

# Always Take Backup of Backup

PCbots Labs

## **AZURE BACKUP NOTES FROM THE FIELD VLADIMIR STEFANOVIC**



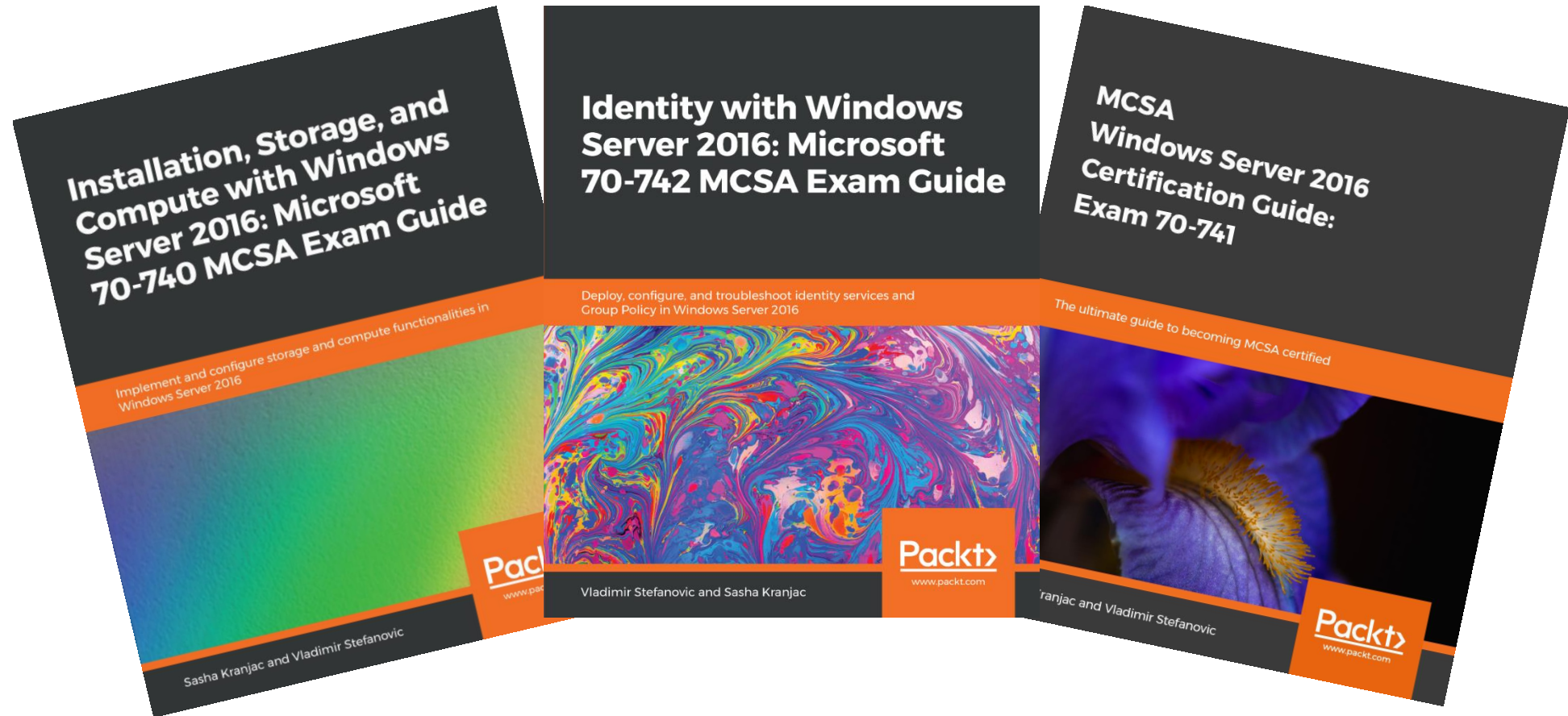
# WHO AM I

---

- Vladimir Stefanović
- System Engineer, 10+ years of experience
- MCT, MCSE: Cloud Infrastructure, MCSA: Office365, Azure Administrator & Azure Architecting, CompTIA Security & Network
- Book author, conference speaker, technical trainer and Azure UG Leader



# MY BOOKS – MCSA 2016 EXAM GUIDE



# WHERE I AM FROM (1) ...

- Serbia, small Balkan country and that was a long flight

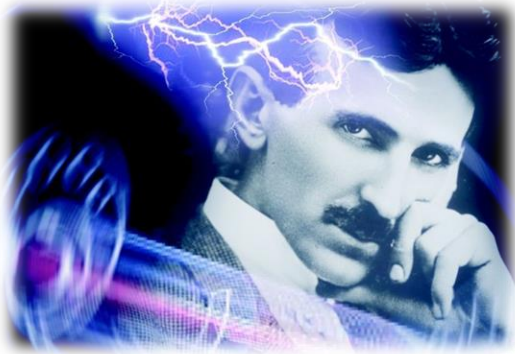




# WHERE I AM FROM (2) ...

---

- Country of brilliant minds ...



- and famous sportists



# AGENDA

---

- Azure Backup features
- Azure Backup components
- Backup Azure workload – Azure VM and Azure File Share
- On-premise backup with Azure Backup
- Demo – Azure workload
- Demo - On-premise workload

# AZURE BACKUP FEATURES

---

- Microsoft implementation of cloud backup solution
- Azure Backup features
  - *There is no cost for using on-premises storage \**
  - *There are no maintenance or monitoring. Azure Backup is PaaS \**
  - *Multiple storage options are supported (LRS, GRS)*
  - *Azure Backup doesn't limit or charge for the amount of data you transfer, except if you use the Import/Export service to import large amounts of data*
  - *Data encryption securely transmit and store your data in the public cloud*
  - *Application-consistent backup guarantee you that a recovery point has all required data to restore the backup copy*
  - *Azure Backup has a limit of 9999 recovery points per protected instance*

