

# RDS with automated backups of SQL Workloads

## Prepared for

Service Providers

## Prepared by

Manish Dhall – Cloud Solutions Strategist  
Microsoft OCP

People Tech Group (SI Partner)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2013 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Revision and Signoff Sheet

## Change Record

Date	Author	Version	Change Reference
March 16, 2018	Manish Dhall	1.0	Initial draft for review/discussion

## Reviewers

Name	Version Approved	Position	Date

# Table of Contents

Introduction .....	5
Purpose.....	5
Prerequisites .....	5
Deployment Steps .....	6

# Introduction

Azure Backup Server can protect application workloads such as Hyper-V VMs, Microsoft SQL Server, SharePoint Server, Microsoft Exchange, and Windows clients from a single console. We can also protect Infrastructure as a Service (IaaS) workloads, like VMs in Azure.

Azure Backup Server inherits much of the workload backup functionality from Data Protection Manager (DPM).

## Purpose

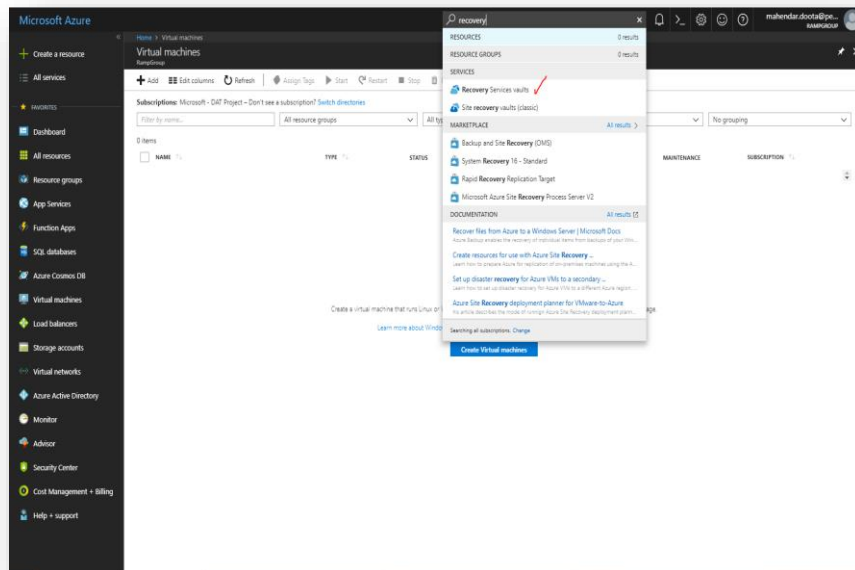
This document describes basic backup and restore terms and introduces backup and restore strategies for SQL Server and security considerations for SQL Server backup and restore.

## Prerequisites

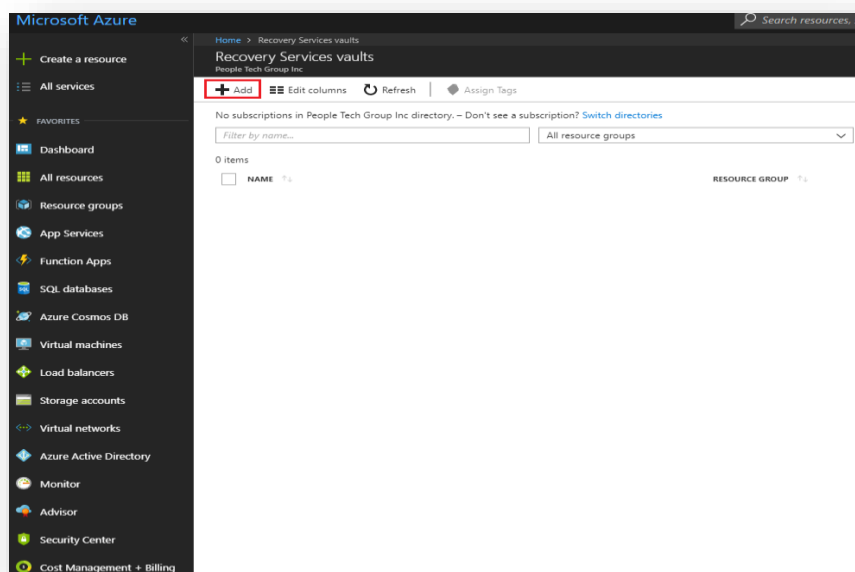
- A VM running with SQL Server 2016 SP1 Standard on Windows Server 2016

# Deployment Steps

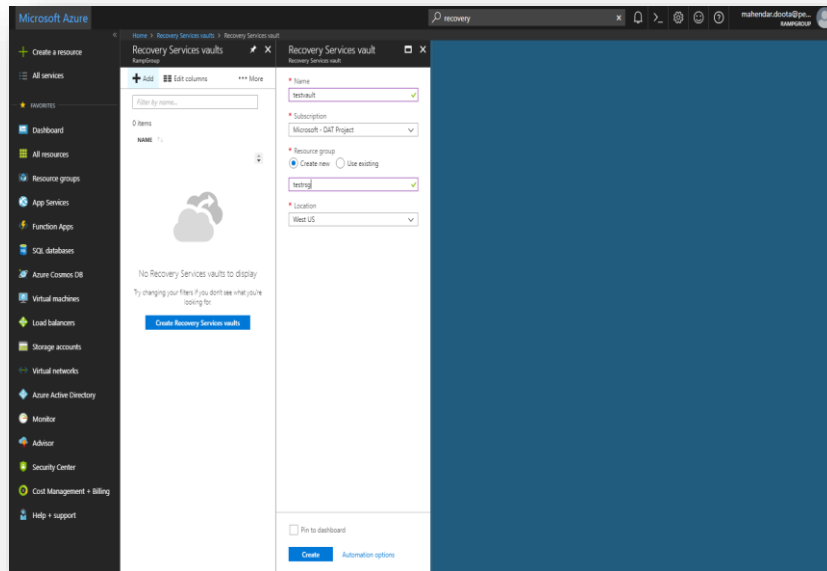
1. Login to the Azure portal.
2. On the **Hub** menu, click **Browse** and in the list of resources, type **Recovery Services**. As you begin typing, the list filters based on your input. Click **Recovery Services vault**



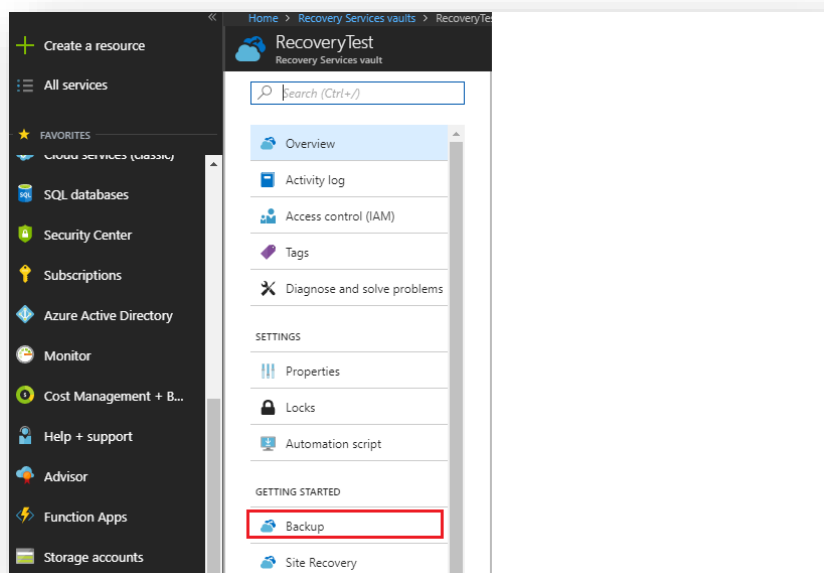
3. On the **Recovery Services vaults** menu, click **Add**



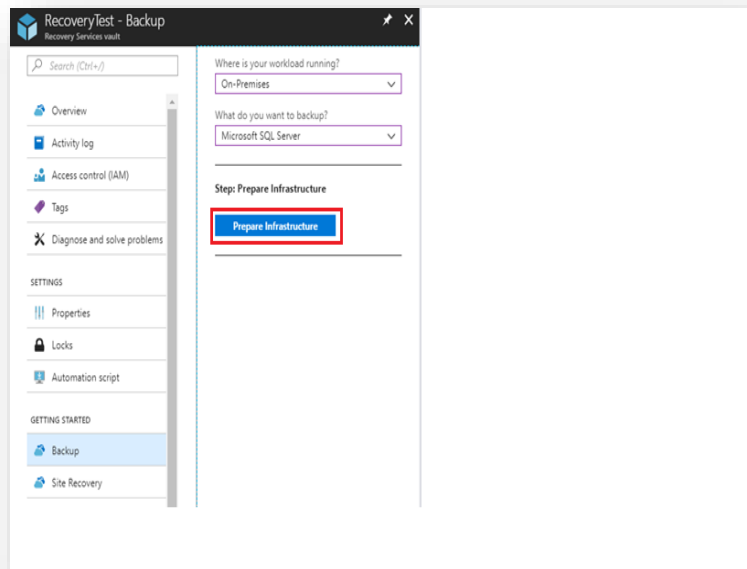
4. The **Recovery Services** vault blade opens, prompting you to specify a **Name**, **Subscription**, **Resource group**, and **Location**
5. Click **Create**



