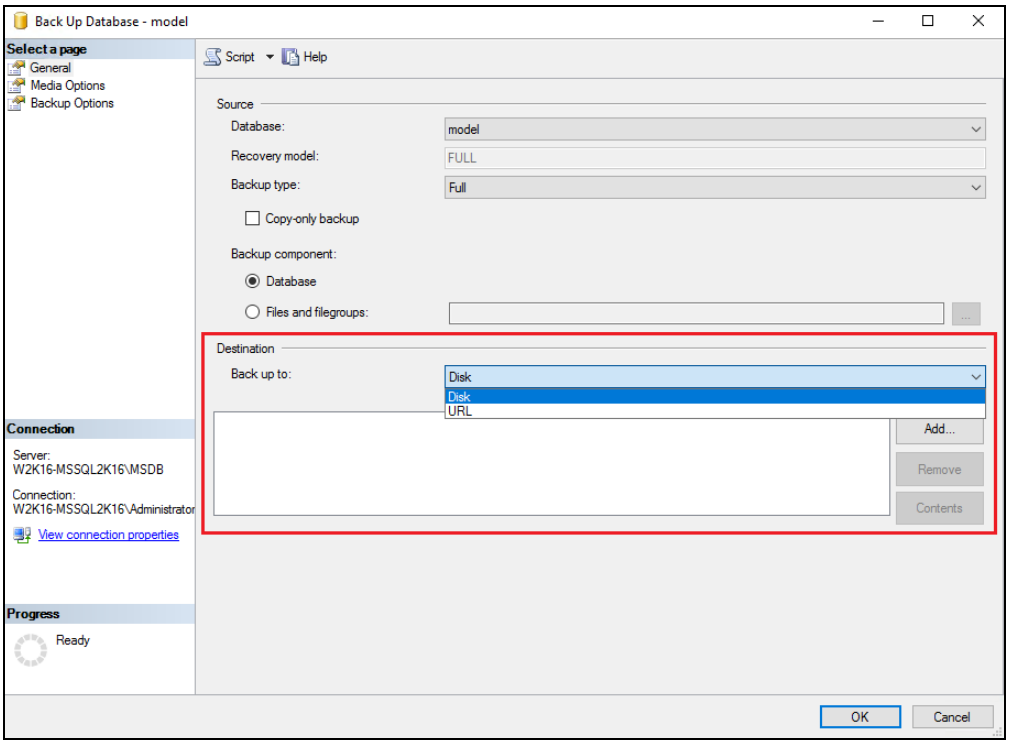
4. Right click the database name, then go to **Tasks** > **Back Up**. The Back Up Database dialog box shows.



5. In the **Source** section, confirm the database name, then select Transaction Log in the **Backup type** drop-down menu.



6. Select **Disk** or **URL** as the destination of the backup, then click **Add** to select a destination path.



Source

Database: model

Recovery model: FULL

Backup type: Full

☐ Copy-only backup

Backup component:

● Database

○ Files and filegroups:

Destination

Back up to: Disk

Disk

URL

Connection

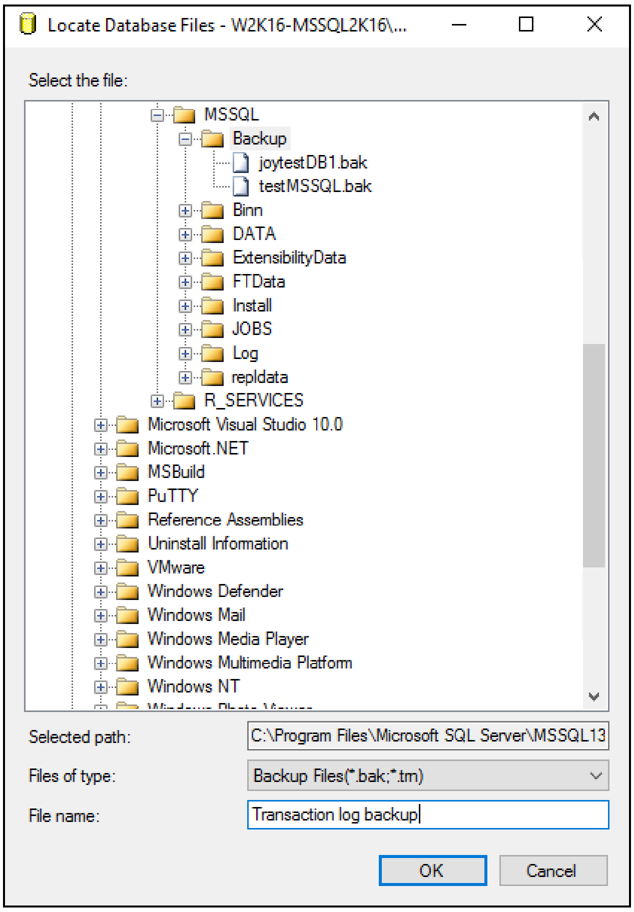
Server:
W2K16-MSSQL2K16\MSDB

Connection:
W2K16-MSSQL2K16\Administrator

Progress

Ready

7. After selecting the destination path, click **OK** twice to proceed.



Select the file:

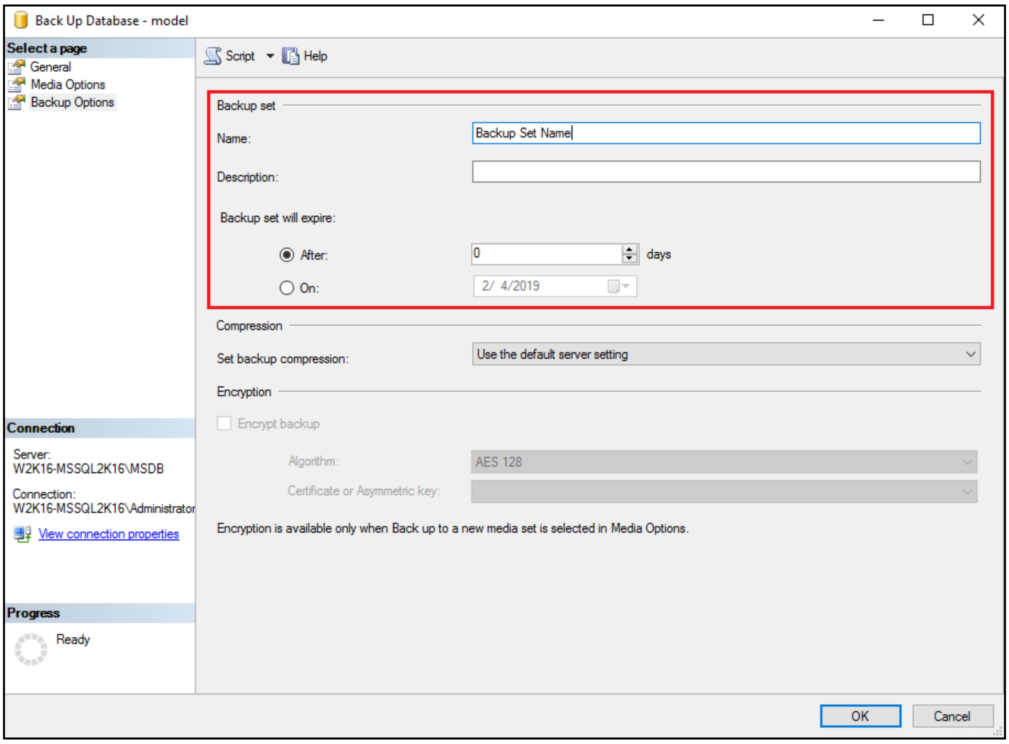
Selected path: C:\Program Files\Microsoft SQL Server\MSSQL13

Files of type: Backup Files(*.bak;*.tm)

File name: Transaction log backup

8. Go to the **Backup Options**, then in the **Backup set** section, name the backup set and enter a description of the backup set if needed.

   Configure the Backup set to expire after a specified number of day or on a specified date. Set to 0 day if you do not want the backup set to expire



Back Up Database - model

Select a page
- General
- Media Options
- Backup Options

Backup set

Name: Backup Set Name

Description:

Backup set will expire:

● After: 0 days

○ On: 2/ 4/2019

Compression

Set backup compression: Use the default server setting

Encryption

□ Encrypt backup

Algorithm: AES 128

Certificate or Asymmetric key:

Encryption is available only when Back up to a new media set is selected in Media Options.