# AZURE BACKUP COMPONENTS (1)

---

- Azure Backup (MARS) agent
  - *Backup files, folders and System State on Windows OS*
  - *Max 3x per day*
  - *No Linux support, no application-aware support*
- System Center DPM
  - *Application-aware backup and granular restore*
  - *Back up and restore VMware VMs using DPM 2012 R2*
  - *Linux support on Hyper-V and VMware VMs*
  - *Cannot backup Oracle databases*



# AZURE BACKUP COMPONENTS (2)

---

- Azure Backup Server (System Center DPM with limited features)
  - *Application-aware backup and granular restore*
  - *Back up and restore VMware VMs*
  - *Linux support on Hyper-V and VMware VMs*
  - *Doesn't require a System Center license, but requires live Azure subscription*
  - *No support for tape backup, no support for Oracle databases*
- Azure IaaS VM backup
  - *Application-aware backup*
  - *Native backups for Windows/Linux*
  - *No agent installation required, no backup infrastructure needed*

# BACKUP AZURE WORKLOAD – AZURE VM

---

- What you need before start
  - *Azure virtual machines*
  - *Recovery services vault*
- What can be backed up
  - *Azure VMs, Windows and Linux*
  - *Azure SQL VM (preview)*
- What can be restored
  - *Complete virtual machine*
  - *Virtual machine disk(s)*
  - *Files from virtual machine*

# BACKUP AZURE WORKLOAD – AZURE FILES

---

- RA-GRS Azure file shares cannot be protected
- Azure file shares that have Virtual Networks or Firewall enabled cannot be protected
- Scheduled backups is limited to 1x per day, on-demand 4x per day
- Do not delete snapshots created by Azure Backup. Deleting snapshots can result in loss of recovery points
- Do not delete file shares that are protected by Azure Backup. The current solution will delete all snapshots taken by Azure Backup once the file share is deleted and hence lose all restore points

# ON-PREMISE BACKUP WITH AZURE BACKUP

---

- Azure backup can be used for on-premise backup
  - *Hyper-V environment*
  - *Vmware environment*
  - *Single physical or virtual machine using agent*
- For virtualized environment (Hyper-V and Vmware), you need:
  - *Valid Azure subscription and Recovery Services vault*
  - *Domain environment*
  - *System Center DPM or Azure Backup Server (DPM with limited features)*
  - *Enough storage for backup on local disks (1.5x of data size)*

# AZURE BACKUP SERVER V3

---

- Prerequisites
  - **Supported OS:** *Windows Server 2016 or Windows Server 2019*
  - **Processor:** *Minimum: 1 GHz, Recommended: 2.33 GHz*
  - **RAM:** *Minimum: 8GB, Recommended: 10GB*
  - **Hard Drive Space:** *Minimum 5GB, Recommended 10GB*
  - **Local disk for backup:** *1.5 times size of data to be protected*
  - **Hyper-V PowerShell** *need to be installed*



**DEMO**

**BACKUP AZURE WORKLOAD**

---

# DEMO

**BACKUP ON PREMISE WORKLOAD (SLIDES MOSTLY)**

---

# PREPARING AZURE ENVIROMENT

## Recovery Services vault

Recovery Services vault

\* Name  
azure-backup-namct ✓

\* Subscription  
MSDN Platforms ▼

\* Resource group  
NAMCT-Summit-2019 ▼

[Create new](#)

\* Location  
North Central US ▼

Home > azure-backup-namct - Backup

### azure-backup-namct - Backup

Recovery Services vault

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Properties
- Locks
- Automation script

Getting started

- Backup
- Site Recovery

Where is your workload running?

On-Premises ▼

What do you want to backup?

0 selected ^

- ☐ Files and folders
- ☐ Hyper-V Virtual Machines
- ☐ VMware Virtual Machines
- ☐ Microsoft SQL Server
- ☐ Microsoft SharePoint
- ☐ Microsoft Exchange
- ☐ System State
- ☐ Bare Metal Recovery

# INSTALL AZURE BACKUP SERVER

Prepare infrastructure

☐ Already using [System Center Data Protection Manager](#) or any other [System Center Product](#)

Azure Backup Server

Please follow the steps mentioned below.

1. Install Microsoft Azure Backup Server

[Download](#)

2. Download vault credentials to register the server to the vault. Vault credentials will expire after 2 days.

☐ Already downloaded or using the latest Azure Backup Server installation

Download

3. Post infrastructure preparation, please use Microsoft Azure Backup Server UI(on-premises) to configure backup.

[Learn More](#)

Microsoft

Microsoft Azure Backup Server

Data Protection Manager

Install

[Microsoft Azure Backup Server](#)

[DPM Protection Agent](#)

[DPM Remote Administration](#)