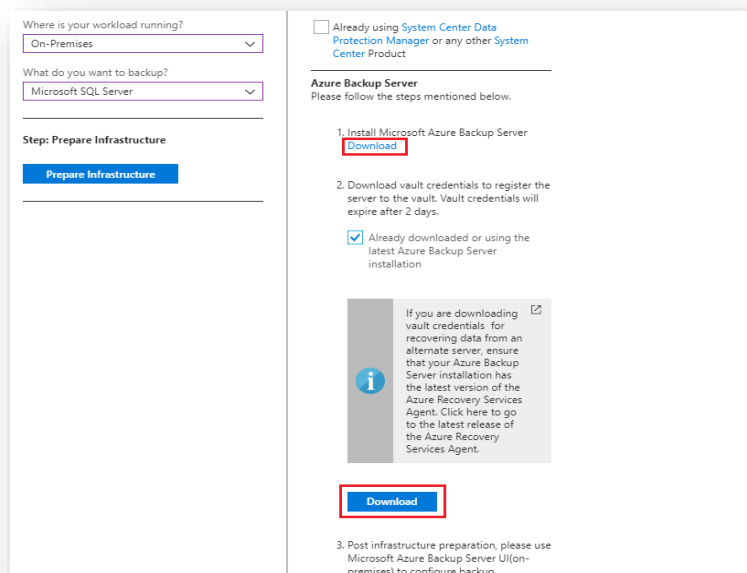
6. Specify **Recovery Services vaults**, then click **Backup**



7. Specify On-Premises and Microsoft SQL Server
8. Click Prepare Infrastructure



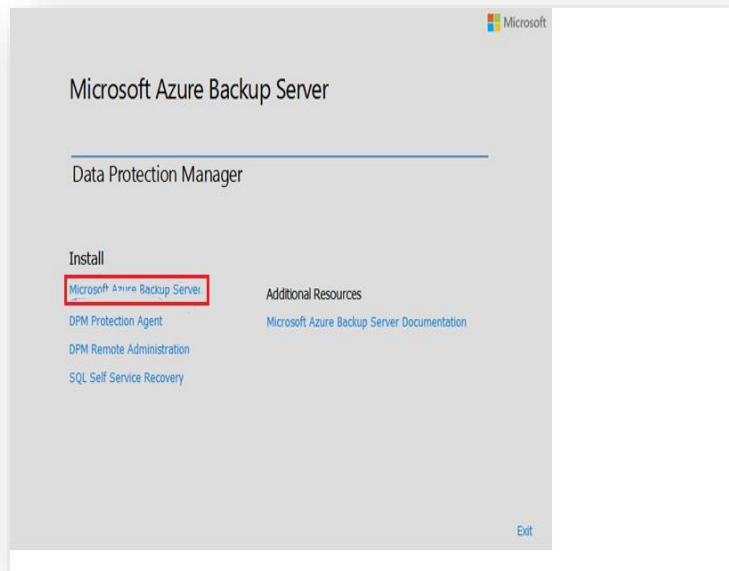
9. Download Install Microsoft Azure Backup Server



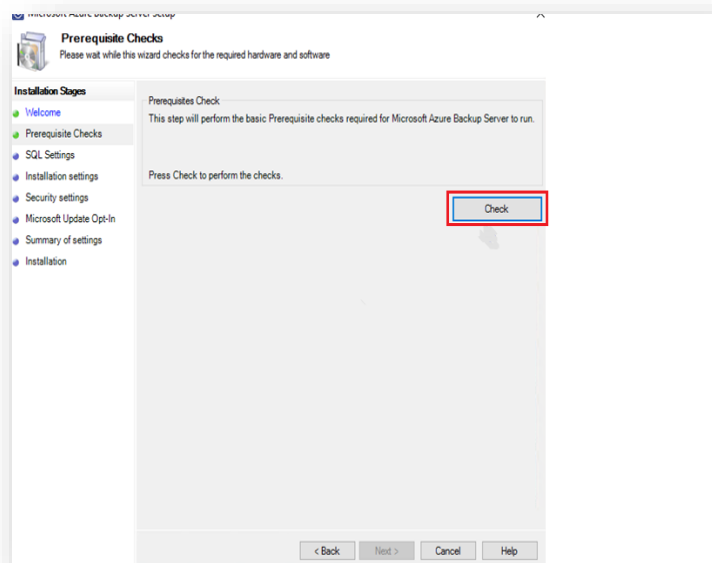
10. Download the **Credentials** file to the SQL Server, this will be used in the setup process
11. Login to SQL Server and copy the download files to Server along with the Credentials file
12. Run the installer



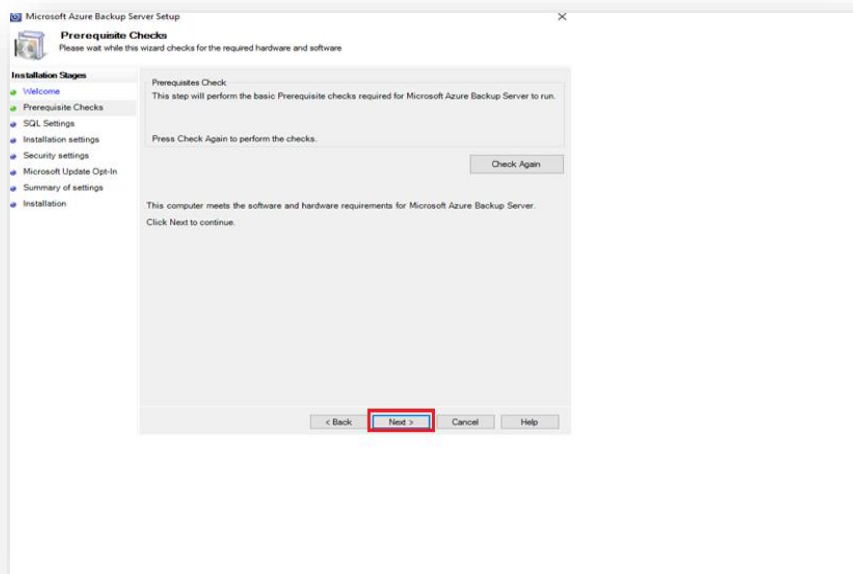
13. Click **MicrosoftAzureBackupInstaller.exe**. This will launch the **Microsoft Azure Backup Server Setup Wizard** to extract the setup files to a specified location



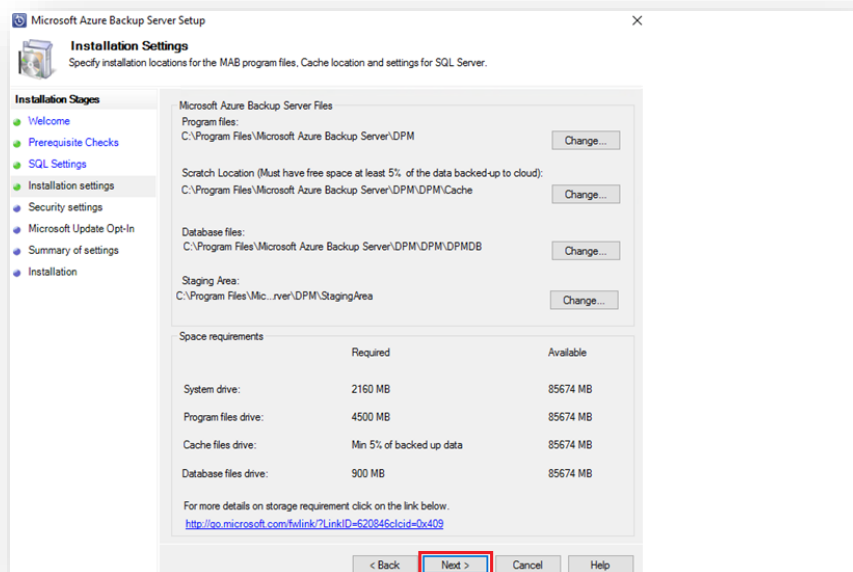
14. Continue through the wizard and click on the **Extract** button to begin the extraction process
15. Once the extraction process completes, check the box to launch the extracted **setup.exe** to begin installing **Microsoft Azure Backup Server**, then click on the **Finish** button
16. Click on **Microsoft Azure Backup**
17. Click **Next**
18. Click **Check**