Connection

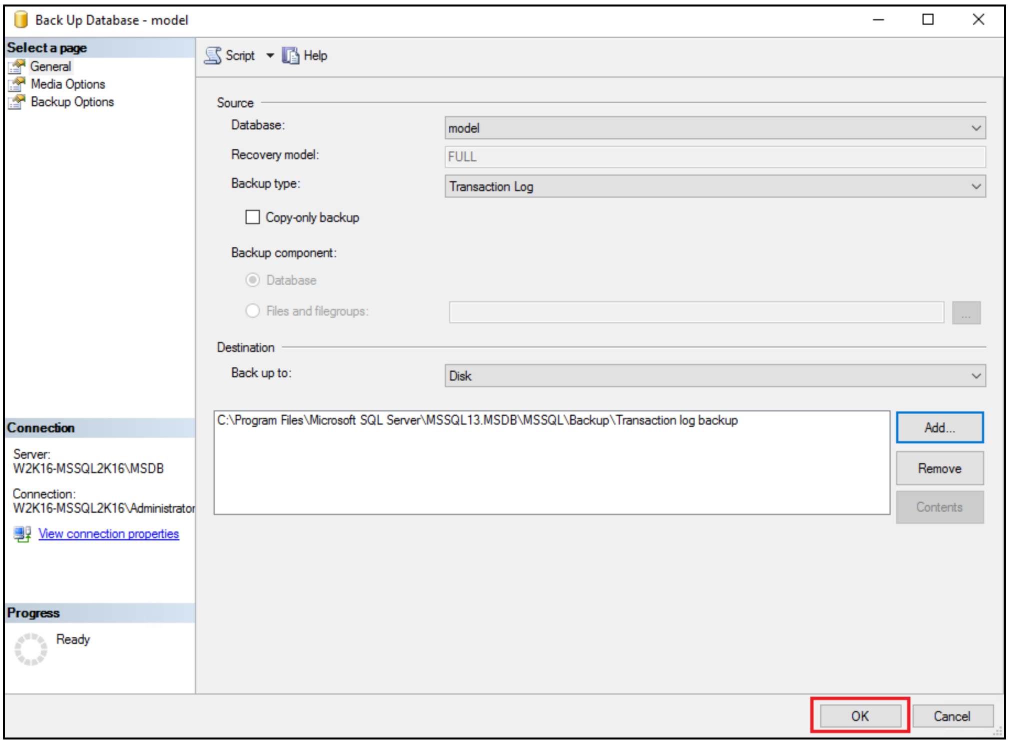
Server:
W2K16-MSSQL2K16\MSDB

Connection:
W2K16-MSSQL2K16\Administrator

Progress

Ready

9. Click **OK** to start the transaction log backup when you are done with all the necessary settings in the **Back Up Database** dialog box.



Back Up Database - model

Select a page
- General
- Media Options
- Backup Options

Source

Database: model

Recovery model: FULL

Backup type: Transaction Log

□ Copy-only backup

Backup component:

● Database

○ Files and filegroups:

Destination

Back up to: Disk

C:\Program Files\Microsoft SQL Server\MSSQL13.MSDB\MSSQL\Backup\Transaction log backup

Connection

Server:
W2K16-MSSQL2K16\MSDB

Connection:
W2K16-MSSQL2K16\Administrator

Progress

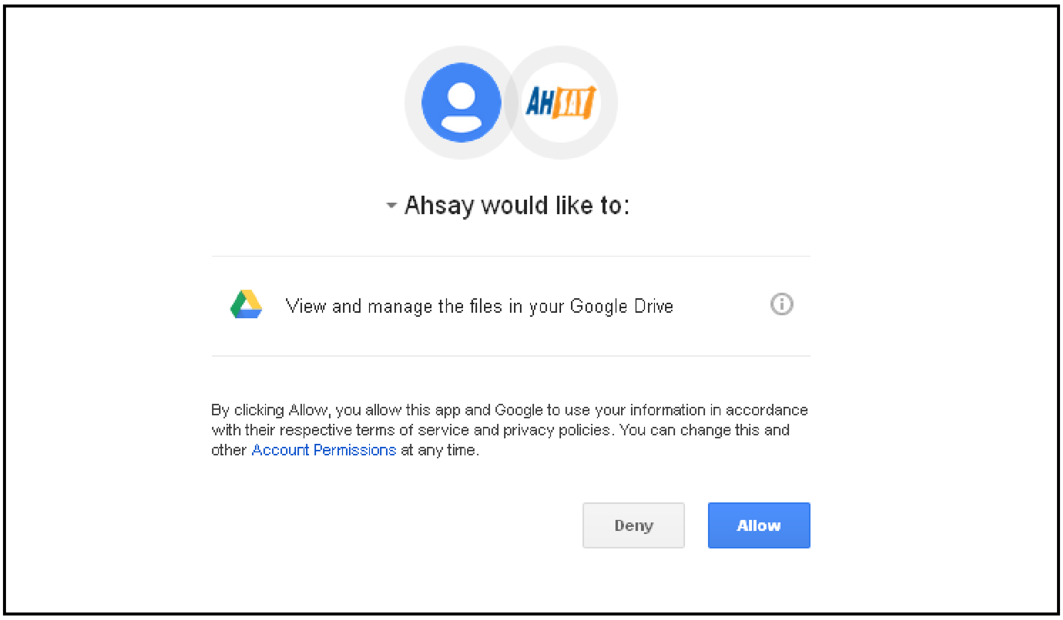
Ready

Appendix C Cloud Storage as Backup Destination

For most cloud storage provider (e.g. Dropbox, Google Drive ... etc.), you need to allow AhsayOBM to access the cloud destination. Click **OK** / **Test**, you will be prompted to log in to the corresponding cloud service.