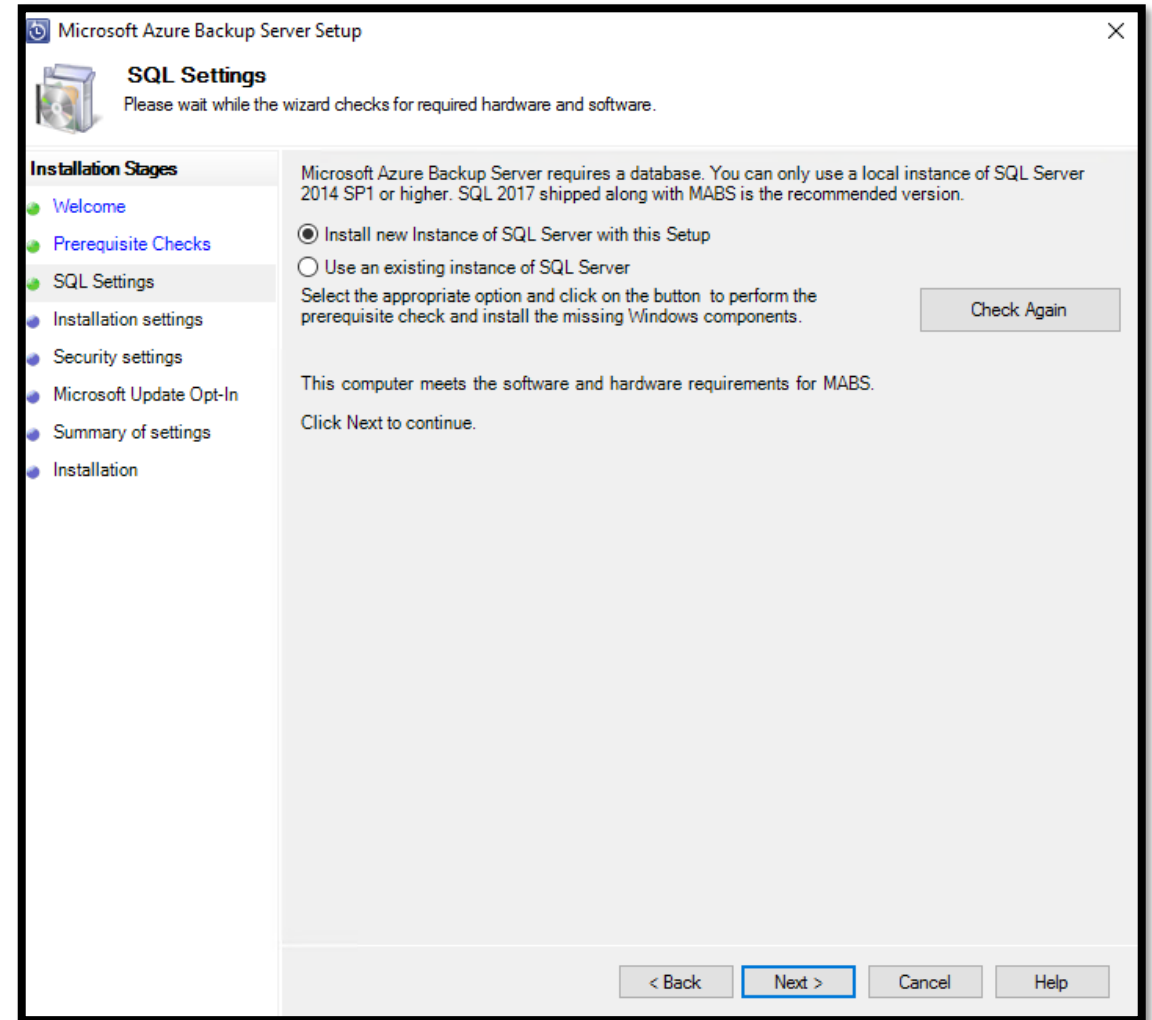
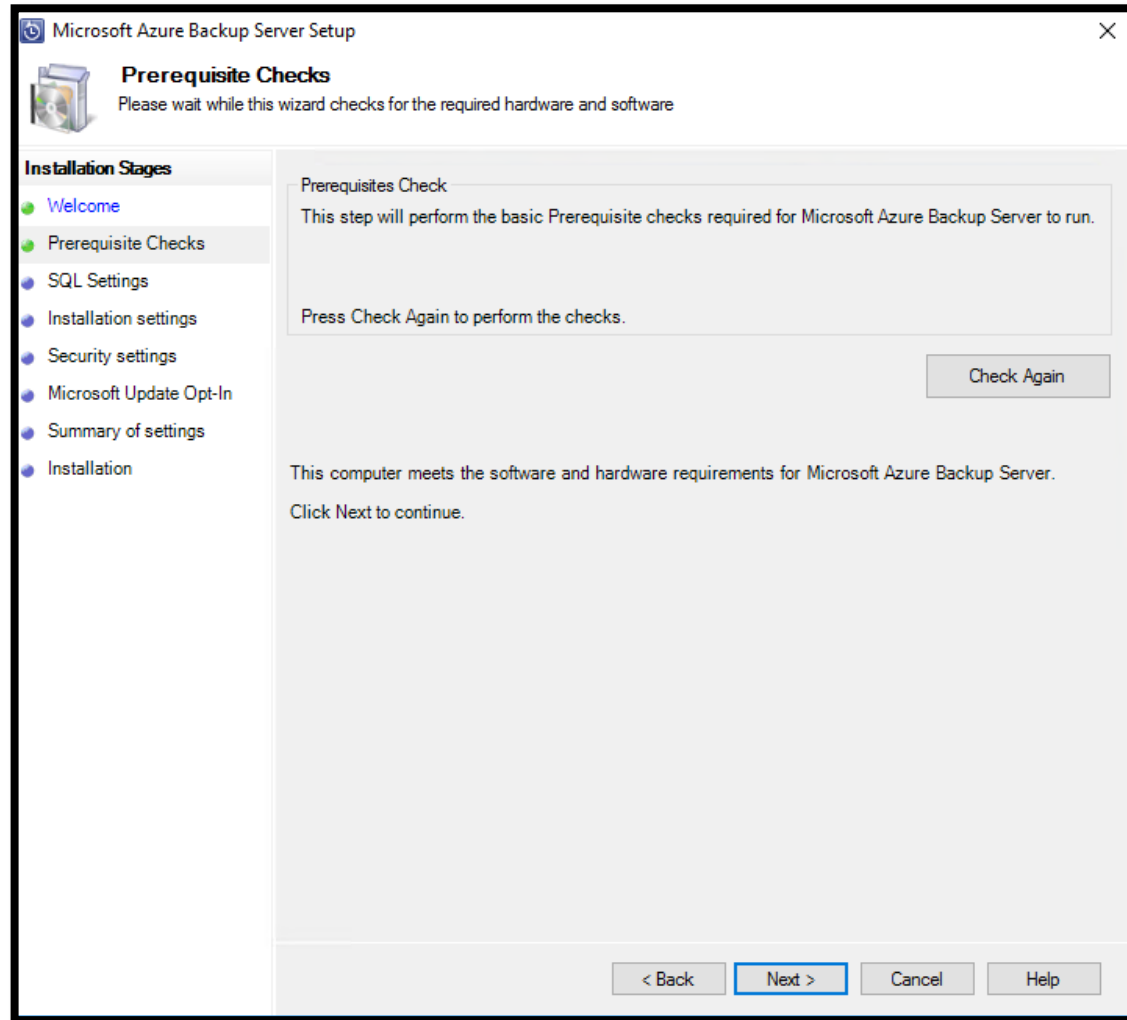
[SQL Self Service Recovery](#)