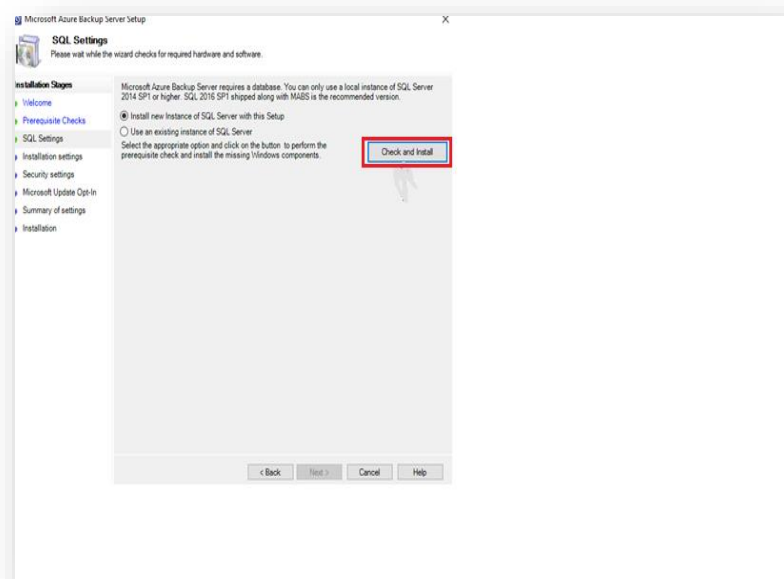
19. Click **Next**



20. Click **Next**

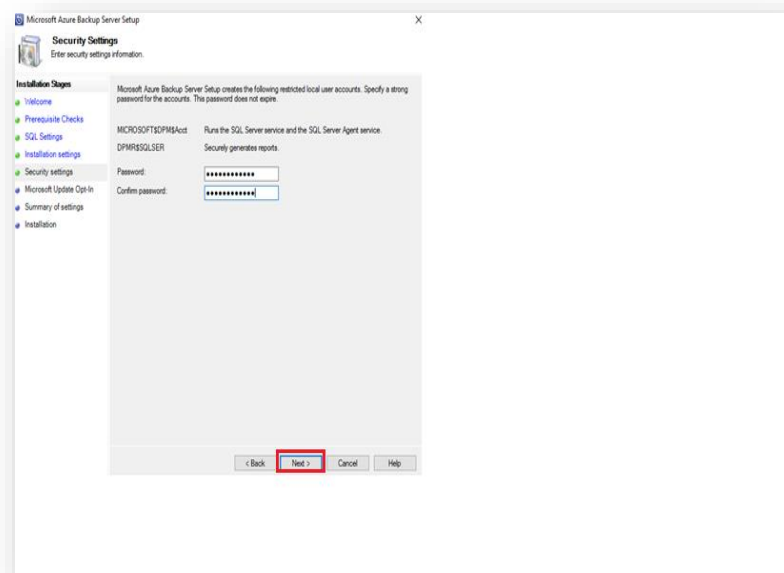


21. Select **Install New Instance of SQL Server with this Setup**, then click the **Check and Install** button

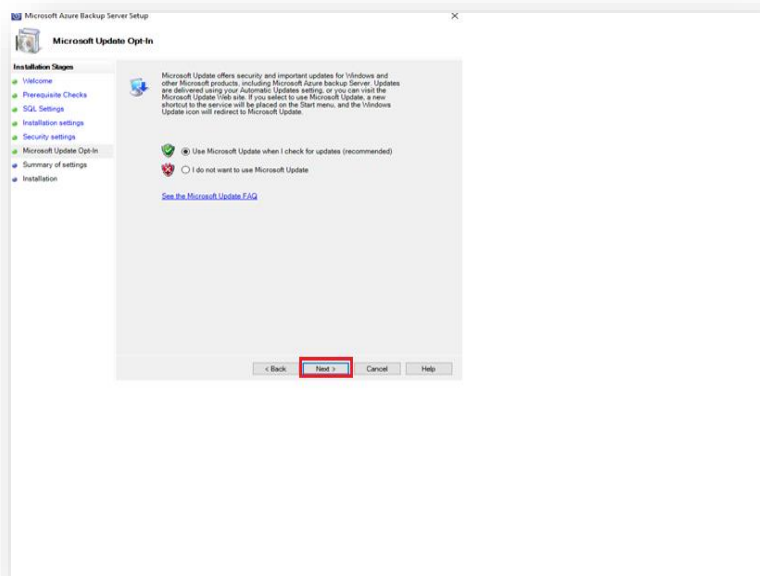


**NOTE:** In case a warning about restart of the machine is notified, please restart the machine and go to the C: drive, click **Microsoft Azure Backup Server**, and then **Run the Setup as Administrator**