Important: The authentication request will be opened in a new tab / window on the browser, ensure that the pop-up tab / window is not blocked (e.g. pop-up blocker in your browser).

Click **Allow** to permit AhsayOBM to access the cloud storage.



Ahsay would like to:

View and manage the files in your Google Drive

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

Enter the authentication code returned in AhsayOBM to complete the destination setup.

NOTE: *A backup destination can be set to a supported cloud storage, backup server, FTP / SFTP server, network storage, or local / removable drive on your computer.*

Multiple backup destinations can be configured for a single backup set. In fact, it is recommended for you to setup at least 2 backup destinations for your backup set.

For more details on backup destination, for example which cloud service providers are supported, destination type, or limitation, you can refer to the following article: https://wiki.ahsay.com/doku.php?id=public:8002_faq:faq_on_backup_destination

Appendix D Uninstall AhsayOBM

Refer to the Appendix of the AhsayOBM Quick Start Guide for the corresponding operating system for details on how to uninstall AhsayOBM: https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

Appendix E ODBC Mode Authentication Method Permissions Check

There are two types of authentication method in ODBC backup mode; Trusted Authentication and MS SQL Authentication. The following procedures can help to determine:

1. If the login credentials used to authenticate a MS SQL Server database backup in ODBC backup mode has the correct permissions.
2. To obtain the size of the spooled database(s) in order to make sure the drive where the temporary folder is located has enough space to accommodate the spooling of the database(s) during backups.

Trusted Authentication

To verify if the login credentials for Trusted Authentication have the correct permissions to access and spool your MS SQL Server database(s) for a backup job, it is recommended to use the following command:

```
osql -E -Q "DECLARE @dbname char(64) SET @dbname = 'xxx' BACKUP DATABASE
@dbname TO DISK = '%temporary_path%\%database_name.txt' WITH SKIP"
```

NOTE:

1. %temporary_path% is the location of the temporary folder on the MS SQL Server backup set (e.g. E:\temp)
2. 'xxx' is the name of the database selected for backup

Example Scenario: Trusted Authentication using Windows User Account with Sufficient Permissions

1. Log in to Windows using a specific account (e.g. Administrator).
2. Open the command prompt.
3. Use the following osql command.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>osql -E -Q "DECLARE @dbname char(64) SET
@dbname = 'adventureworks2016' BACKUP DATABASE @dbname TO DISK
='E:\temp\adventureworks2016.bak' WITH SKIP"
Processed 26240 pages for database 'adventureworks2016
', file
'AdventureWorks2016_Data' on file 5.
Processed 2 pages for database 'adventureworks2016
', file
'AdventureWorks2016_Log' on file 5.
BACKUP DATABASE successfully processed 26242 pages in 14.397 seconds
(14.239 MB/sec).

C:\Users\Administrator>
```

On the example above,
@dbname = 'adventureworks2016'
'adventureworks2016' is the name of the database selected for backup
@dbname TO DISK ='E:\temp\adventureworks2016.bak'
'E:\temp' is the temporary folder of the MS SQL Server backup set

4. If the ‘adventureworks2016’ database is successfully saved to the temporary folder (E:\Temp), then it is verified that the account has the correct permissions. To check if the database is created successfully, and to obtain the size of the spooled database(s) in order to make sure the temporary drive has enough space to accommodate the spooling of the database files during backups, run the following command.

```
C:\Users\Administrator>dir E:\Temp
 Volume in drive E has no label.
 Volume Serial Number is 16F4-EB51
 Directory of E:\Temp
09/07/2020  11:18 AM    <DIR>          .
09/07/2020  11:18 AM    <DIR>          ..
09/07/2020  12:06 PM     1,075,228,160 adventureworks2016.bak
09/07/2020  11:18 AM       215,046,656 inventory.bak
09/04/2020  06:42 PM         4,024,832 master.bak
               3 File(s)  1,429,402,815 bytes
               2 Dir(s)  21,348,990,976 bytes free

C:\Users\Administrator>
```

Example Scenario: Trusted Authentication using Account with Incorrect Permissions

The following error message will be displayed when using a Windows login account which does not have the correct permissions to access the MS SQL database(s).