Additional Resources

[Microsoft Azure Backup Server Documentation](#)

Exit

# INSTALL AZURE BACKUP SERVER





# INSTALL AZURE BACKUP SERVER

**Microsoft Azure Backup Server Setup**

**SQL Settings**  
Please wait while the wizard checks for required hardware and software.

**Installation Stages**

- Welcome
- Prerequisite Checks
- SQL Settings
- Installation settings
- Security settings
- Microsoft Update Opt-In
- Summary of settings
- Installation

Microsoft Azure Backup Server Files

Program files:  
C:\Program Files\Microsoft Azure Backup Server\DPM Change...

Scratch Location (Must have free space at least 5% of the data backed-up to cloud):  
C:\Program Files\Microsoft Azure Backup Server\DPM\DPM\Cache Change...

Database files:  
C:\Program Files\Microsoft Azure Backup Server\DPM\DPM\DPMDb Change...

Staging Area:  
C:\Program Files\Mic...rver\DPM\StagingArea Change...

Space requirements

	Required	Available
System drive:	2160 MB	7143 MB
Program files drive:	4500 MB	7143 MB
Cache files drive:	Min 5% of backed up data	7143 MB
Database files drive:	900 MB	7143 MB

For more details on storage requirement click on the link below.  
<http://go.microsoft.com/fwlink/?LinkID=620846&clcid=0x409>

< Back **Next >** Cancel Help

**Microsoft Azure Backup Server Setup**

**Security Settings**  
Enter security settings information.

**Installation Stages**

- Welcome
- Prerequisite Checks
- SQL Settings
- Installation settings
- Security settings
- Microsoft Update Opt-In
- Summary of settings
- Installation

Microsoft Azure Backup Server Setup creates the following restricted local user accounts. Specify a strong password for the accounts. This password does not expire.

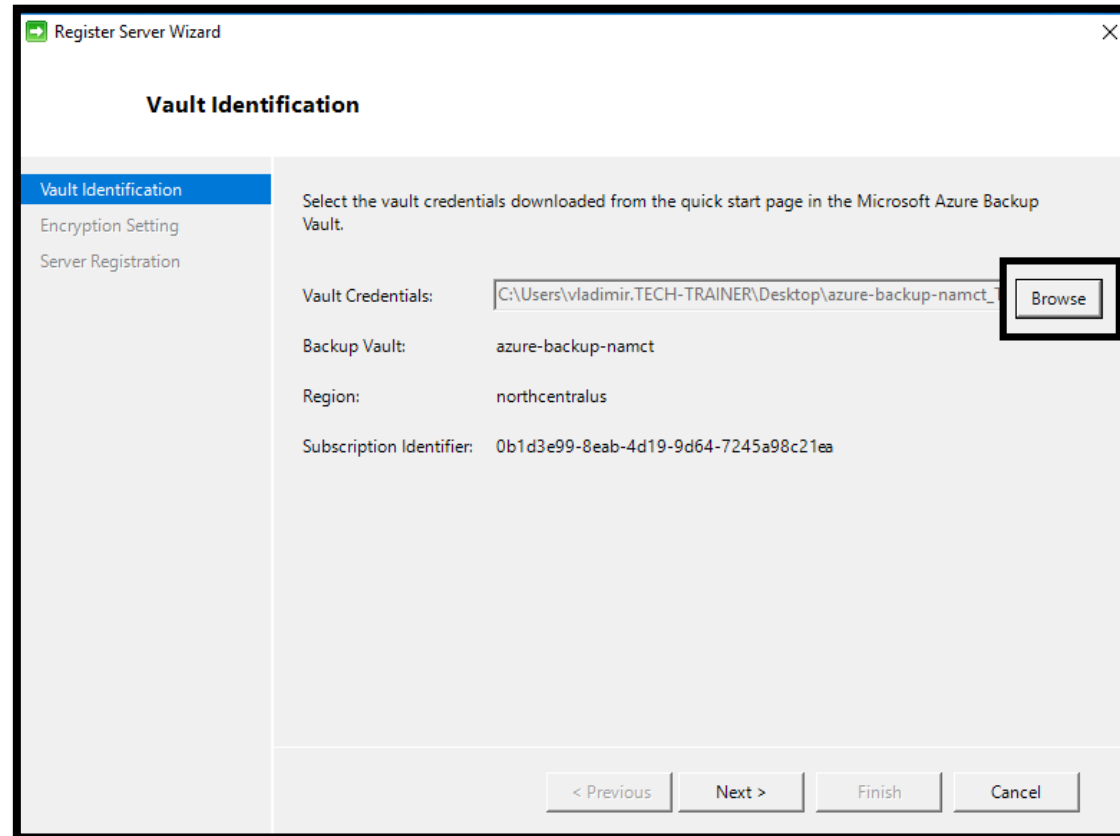
MICROSOFT\$DPM\$Acct	Runs the SQL Server service and the SQL Server Agent service.
DPMR\$ABS01	Securely generates reports.