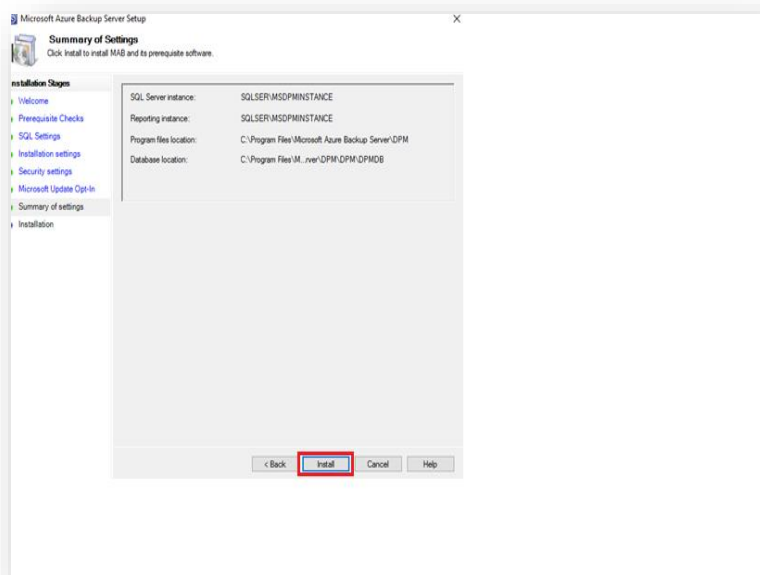
22. Specify a **password**



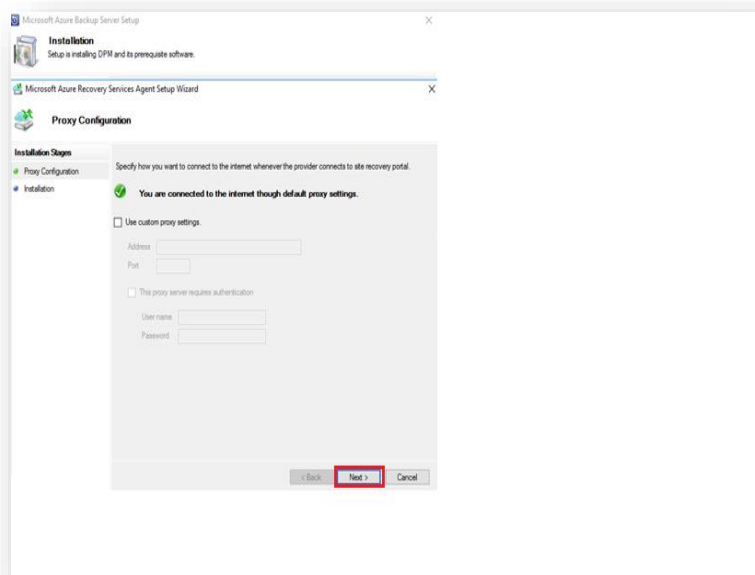
## 23. Click Next



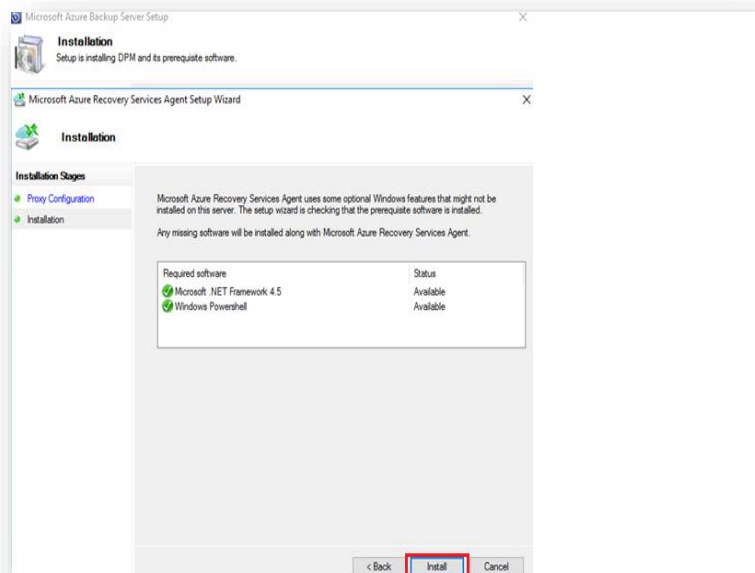
## 24. Click Install



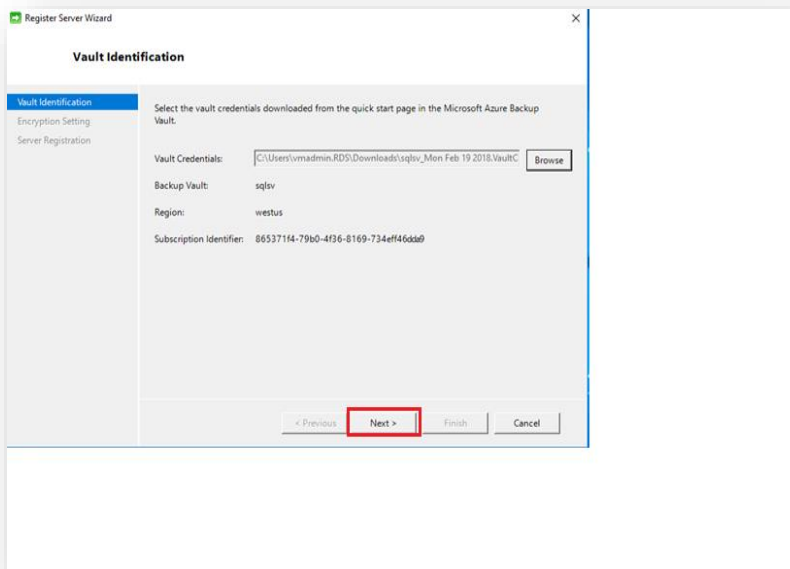
25. Click Next



26. Click Install



27. Specify Azure backup credentials, then click **Next**

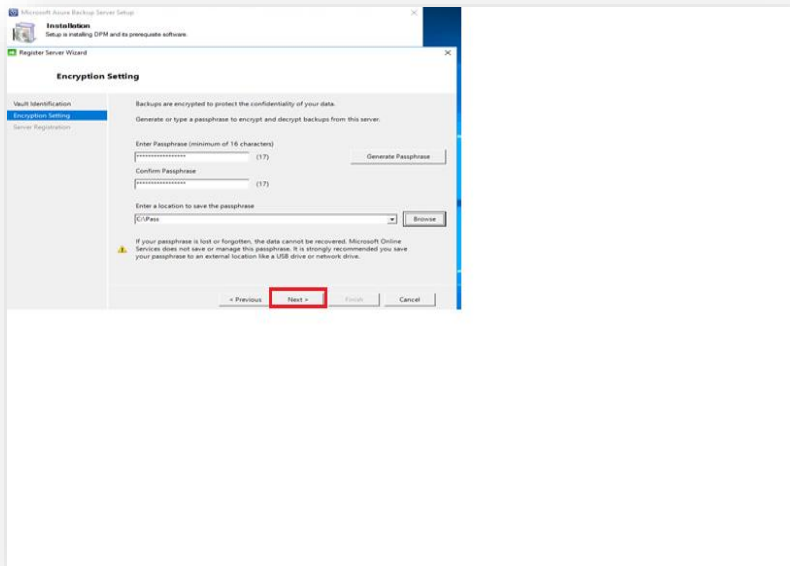


The screenshot shows the 'Register Server Wizard' window, specifically the 'Vault Identification' step. The left sidebar has three tabs: 'Vault Identification' (selected), 'Encryption Setting', and 'Server Registration'. The main area contains the following fields and text:

- Text: "Select the vault credentials downloaded from the quick start page in the Microsoft Azure Backup Vault."
- Field: "Vault Credentials:" with a text box containing "C:\Users\vmadmin.RDS\Downloads\sqlsv\_Mon Feb 19 2018\VaultC" and a "Browse" button.
- Field: "Backup Vault:" with a text box containing "sqlsv".
- Field: "Region:" with a text box containing "westus".
- Field: "Subscription Identifier:" with a text box containing "86537154-79b0-4f36-b169-734eff46dda9".

At the bottom, there are four buttons: "< Previous", "Next >" (highlighted with a red box), "Finish", and "Cancel".

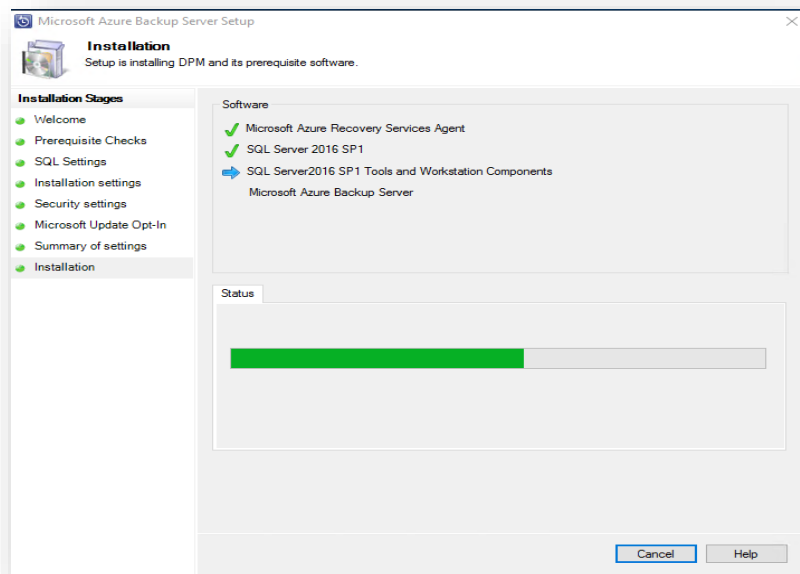
28. Specify a new password, then click **Next**



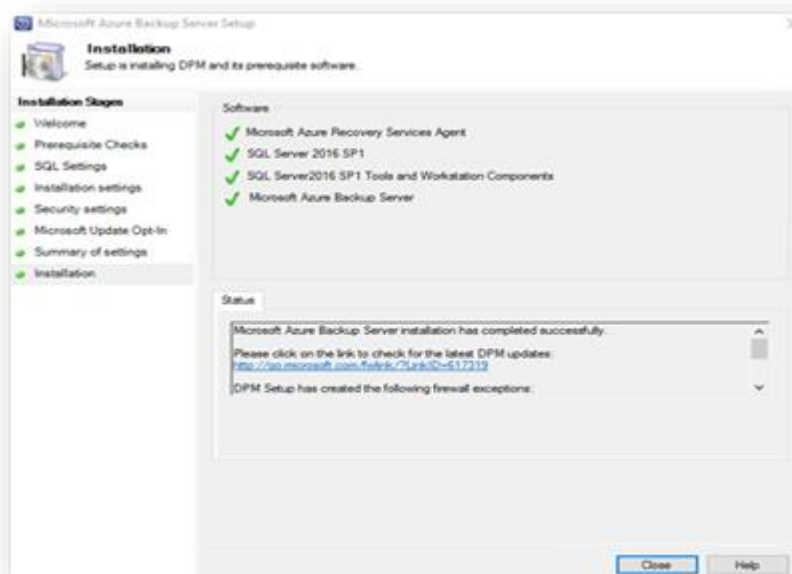
The screenshot shows the 'Register Server Wizard' window, specifically the 'Encryption Setting' step. The left sidebar has three tabs: 'Vault Identification', 'Encryption Setting' (selected), and 'Server Registration'. The main area contains the following fields and text:

- Text: "Backups are encrypted to protect the confidentiality of your data. Generate or type a passphrase to encrypt and decrypt backups from this server."
- Field: "Enter Passphrase (minimum of 16 characters)" with a text box containing "\*\*\*\*\*" and a "Generate Passphrase" button.
- Field: "Confirm Passphrase" with a text box containing "\*\*\*\*\*".
- Field: "Enter a location to save the passphrase" with a text box containing "C:\Users" and a "Browse" button.

At the bottom, there are four buttons: "< Previous", "Next >" (highlighted with a red box), "Finish", and "Cancel".