```
C:\Users\backup1>osql -E -Q "DECLARE @dbname char(64) SET @dbname =
'adventureworks2016' BACKUP DATABASE @dbname TO DISK
='E:\temp\adventureworks2016.bak' WITH SKIP"
[ODBC Driver 13 for SQL Server]Named Pipes Provider: Could not open
a connection to SQL Server [2].
Login failed for user 'W2K16-MSSQL2K16\backup1'.
[ODBC Driver 13 for SQL Server]A network-related or instance-
specific error
has occurred while establishing a connection to SQL Server. Server
is not
found or not accessible. Check if instance name is correct and if
SQL Server
is configured to allow remote connections. For more information see
SQL Server
Books Online.

C:\Users\backup1>
```

On the example above, the user ‘backup1’ does not have the correct permissions. Therefore, a MS SQL Server connection cannot be established.

MS SQL Authentication

To verify if the login credentials for MS SQL Authentication have the correct permissions to access and spool your MS SQL Server database(s) for a backup job, it is recommended to use the following command:

```
osql -U USERNAME -P PASSWORD -Q "DECLARE @dbname char(64) SET @dbname =
'xxx' BACKUP DATABASE @dbname TO DISK =
'%temporary_path%\%database_name.txt' WITH SKIP"
```

NOTE:

1. %temporary_path% is the location of the temporary folder on the MS SQL Server backup set (e.g. E:\temp)
2. 'xxx' is the name of the database selected for backup
3. USERNAME is the username of the MS SQL Server account
4. PASSWORD is the password of the MS SQL Server account

Example Scenario: MS SQL Authentication using Account with Sufficient Permissions

1. Log in to Windows using a specific account (e.g. Administrator).
2. Open the command prompt.
3. Use the following osql command.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>osql -U sa -P abc123$% -Q "DECLARE @dbname
char(64) SET @dbname = 'master' BACKUP DATABASE @dbname TO DISK =
'E:\temp\master.bak' WITH SKIP"

Processed 480 pages for database 'master
', file 'master' on

file 2.

Processed 3 pages for database 'master
', file 'mastlog' on

file 2.

BACKUP DATABASE successfully processed 483 pages in 0.785 seconds
(4.802 MB/sec).

C:\Users\Administrator>
```

On the example above,
osql -U sa
'sa' is the default username of the MS SQL Server account
-P abc123$%
'abc123$%' is the password of the MS SQL Server account
@dbname = 'master'
'master' is the name of the database selected for backup
@dbname TO DISK = 'E:\temp\master.bak'
'E:\temp' is the temporary folder of the MS SQL Server backup set

4. If the "master" database is successfully saved to the temporary folder (E:\Temp), then it is verified that the account has the correct permissions. To check if the database is created successfully, and to obtain the size of the spooled database(s) in order to make sure the temporary drive has enough space to accommodate the spooling of the database files during backups, run the following command.

```
C:\Users\Administrator>dir E:\Temp
 Volume in drive E has no label.
 Volume Serial Number is 16F4-EB51
 Directory of E:\Temp
09/07/2020  11:18 AM    <DIR>          .
09/07/2020  11:18 AM    <DIR>          ..
09/07/2020  12:06 PM     1,075,228,160 adventureworks2016.bak
```

```
09/07/2020  11:18 AM       215,046,656 inventory.bak
09/04/2020  06:42 PM         4,024,832 master.bak
               3 File(s)  1,429,402,815 bytes
               2 Dir(s)  21,348,990,976 bytes free

C:\Users\Administrator>
```

Example Scenario: MS SQL Authentication using Account with Incorrect Permissions

The following error message will be displayed when using a MS SQL account which does not have the correct permissions to access the MS SQL database(s).

```
C:\Users\Administrator>osql -U mssql1 -P abc123$% -Q "DECLARE
@dbname char(64) SET @dbname = 'master' BACKUP DATABASE @dbname TO
DISK = 'E:\temp\master.bak' WITH SKIP"
[ODBC Driver 13 for SQL Server]Named Pipes Provider: Could not open
a connection to SQL Server [2].
Login failed for user 'mssql1'.
[ODBC Driver 13 for SQL Server]A network-related or instance-
specific error
has occurred while establishing a connection to SQL Server. Server
is not
found or not accessible. Check if instance name is correct and if
SQL Server
is configured to allow remote connections. For more information see
SQL Server
Books Online.

C:\Users\Administrator>
```

On the example above, ‘mssql1’ is the username of the MS SQL Server account which does not have the correct permissions. Therefore, a MS SQL Server connection cannot be established.