Password:

Confirm password:

< Back **Next >** Cancel Help

# INSTALL AZURE BACKUP SERVER



The screenshot shows the 'Register Server Wizard' window, specifically the 'Vault Identification' step. The window has a title bar with a green icon and the text 'Register Server Wizard'. The main title is 'Vault Identification'. On the left, there is a sidebar with three items: 'Vault Identification' (selected and highlighted in blue), 'Encryption Setting', and 'Server Registration'. The main area contains the following text: 'Select the vault credentials downloaded from the quick start page in the Microsoft Azure Backup Vault.' Below this, there are four fields: 'Vault Credentials:' with a text box containing 'C:\Users\vladimir.TECH-TRAINER\Desktop\azure-backup-namct\_...' and a 'Browse' button; 'Backup Vault:' with the value 'azure-backup-namct'; 'Region:' with the value 'northcentralus'; and 'Subscription Identifier:' with the value '0b1d3e99-8eab-4d19-9d64-7245a98c21ea'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Register Server Wizard

### Vault Identification

Vault Identification  
Encryption Setting  
Server Registration

Select the vault credentials downloaded from the quick start page in the Microsoft Azure Backup Vault.

Vault Credentials: C:\Users\vladimir.TECH-TRAINER\Desktop\azure-backup-namct\_... **Browse**

Backup Vault: azure-backup-namct

Region: northcentralus

Subscription Identifier: 0b1d3e99-8eab-4d19-9d64-7245a98c21ea

< Previous Next > Finish Cancel

# CONFIGURE AZURE BACKUP SERVER

Production Server Addition Wizard

**Select Computers**  
Select the computers on which to install the protection agents.

**Steps:**

- Select Production Server type
- Select agent deployment method
- Select computers
- Enter credentials
- Choose restart method
- Summary
- Installation

☒ Windows Servers  
Install agent to protect Windows servers.

☐ VMware Servers  
Connect with VMware servers to protect VMware VMs.

< Back Next Cancel Help

Production Server Addition Wizard

**Select Computers**  
Select the computers on which to install the protection agents.

**Steps:**

- Select Production Server type
- Select agent deployment method
- Select computers
- Enter credentials
- Choose restart method
- Summary
- Installation

☒ Install agents  
Recommended for computers that are not behind firewalls, or computers that have the required exceptions created in the firewall. Selecting this option will install protection agent in the computers. Click help for more information.

☐ Attach agents  
Recommended for  
- computers behind firewall.  
- computers on which agent is already installed.  
- computers on which agent will be installed externally.  
Selecting this option will add the protected computers to the DPM server. If you have not already installed the agent, then you must manually install it on the protected computer by executing the DPMAgentInstaller. Click help for more information.

☐ Computer on trusted domain  
The computer belongs to the same domain as, or is in a domain that has a two-way trust with, the DPM server domain.

☐ Computer in a workgroup or untrusted domain  
The computer is part of a workgroup or on a domain that does not have two-way trust with the DPM server domain.

< Back Next Cancel Help

# CONFIGURE AZURE BACKUP SERVER

**Production Server Addition Wizard**

**Select Computers**  
Select the computers on which to install the protection agents.

**Steps:**

- Select Production Server type
- Select agent deployment method
- Select computers**
- Enter credentials
- Choose restart method
- Summary
- Installation

The computers listed are in the same domain as the DPM server. To add a computer from a different domain, type the fully qualified domain name. For example: machinename.domain.contoso.com

Computer name:

Selected computers:

Computer	Domain
HYPERV	tech-trainer.l...

Computer Domain  
DC01 tech-trainer.l...

Click Advanced to install an earlier version of the protection agent.

**Production Server Addition Wizard**

**Select Computers**  
Select the computers on which to install the protection agents.

**Steps:**

- Select Production Server type
- Select agent deployment method
- Select computers
- Enter credentials**
- Choose restart method
- Summary
- Installation

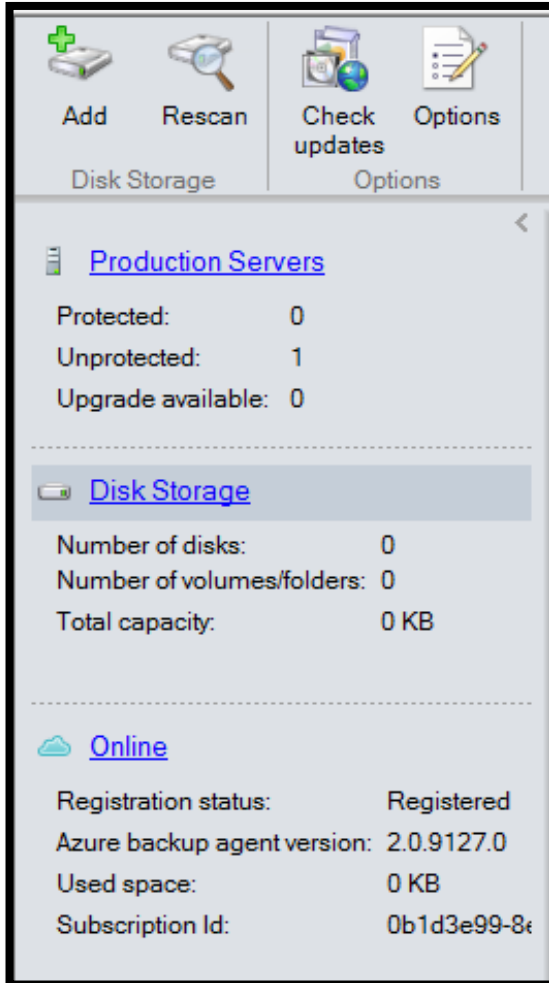
Please specify username and domain for a domain account that has administrator rights on the computers on which you wish to install agents. DPM uses the credentials to install the protection agents.