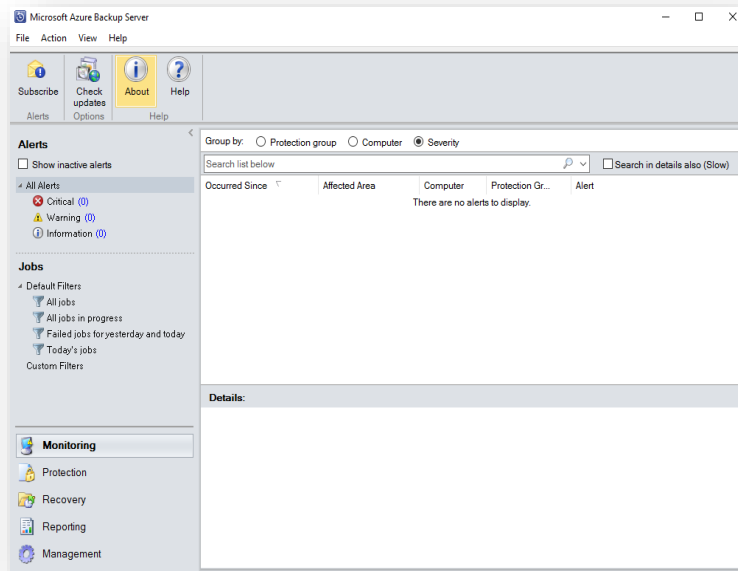


29. When the installation completes, click **Close**

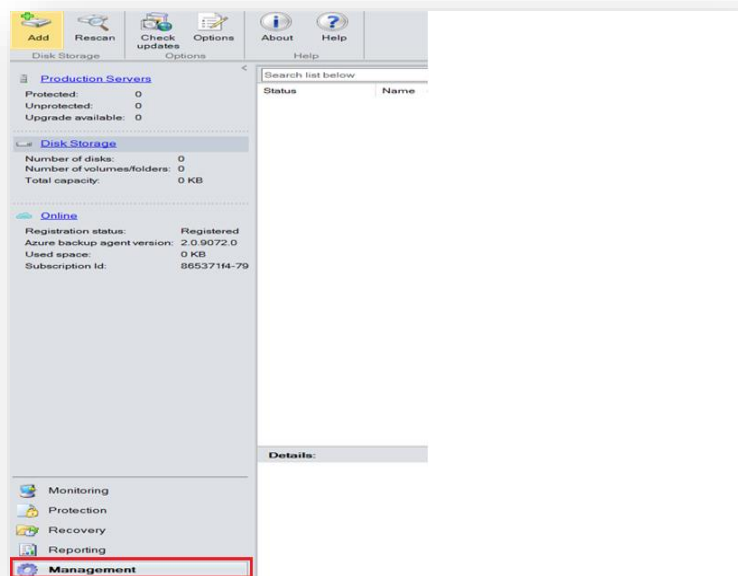


## Create a backup policy to protect SQL Server databases to Azure

1. On the Microsoft Azure Backup Server, click Management

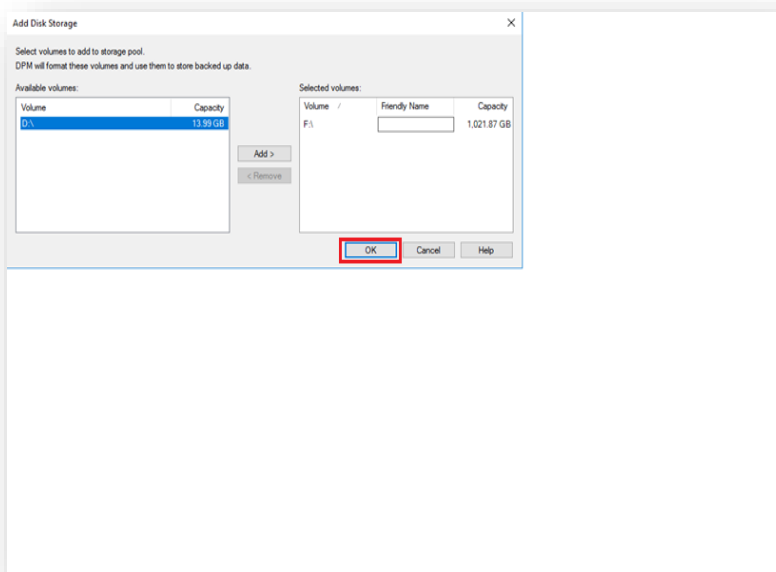


2. Click Disk Storage, then Add

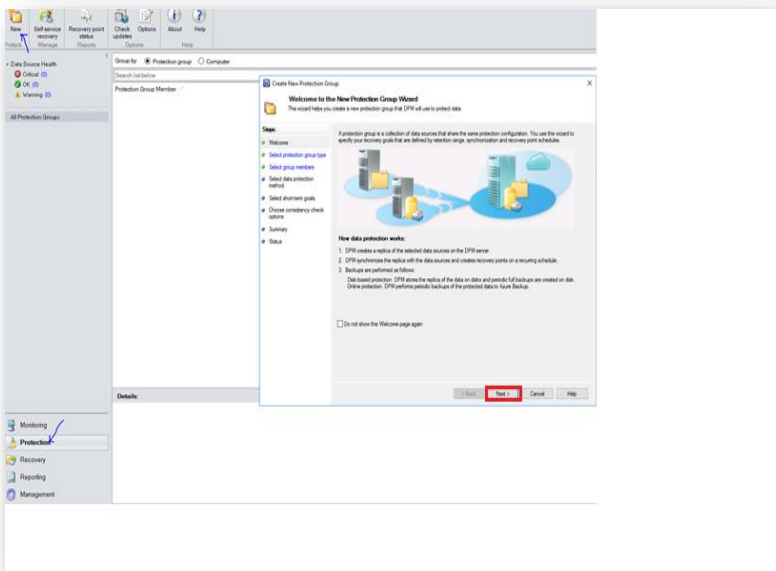




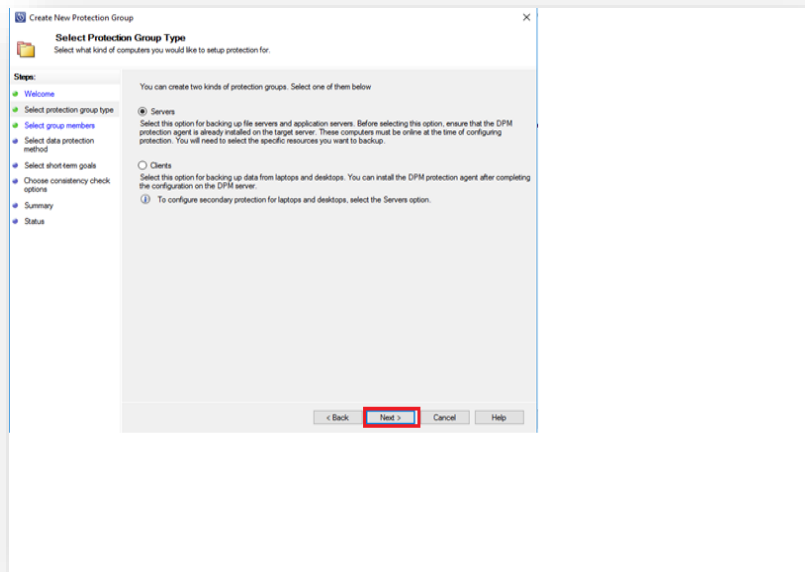
- Specify a new free disk to add, then click **OK**



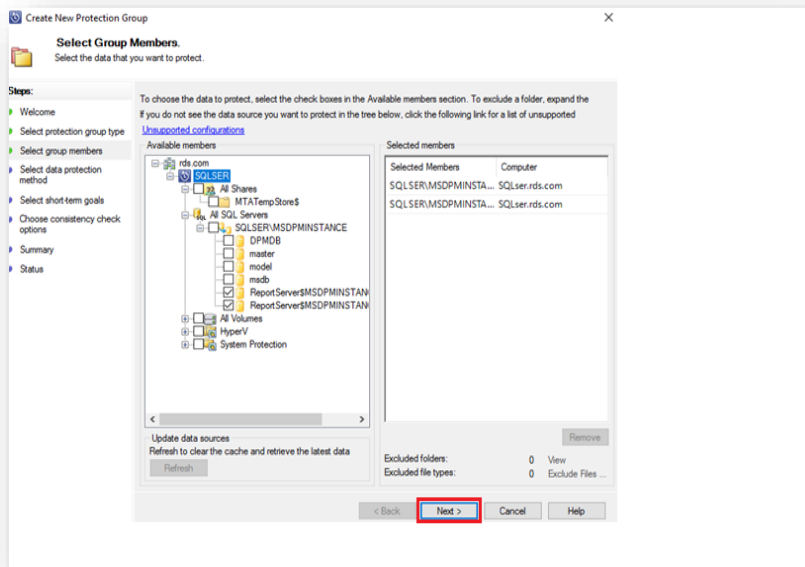
- Specify **Protection Type** and select **Add**, then click **Next**