User name:

Password:

Domain:

# CONFIGURE AZURE BACKUP SERVER



The screenshot shows the Azure Backup Server console. At the top, there are four icons: Add (green plus), Rescan (magnifying glass), Check updates (globe), and Options (pencil). Below these are labels: 'Add', 'Rescan', 'Check updates', and 'Options'. Under 'Disk Storage', there is a 'Production Servers' section with a left arrow icon. It shows 'Protected: 0', 'Unprotected: 1', and 'Upgrade available: 0'. Below this is the 'Disk Storage' section, which is highlighted. It shows 'Number of disks: 0', 'Number of volumes/folders: 0', and 'Total capacity: 0 KB'. At the bottom is the 'Online' section, which shows 'Registration status: Registered', 'Azure backup agent version: 2.0.9127.0', 'Used space: 0 KB', and 'Subscription Id: 0b1d3e99-8e'.

**Production Servers**

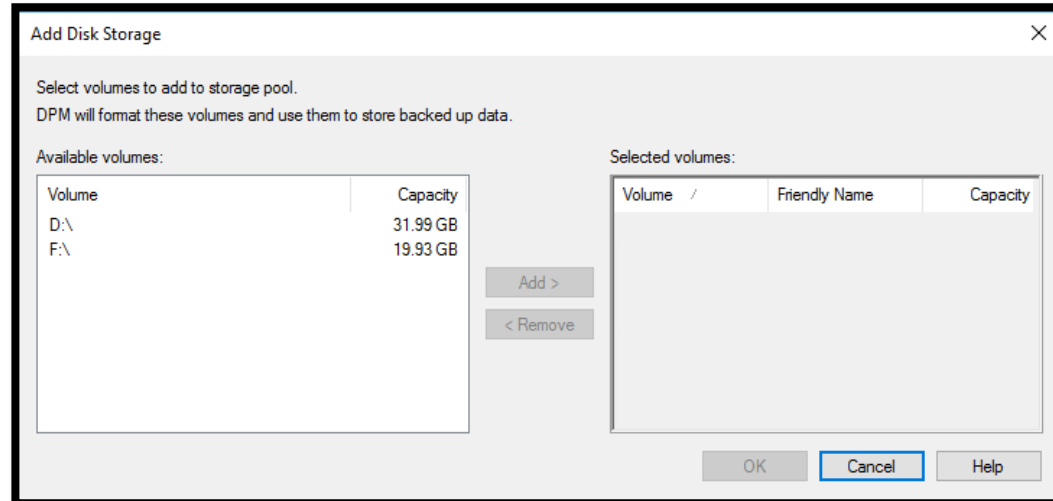
Protected: 0  
Unprotected: 1  
Upgrade available: 0

**Disk Storage**

Number of disks: 0  
Number of volumes/folders: 0  
Total capacity: 0 KB

**Online**

Registration status: Registered  
Azure backup agent version: 2.0.9127.0  
Used space: 0 KB  
Subscription Id: 0b1d3e99-8e



The screenshot shows the 'Add Disk Storage' dialog box. It has a title bar with 'Add Disk Storage' and a close button. The main text says 'Select volumes to add to storage pool. DPM will format these volumes and use them to store backed up data.' Below this, there are two tables. The first table, 'Available volumes', has two columns: 'Volume' and 'Capacity'. It lists 'D:\' with '31.99 GB' and 'F:\' with '19.93 GB'. The second table, 'Selected volumes', has three columns: 'Volume /', 'Friendly Name', and 'Capacity'. It is currently empty. Between the tables are 'Add >' and '< Remove' buttons. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

**Add Disk Storage**

Select volumes to add to storage pool.  
DPM will format these volumes and use them to store backed up data.

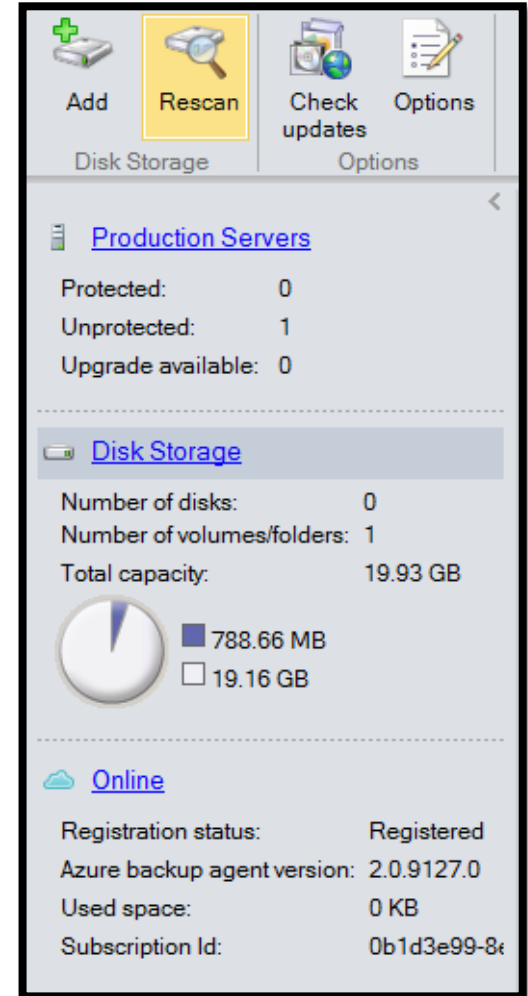
Available volumes:

Volume	Capacity
D:\	31.99 GB
F:\	19.93 GB

Selected volumes:

Volume /	Friendly Name	Capacity
----------	---------------	----------

Buttons: Add >, < Remove, OK, Cancel, Help



The screenshot shows the Azure Backup Server console after configuration. The 'Rescan' button is highlighted in yellow. The 'Disk Storage' section is now expanded, showing 'Number of disks: 0', 'Number of volumes/folders: 1', and 'Total capacity: 19.93 GB'. Below this is a pie chart showing '788.66 MB' (blue) and '19.16 GB' (white). The 'Online' section remains the same as in the first screenshot.

**Production Servers**

Protected: 0  
Unprotected: 1  
Upgrade available: 0

**Disk Storage**

Number of disks: 0  
Number of volumes/folders: 1  
Total capacity: 19.93 GB

788.66 MB  
19.16 GB

**Online**

Registration status: Registered  
Azure backup agent version: 2.0.9127.0  
Used space: 0 KB  
Subscription Id: 0b1d3e99-8e



# CONFIGURE AZURE BACKUP SERVER

---

# CONFIGURE AZURE BACKUP SERVER

Create New Protection Group

Welcome to the New Protection Group Wizard  
This wizard helps you create a new protection group that DPM will use to protect data.

Steps:

Welcome

Select protection group type

Select group members

Specify protection rules

Select data protection method

Select short-term goals

Choose consistency check options

Summary

Status

You can create two kinds of protection groups. Select one of them below

☒ Servers  
Select this option for backing up file servers and application servers. Before selecting this option, ensure that the DPM protection agent is already installed on the target server. These computers must be online at the time of configuring protection. You will need to select the specific resources you want to backup.

☐ Clients  
Select this option for backing up data from laptops and desktops. You can install the DPM protection agent after completing the configuration on the DPM server.  

To configure secondary protection for laptops and desktops, select the Servers option.

< Back

Next >

Cancel

Help

Create New Protection Group

Select Group Members.  
Select the data that you want to protect.

Steps:

Welcome

Select protection group type

Select group members

Select data protection method

Select short-term goals

Choose consistency check options

Summary

Status

To choose the data to protect, select the check boxes in the Available members section. To exclude a folder, expand the folder. If you do not see the data source you want to protect in the tree below, click the following link for a list of unsupported configurations

Available members

tech-trainer.local

ABS01

HYPERV

All Shares

All Volumes

HyperV

Host Component

☒ RCT\centOS-01

☒ RCT\centOS-02

☐ System Protection

Update data sources

Refresh to clear the cache and retrieve the latest data

Refresh

Selected members

Selected Members	Computer
RCT\centOS-01	HyperV.tech-trainer.local
RCT\centOS-02	HyperV.tech-trainer.local

Remove

Excluded folders: 0 View

Excluded file types: 0 Exclude Files ...

< Back

Next >

Cancel

Help

# CONFIGURE AZURE BACKUP SERVER

Create New Protection Group

Select Data Protection Method

DPM can help provide disk, online and tape based data protection.

Steps:

Welcome

Select protection group type

Select group members

Select data protection method

Select short-term goals

Choose consistency check options


Summary


Status

Protection group name:

Protection method

Select your protection method.

 ☒ I want short-term protection using:

 ☒ I want online protection

< Back

Next >

Cancel

Help

Create New Protection Group

Specify Short-Term Goals

DPM will create a protection plan using your short-term recovery goals.

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

Specify online retention policy

Choose online replication

Summary

Status

Specify your short-term recovery goals for disk-based protection.

Retention range:  days

Application recovery points

For applications the recovery point is as per synchronization frequency when they support incremental, otherwise the recovery point is as per express full backup.

Recovery points: Based on express full schedule (20:00 Everyday)

Express Full Backup: 

Modify ...

< Back

Next >

Cancel

Help

# CONFIGURE AZURE BACKUP SERVER

Create New Protection Group

Specify Short-Term Goals

DPM will create a protection plan using your short-term recovery goals.

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

Specify online retention policy

Choose online replication

Summary

Status

Review target storage assigned for each data source and change if need be.

Disk storage allocation for new members

Total data size: 3.13 GB

Disk storage to be provisioned on DPM: 3.79 GB

Disk storage allocation details:

Data Source /	Data Size	Space To ...	Target Storage
RCT\centOS-01 on HyperV.tech-trainer.local	1.57 GB	1.89 GB	ABSBBackup - 15.37 GE ▾
RCT\centOS-02 on HyperV.tech-trainer.local	1.57 GB	1.89 GB	ABSBBackup - 15.37 GE ▾

Available target disk storage:

Name /	Friendly N...	Allowed Dataso...	Total Spa...	Free Space	Underpro...
F:\	ABSBBackup	All	19.93 GB	15.37 GB	0 KB

< Back

Next >

Cancel

Help

Create New Protection Group

Choose Replica Creation Method

To protect the data you have selected, you must initially copy the selected data to the Data Protection Manager computer.

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

Specify online retention policy

Choose online replication

Summary

Status

DPM must create a replica to copy the selected data to the DPM server. How do you want to create the replica?

Replica in DPM Server

☒ Automatically over the network

☒ Now

☐ Later

08-Mar-19 ▾

00:38:56 ▾

☐ Manually

You must transfer the data using removable media.  
For large amounts of data, this operation may be faster than replica creation across the network.

< Back

Next >

Cancel

Help

# CONFIGURE AZURE BACKUP SERVER

Create New Protection Group

Choose Replica Creation Method

To protect the data you have selected, you must initially copy the selected data to the Data Protection Manager computer.

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

Specify online retention policy

Choose online replication

Summary

Status

Running a consistency check on a replica that has become inconsistent allows DPM to continue protecting the data source. You can start a consistency check manually or allow DPM to run it automatically. Use the methods below to customize how DPM can run a consistency check.

☒ Run a consistency check if a replica becomes inconsistent

Select this method if you want DPM to automatically run a consistency check when it finds a replica in an inconsistent state. This method may require DPM to use additional CPU and disk resources.

☐ Run a daily consistency check according to the following schedule

Select this method if you want DPM to check for inconsistent replicas at a specified time every day and then run a consistency check if it finds one. This method may require additional CPU and disk resources during the specified hours.

Start time:

00:00

Maximum duration:

480 hours

Cannot exceed 480 hours (20 days).

< Back

Next >

Cancel

Help

Create New Protection Group

Specify Online Protection Data

Specify the data that you would like DPM to help protect online.

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

Specify online retention policy

Choose online replication

Summary

Status

Select the data source you want to protect online.