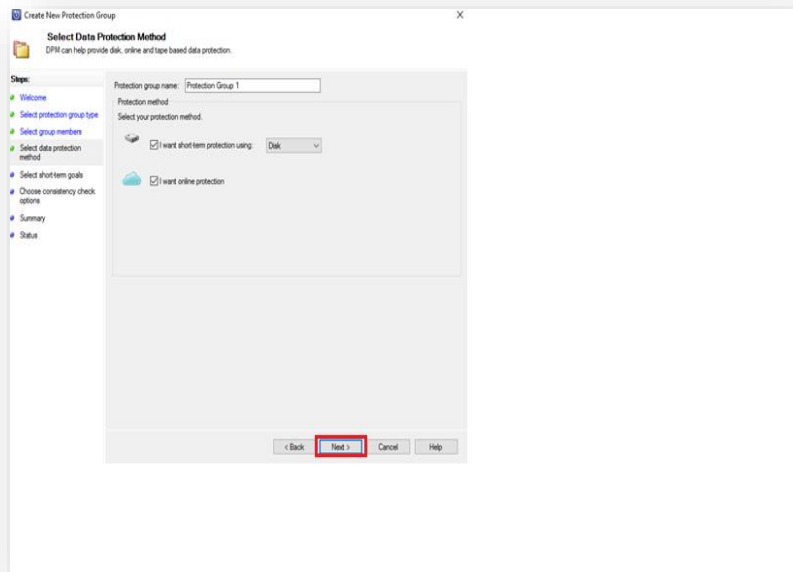
5. Click Next



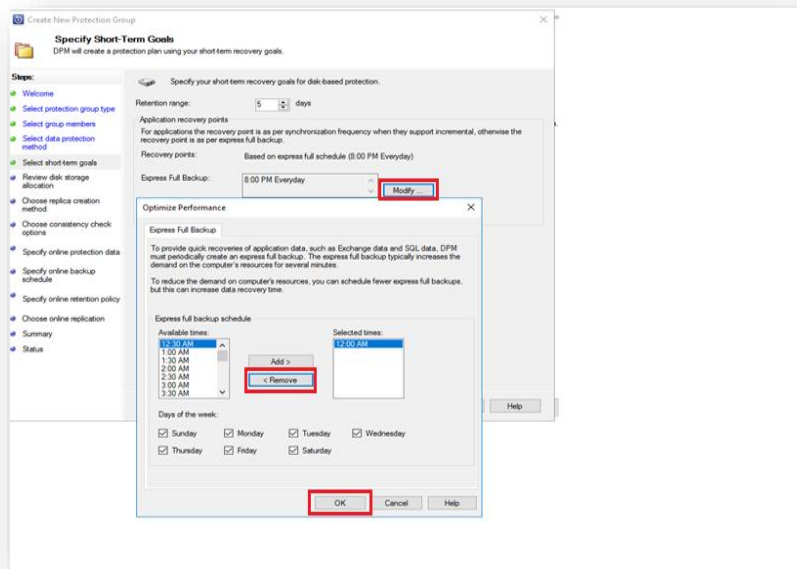
6. Expand the All SQL Shares and select the databases

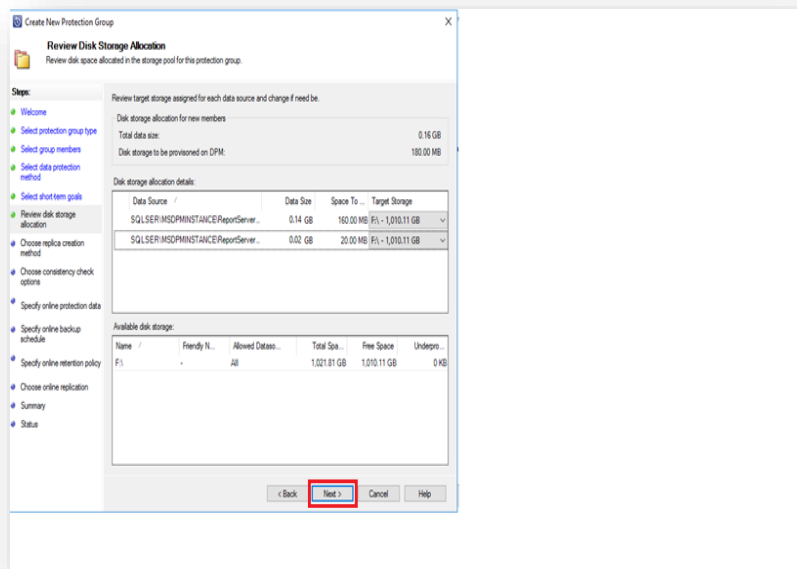


7. Specify a name for the Protection group, then click **Next**

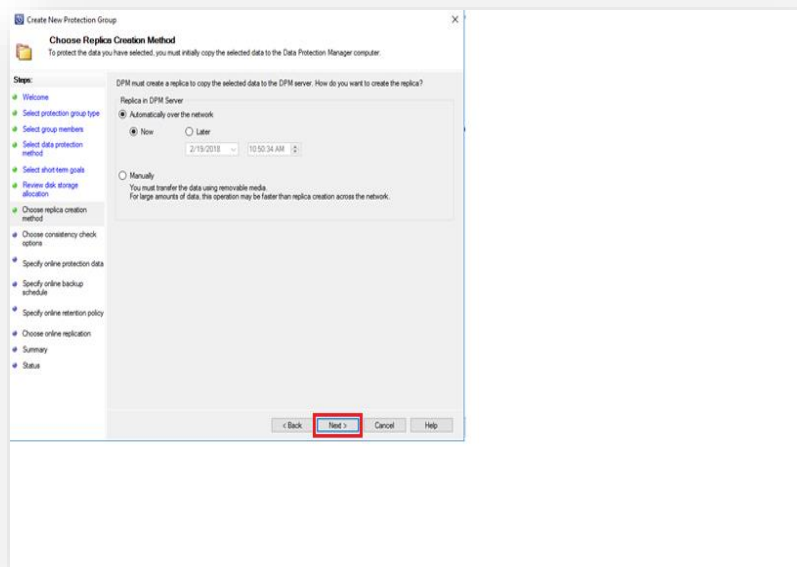


8. Enable Retention range and Express Full Backup, then click **OK**

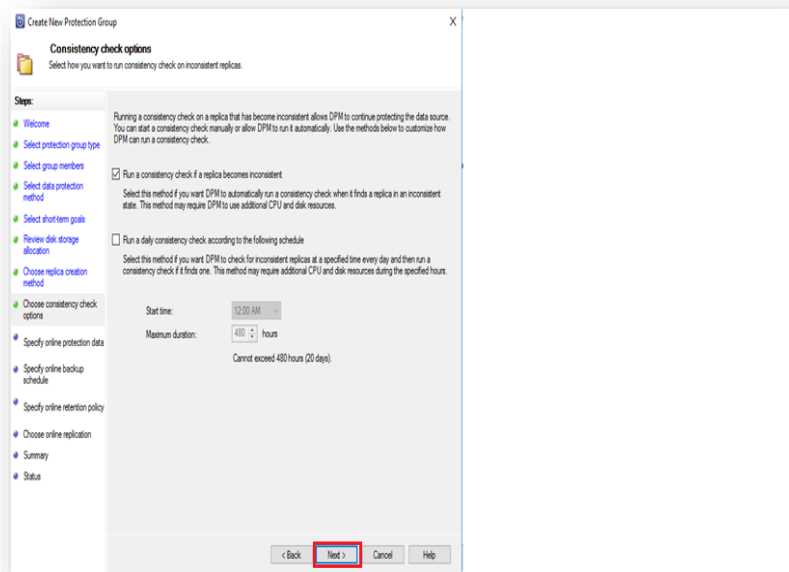




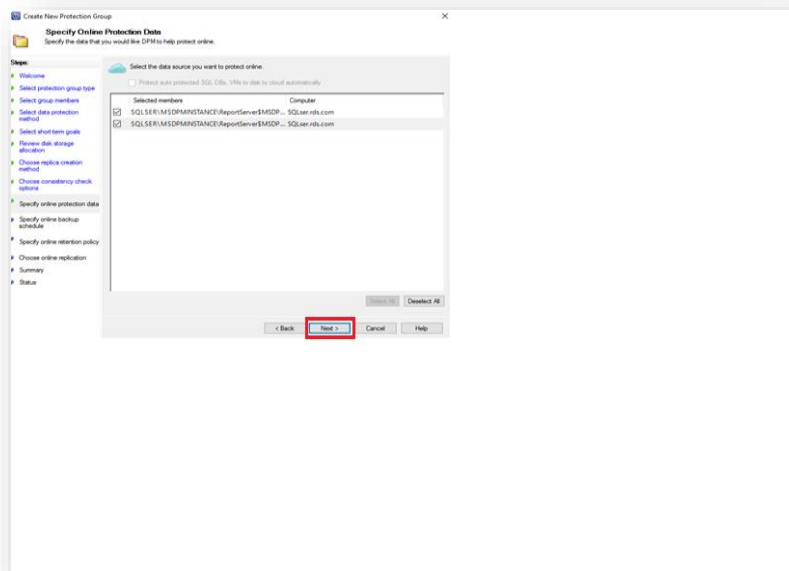
9. Click Next



10. Click Next



11. Specify Databases, then click Next



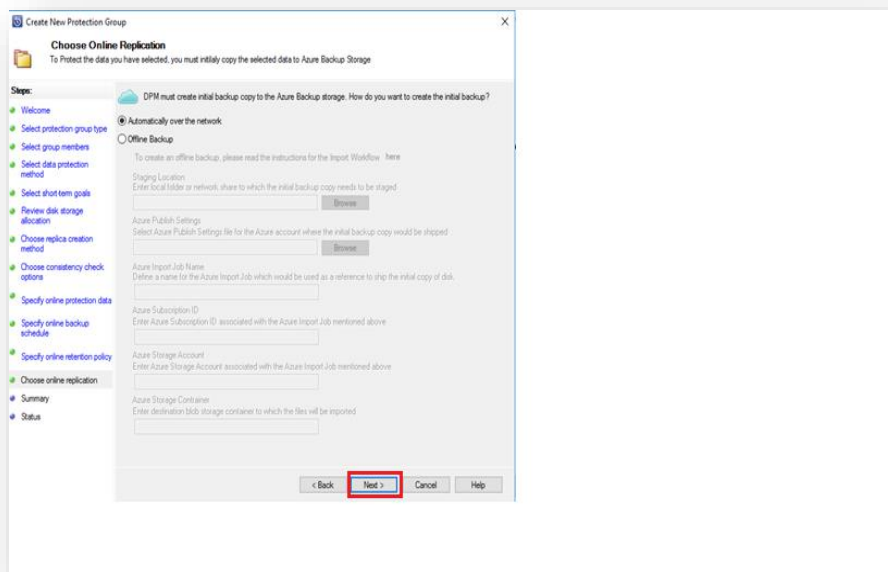
12. Specify the Backup Schedule, then click Next

The screenshot shows the 'Specify Online Backup Schedule' step in the 'Create New Protection Group' wizard. The left sidebar lists the steps: Welcome, Select protection group type, Select group members, Select data protection method, Select short term goals, Review disk storage allocation, Choose replica creation method, Choose consistency check options, Specify online protection data, Specify online backup schedule (current step), Specify online retention policy, Choose online replication, Summary, and Status. The main area is titled 'Specify Online Backup Schedule' and 'Specify online backup schedule which DPM will use to generate your protection plan'. It contains a 'Schedule a backup every' section with radio buttons for Day, Week, Month, and Year. The 'Day' option is selected. Below this, it says 'At following times (Maximum allowed is two times a day)' with a dropdown menu showing '12:00 AM' and a 'None' button. A note at the bottom states: 'DPM will create an online recovery point using the latest DPM replica on disk. No new data will be transferred from the protected computers. If you would like DPM to help protect the latest computer data online, please create a new recovery point on disk before creating an online recovery point.' At the bottom right, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a red rectangle.

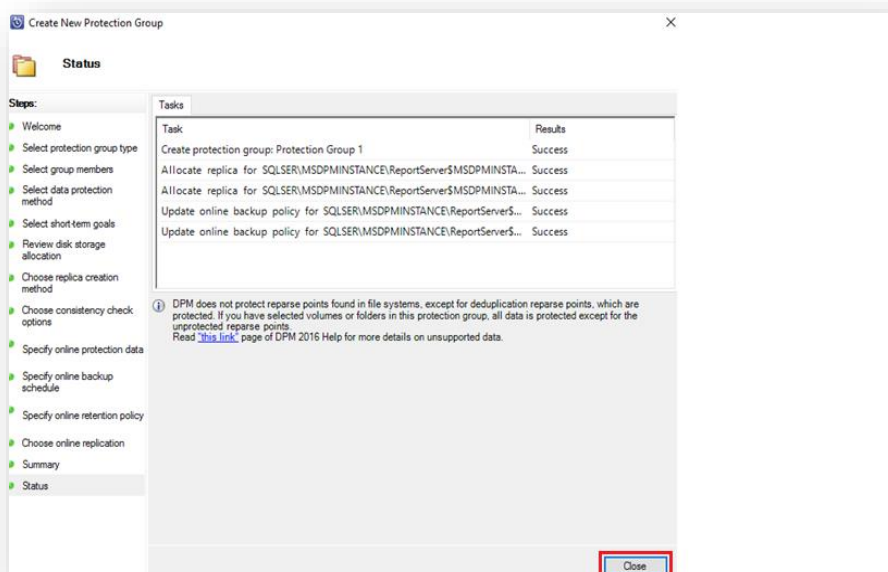
13. Specify the Schedule retention policy, then click Next

The screenshot shows the 'Specify Online Retention Policy' step in the 'Create New Protection Group' wizard. The left sidebar is the same as in the previous screenshot. The main area is titled 'Specify Online Retention Policy' and 'Specify the retention policy which DPM will use to generate your protection plan'. It contains four sections: 'Daily Retention Policy' (Retain backup copies taken on at 12:00 AM for 30 Days), 'Weekly Retention Policy' (Retain backup on Saturday at 12:00 AM for 104 Weeks), 'Monthly Retention Policy' (Retain backup on Last Saturday at 12:00 AM for 60 Months), and 'Yearly Retention Policy' (Retain backup on Last Saturday of March at 12:00 AM for 10 Years). Each section has a 'Modify' button. At the bottom right, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a red rectangle.

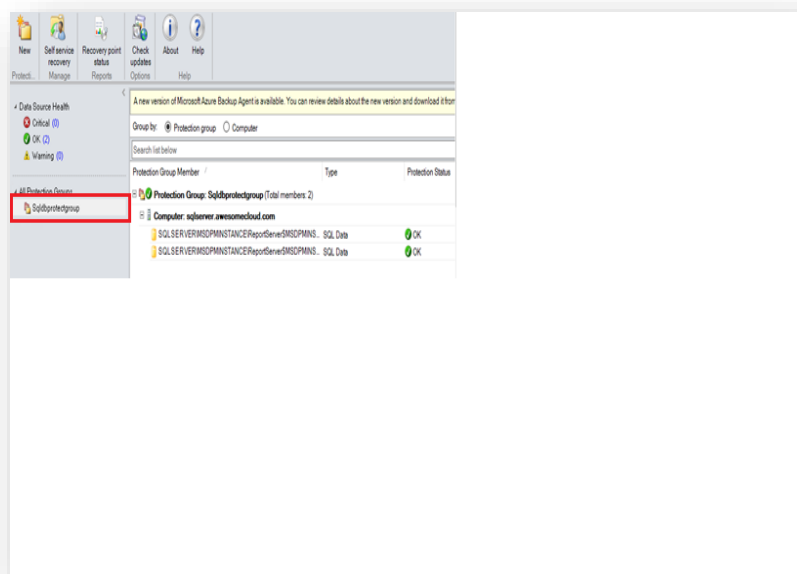
14. Specify **Automatically over the Network**, then click **Next**



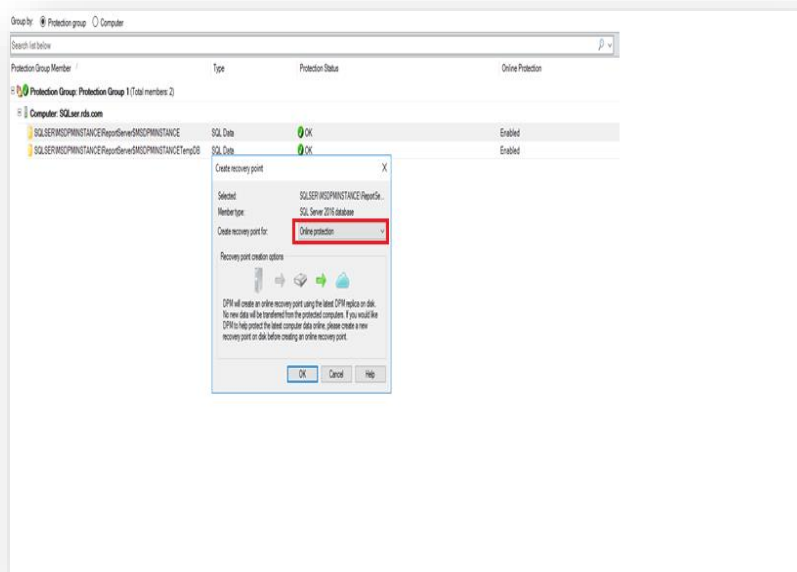
15. Click **Create group**, then click **Close**