☐ Protect auto protected SQL DBs, VMs to disk to cloud automatically

Selected members	Computer
<input checked="" type="checkbox"/> RCT\centOS-01	HyperV.tech-trainer.local
<input checked="" type="checkbox"/> RCT\centOS-02	HyperV.tech-trainer.local

Select All

Deselect All

< Back

Next >


Cancel

Help



# CONFIGURE AZURE BACKUP SERVER

Create New Protection Group

 **Specify Online Protection Data**  
Specify the data that you would like DPM to help protect online.


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
- Specify online retention policy
- Choose online replication
- Summary
- Status

Define the schedule when you want to create a backup copy


Schedule a backup every  
☒ Day ☐ Week ☐ Month ☐ Year

At following times (Maximum allowed is two times a day)  
21:00 None

 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.

< Back Next > Cancel Help

Create New Protection Group

 **Specify Online Retention Policy**  
Specify online backup schedule which DPM will use to generate your protection plan

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
- Specify online retention policy
- Choose online replication
- Summary
- Status

Specify the retention policy which DPM will use to generate your protection plan

☒ Daily Retention policy  
Retain backup copies taken on At 21:00 for 30 Days

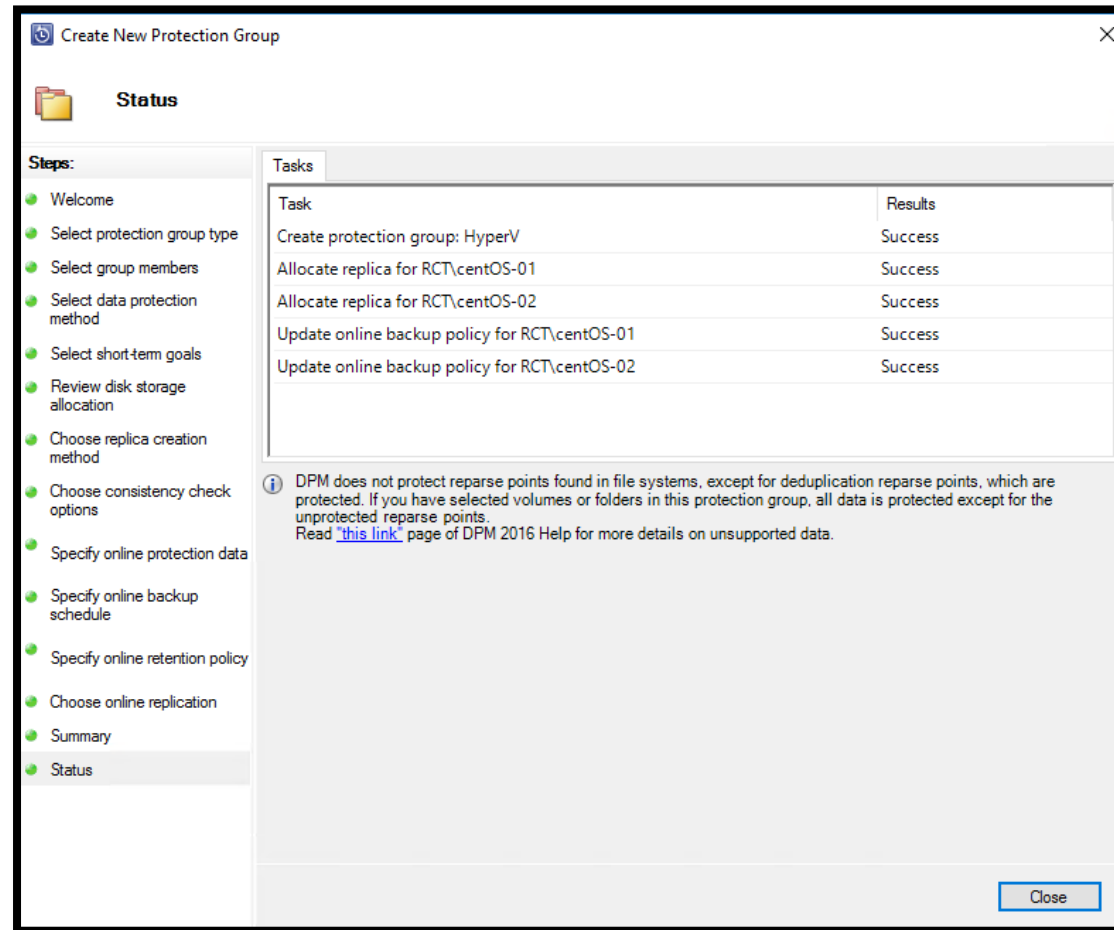
☐ Weekly Retention Policy  
Retain backup copies taken on Saturday At 21:00 for 104 Weeks

☐ Monthly Retention Policy  
Retain backup copies taken on ☒ Last Saturday ☐ Day(s) 1 At 21:00 for 60 Months

☐ Yearly Retention Policy  
Retain backup copies taken on ☒ Last Saturday of March ☐ Day(s) 1 of March At 21:00 for 10 Years

< Back Next > Cancel Help

# CONFIGURE AZURE BACKUP SERVER



# WHAT WE CAN DO IF ABS DIES?

---

- If Azure Backup Server is on Azure VM, you can use Azure Backup ☺
- Azure Backup agent cannot be installed on Azure Backup Server
- 3rd party backup solution
- You need to perform magic:
  - *Backup SQL databases*
  - *Remove „old“ Azure Backup Server from portal*
  - *Re-install Azure Backup Server on new machine with same backup vault*
  - *Restore SQL databases*

# RECAP

---

- Azure Backup features
- Azure Backup components
- Backup Azure workload – Azure VM and Azure File Share
- On-premise backup with Azure Backup
- Demo – Azure workload
- Demo - On-premise workload

Q & A

**OR YOU NEED A BREAK FROM ME 😊**

---