16. Specify the **Protection Group**, then select **database**

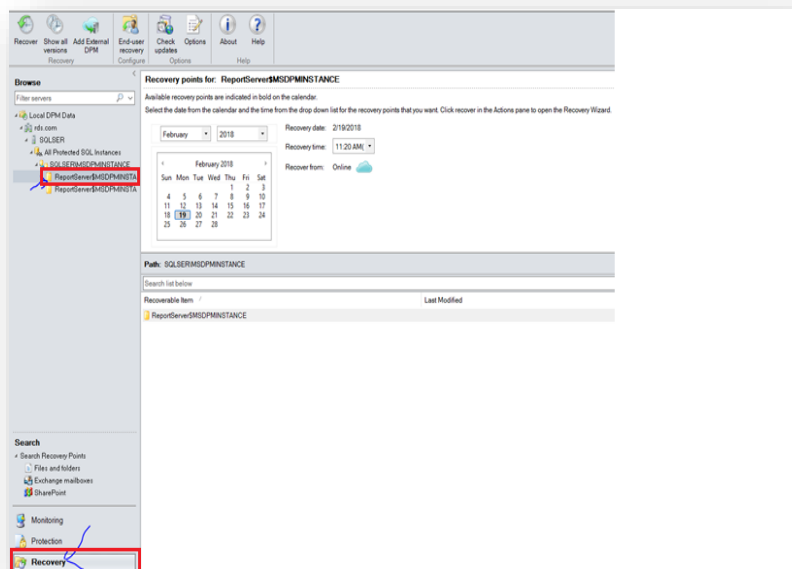


17. Right-click the database and select **Create Recovery Point**, then select online protection

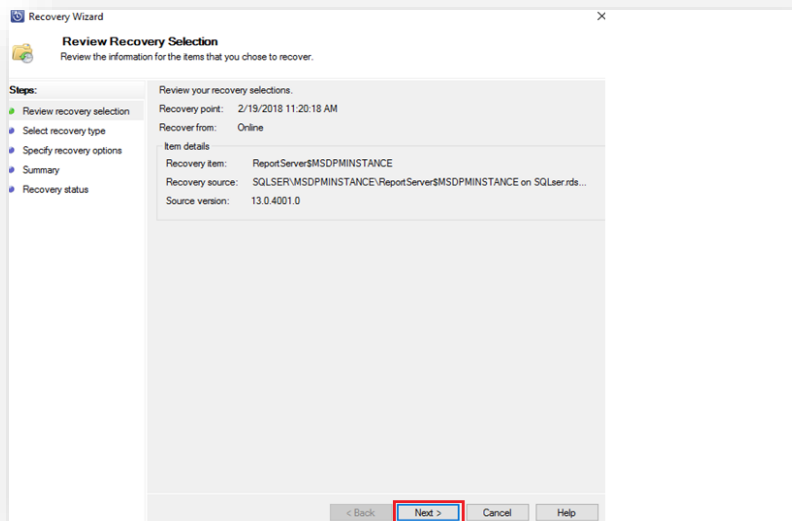




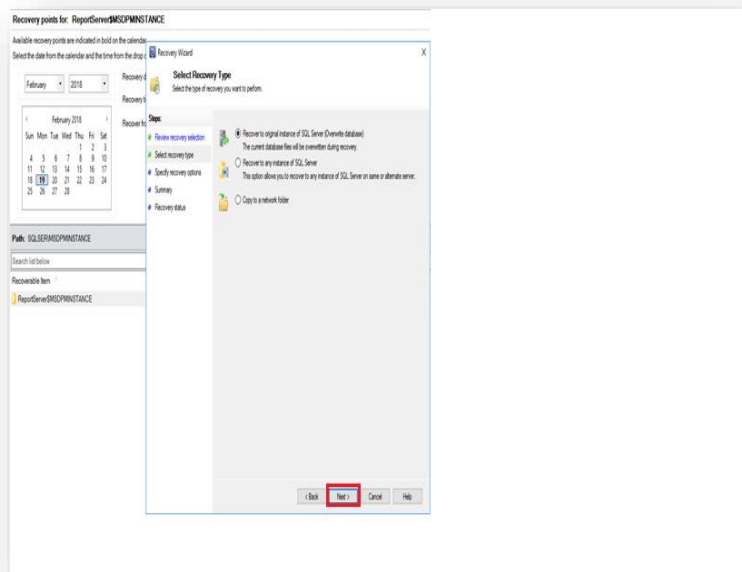
18. Select **Recovery** option, then click **Recovery point**



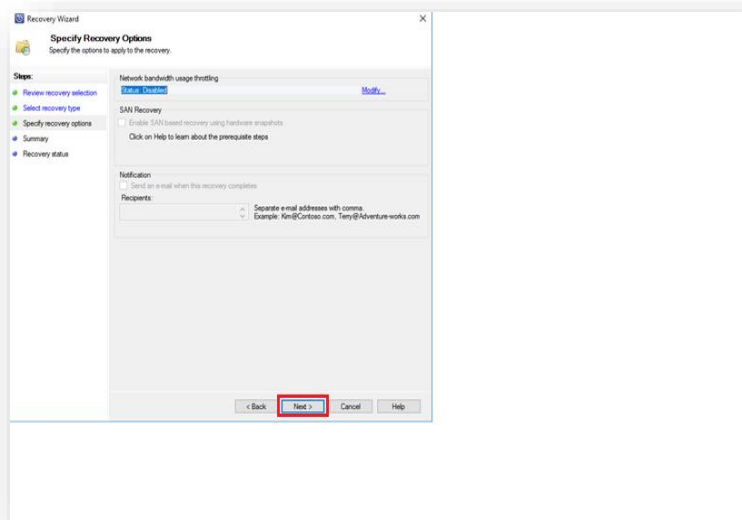
19. Right-click the database name, click **Recovery**, then click **Next** and **Create**



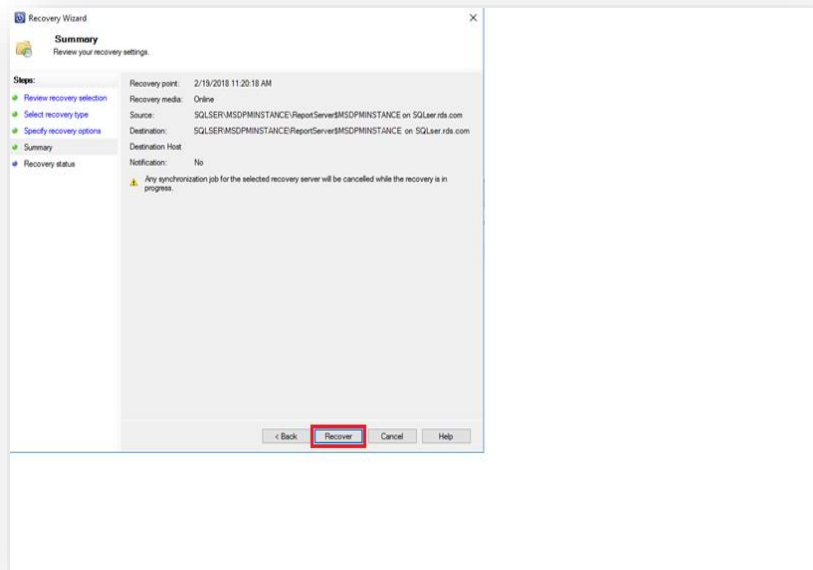
20. Select the recovery type: **Recover to original instance of SQL Server**, then click **Next**



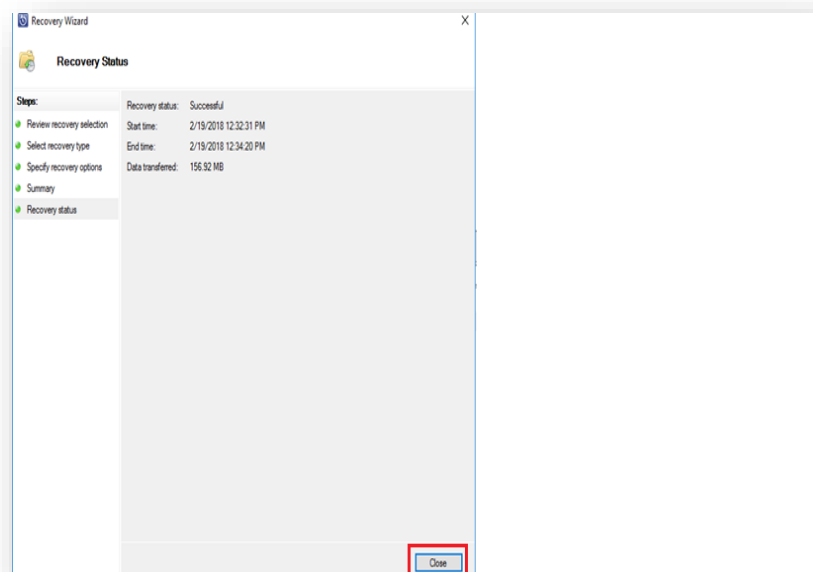
21. Click **Next**



## 22. Click Recover



## 23. Click Close



## References

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup>