

# Azure Backup, Azure Site Recovery Workshop

2018-11-20

RVE

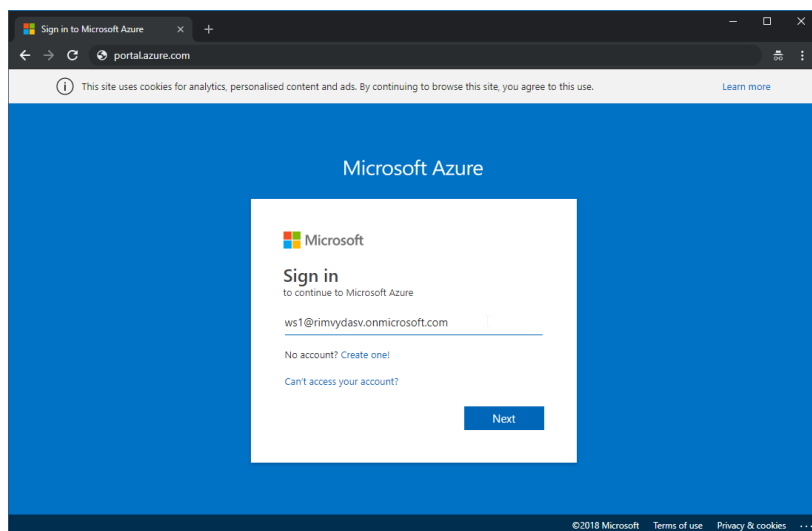
# 1. Azure Portal

<http://portal.azure.com>

Username: wsX@rimvydasv.onmicrosoft.com

Password: Vuhu3395

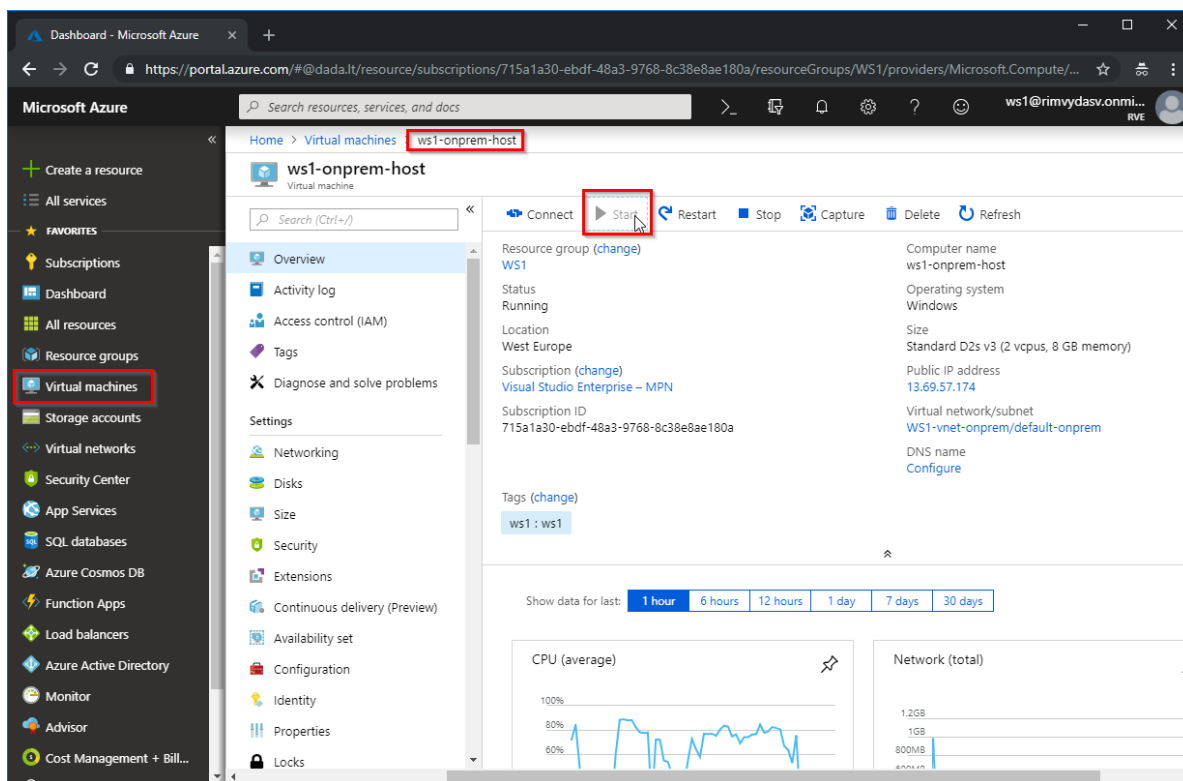
*X – workshop pradžioje Jums suteiktas skaičius.*



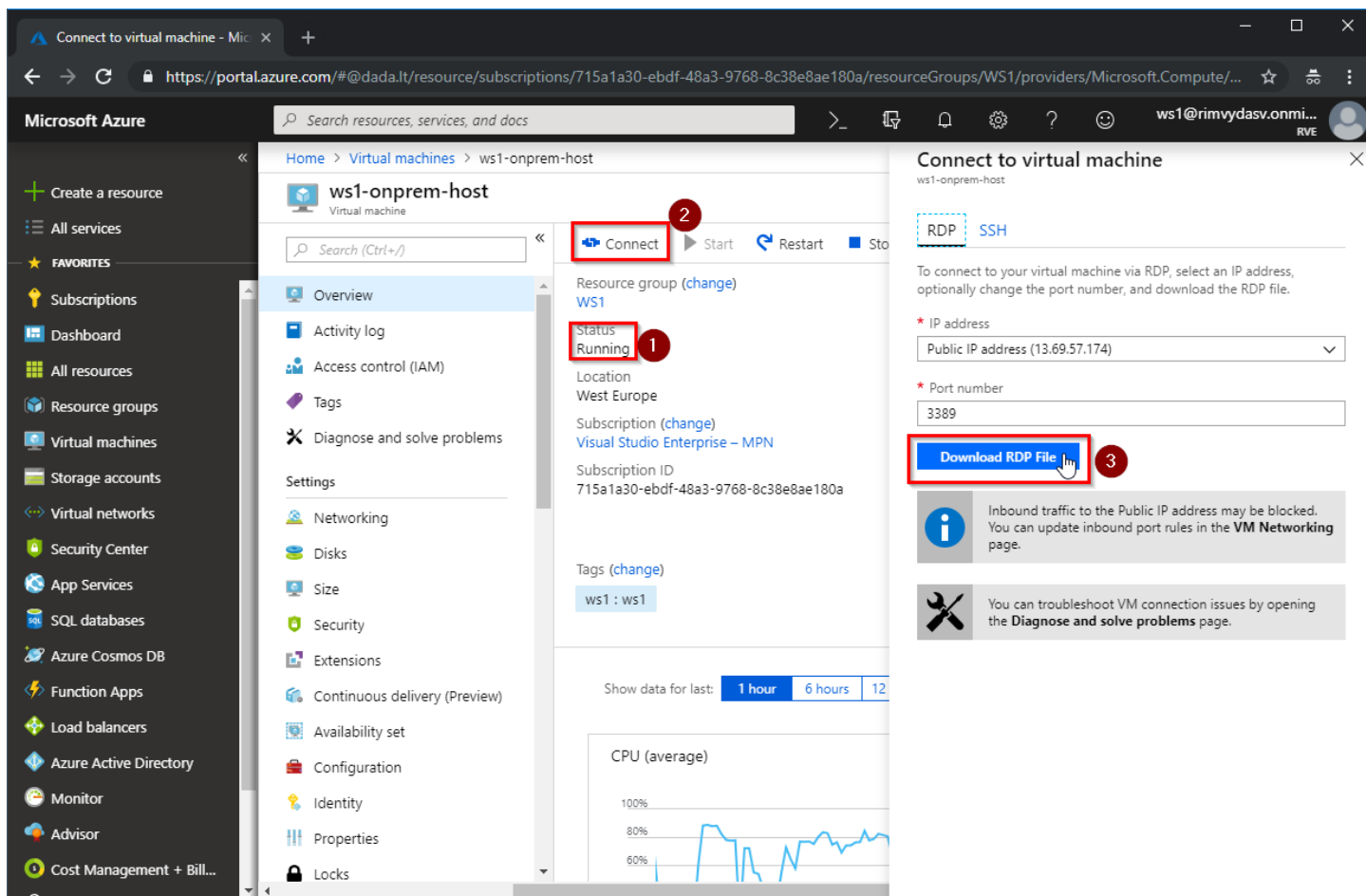
## 2. Resursų paruošimas, prisijungimas

### 2.1. OnPrem Hyper-V serveris “wsX-onprem-host”:

Jūsų „duomenų centrą“ imituoja Azure virtuali mašina su joje esančiomis 3 VM. Jei Host VM statusas ne „Running“ – įjunkite:



Prisijungimas:



Prisijungimui prie “wsX-onprem-host” naudokite RDP failą sugeneruotą Azure portale:

<b>Username:</b>	<b>ws1</b>
<b>Password:</b>	<b>Vuhu33953395</b>

## 2.2. Prisijungimas prie jūsų “duomenų centre” esančių virtualių mašinų:

Jūsų “onprem” virtualios mašinos pasiekiamos per “wsX-onprem-host” esantį Hyper-V Manager (Azure VM naudoja “Nested Virtualization”)

VM prisijungimai (jei statusas ne “Running” – įjunkite):

- 1) VM Windows “**WinSrv2012R2**” (192.168.0.10):

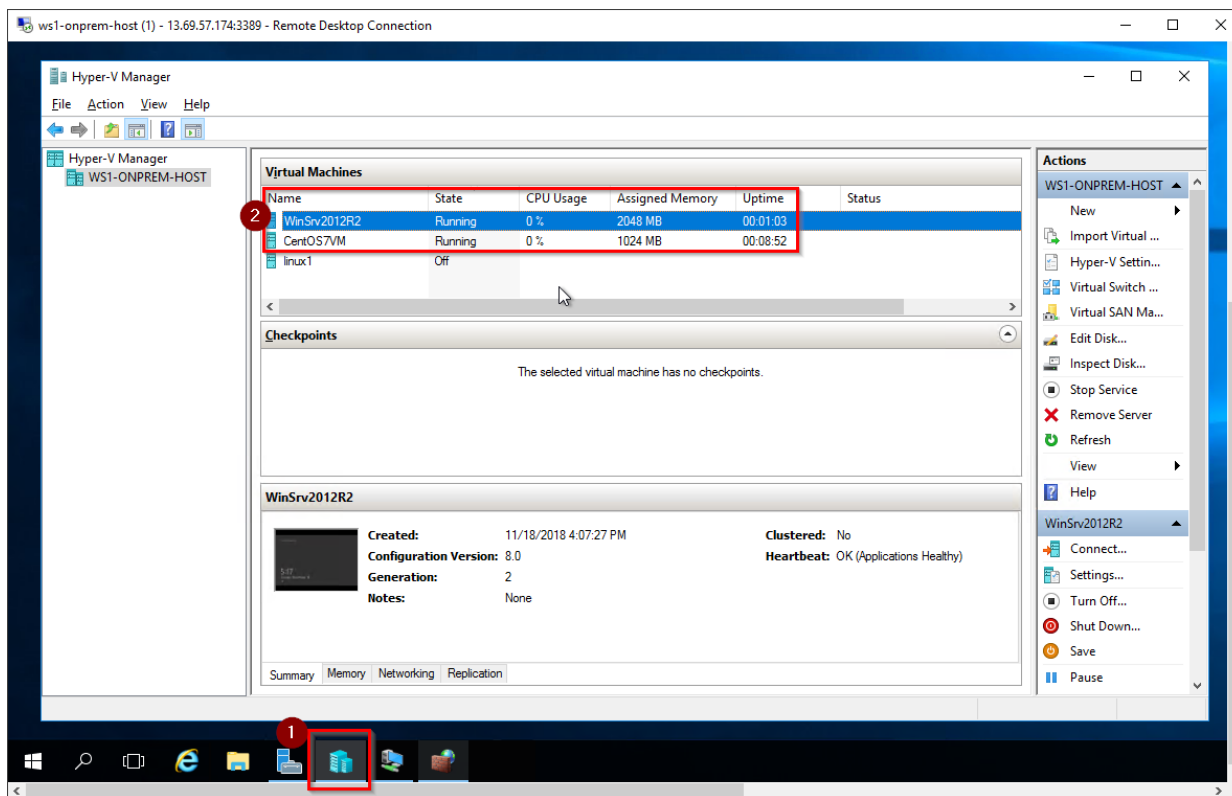
<b>Username:</b>	<b>Administrator</b>
<b>Password:</b>	<b>Vuhu3395</b>

Serveryje veikia IIS serveris. Galite patikrinti vidiniu IP 192.168.0.10 ir išoriniu „wsX-onprem-host“ adresu wsXhost.westeurope.cloudapp.azure.com (firewall nukreipia užklausas).

- 2) VM Linux “**CentOS7VM**” (192.168.0.20):

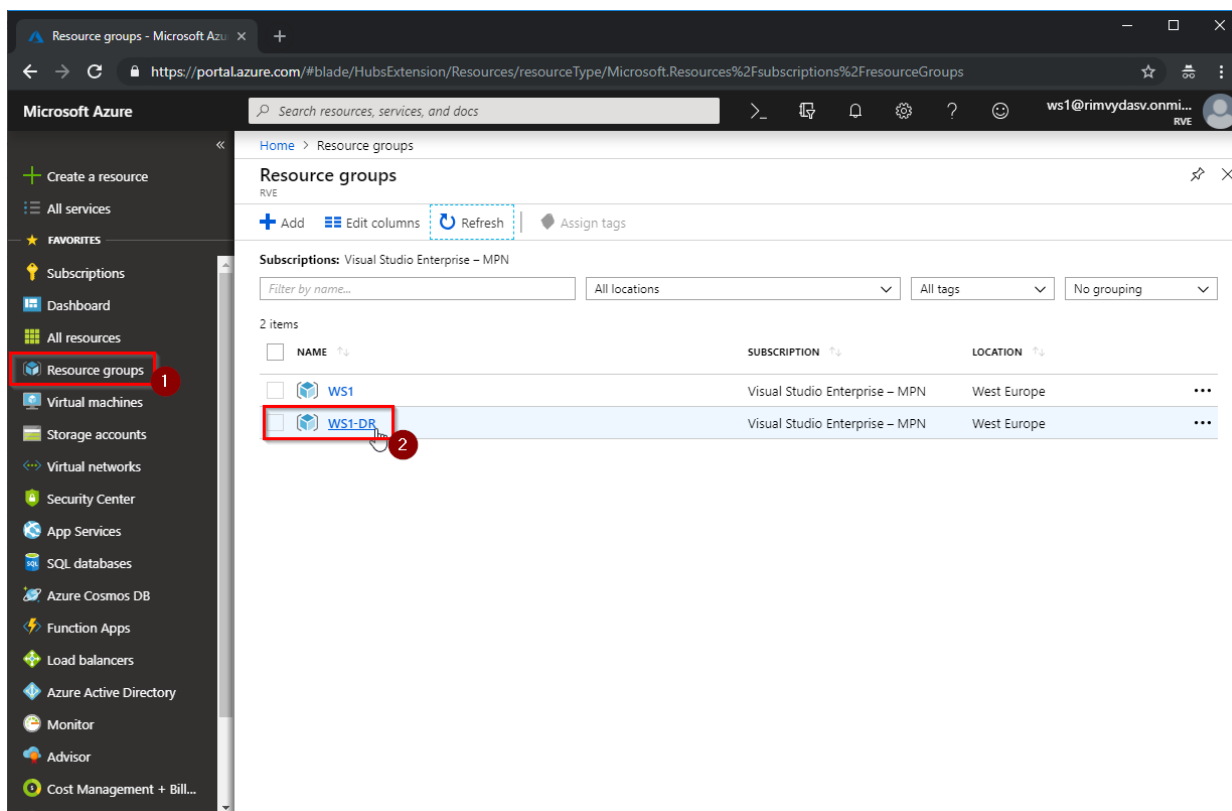
<b>Root username:</b>	<b>ws</b>
<b>Password:</b>	<b>Vuhu3395</b>

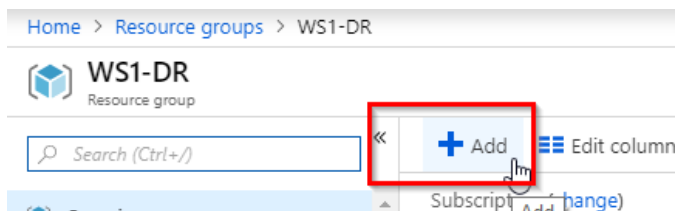
Pabandykite prisijungti prie abiejų VM Hyper-V konsolėje, įsitikinkite, kad jos veikia.



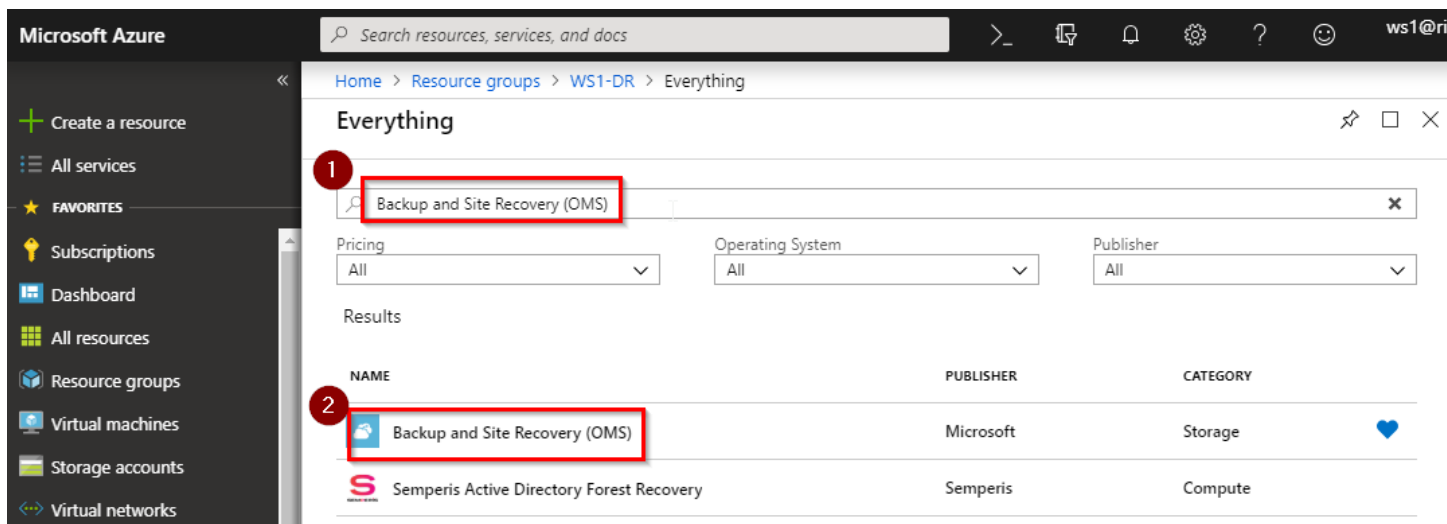
### 3. DR Vault sukūrimas:

3.1. Azure Portale „WSX-DR” resursų grupėje sukurkite naują „Recovery Services Vault“, kuris bus naudojamas Azure Backup ir Azure Site Recovery paslaugoms valdyti:

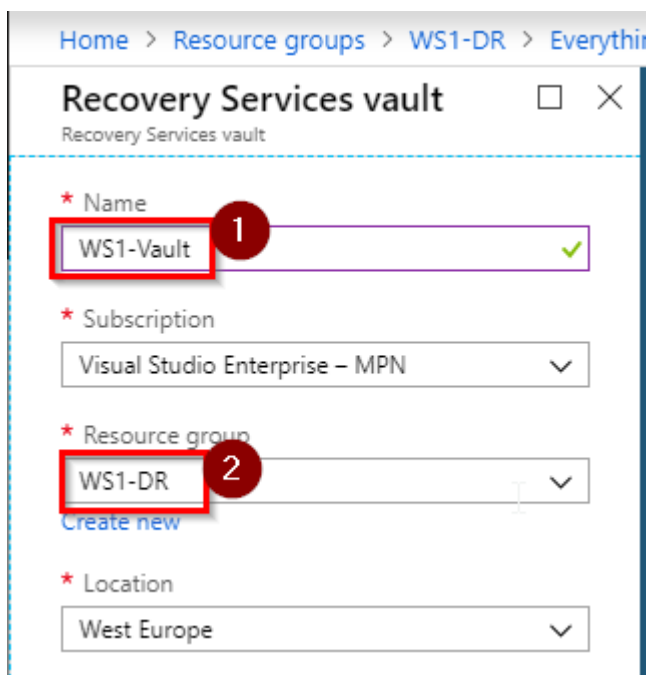




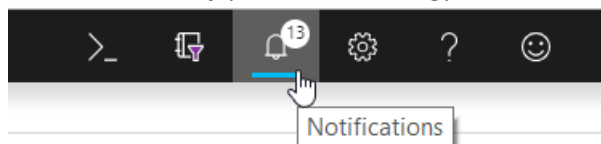
3.2. Azure Marketplace suraskite ir pasirinkite "Backup and Site Recovery (OMS):



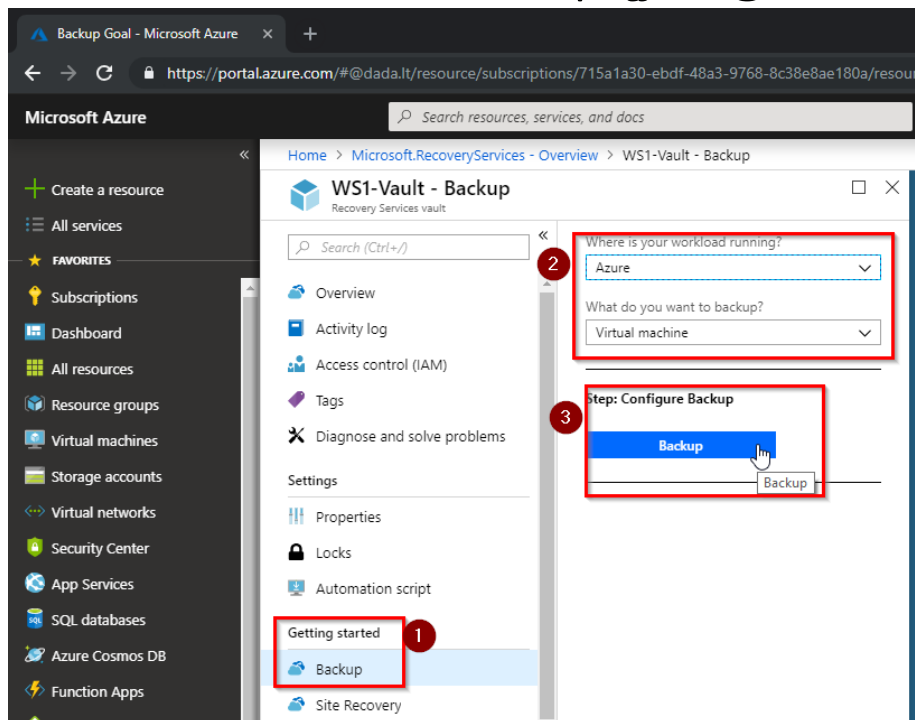
3.3. Pavadinkite „WSX-Vault“ (kur X jums suteiktas skaičius). Būtinai pasirinkite „WSX-DR“ resursų grupę. Spauskite „Create“.



3.4. Stebėkite statusą, palaukite kol saugykla bus sukurta.



## 4. Azure VM backup įjungimas ir konfigūravimas



4.1. Sukurto Recovery Services Vault pasirinkite Backup skiltį. Nurodykite, kad jūsų virtuali mašiną kurią norite apsaugoti yra laikoma Azure.

Sukurkite naują Azure „Backup Policy“. Nustatykite, **kad kopijos būtų daromos kasnakt, vidurnaktį, saugomos 7 dienas. Taip pat sukonfigūruokite 6 kas mėnesines kopijas.**

Overview > WS1-Vault - Backup > Backup > Backup policy

### Backup policy

Choose backup policy ⓘ

DefaultPolicy  
**Create New**  
DefaultPolicy

Daily at 03:30

#### RETENTION RANGE

##### Retention of daily backup point

Retain backup taken every day at 03:30 for 30 Day(s)

Overview > WS1-Vault - Backup > Backup > Backup policy

### Backup policy

Choose backup policy ⓘ

Create New

\* Policy name ⓘ

Policy1

Backup schedule

\* Frequency

Daily

\* Time

22:30

\* Timezone

(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

#### Retention range

☒ Retention of daily backup point.

\* At

22:30

For

7

Day(s)

☐ Retention of weekly backup point.

Not Configured

#### 4.2. Pasirinkite kurią VM apsaugosite:

Backup policy (new) Policy1

Items to backup Select

Filter items ...

VIRTUAL MACHINE NAME	RESOURCE GROUP
<input checked="" type="checkbox"/> ws1-onprem-host	WS1

#### 4.3. Sukurę policy ir pasirinkę VM spauskite “Enable Backup”. Stebėkite kaip vyksta procesas:

Notifications

More events in the activity log → Dismiss all ...

Deployment in progress... Running

Deployment to resource group 'WS1-DR' is in progress.

by me a few seconds ago

Deployment succeeded

Deployment 'Microsoft.RecoveryServices' to resource group 'WS1-DR' was successful.

Go to resource Pin to dashboard

by me 8 minutes ago

#### 4.4. Inicijuokite pirminį backup'ą nelaukdami “Scheduled” laiko:

Home > WS1-DR > WS1-Vault - Backup items > Backup Items (Azure Virtual Machine) > ws1-onprem-host

ws1-onprem-host Backup item

Backup now Restore VM File Recovery Stop backup Resume backup Delete backup data

Alerts and Backup now

View all Alerts (last 24 hours)

View all Jobs (last 24 hours)

Backup status

Backup Pre-Check Passed

Last backup status Warning (Initial backup pending)

Summary

Recovery services vault WS1-Vault

Backup policy Policy1

Oldest restore point -

Restore points

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, [click here](#).

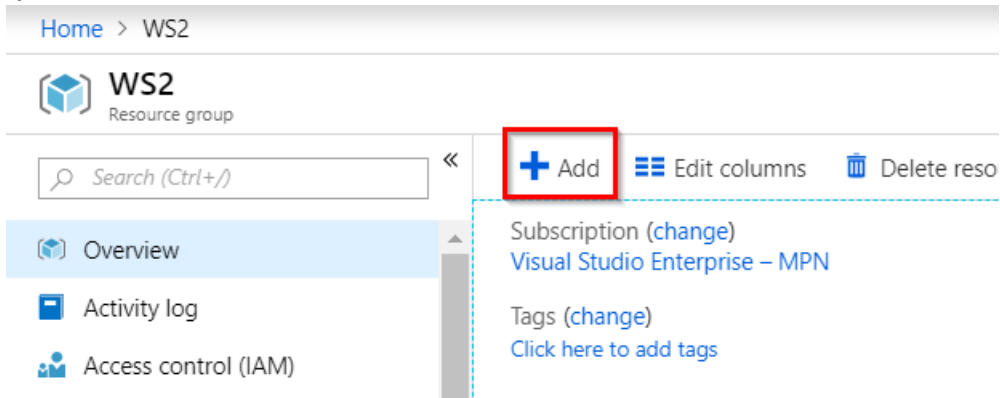
CRASH CONSISTENT 0 APPLICATION CONSISTENT 0 FILE-SYSTEM CONSISTENT 0

TIME CONSISTENCY

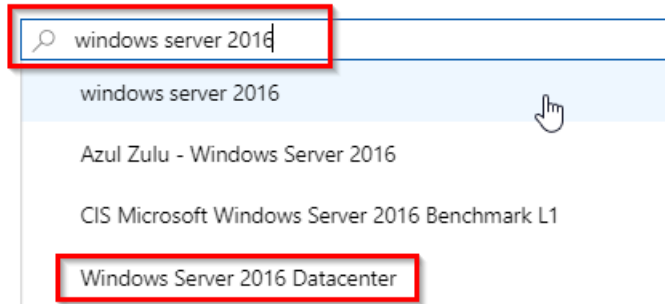
No restore points available.

#### 4.5. Stebėkite kaip vyksta atsarginės kopijos vykdymas. “View all Jobs” rodo visų paskutinių darbų būseną.

5. Išbandykite kitą būdą įjungti atsargines kopijas virtualioms mašinoms. Sukurkite naują VM „wsX“ resursų grupėje:



5.1.



5.2.

Pavadinkite VM „Srv2016-WSX“, atidarykite RDP portą:

Home > WS1 > Everything > Windows Server 2016 Datacenter > Create a virtual machine

### Create a virtual machine

\* Resource group WS1 [Create new](#)

**INSTANCE DETAILS**

\* Virtual machine name Srv2016-WS1

\* Region West Europe

Availability options No infrastructure redundancy required

\* Image Windows Server 2016 Datacenter [Browse all images and disks](#)

\* Size **Standard DS1 v2**  
1 vcpu, 3.5 GB memory [Change size](#)

**ADMINISTRATOR ACCOUNT**

\* Username ws

\* Password .....

\* Confirm password .....

\* Public inbound ports ☐ None ☒ Allow selected ports

\* Select inbound ports ..... RDP

5.3.

5.4.

Prijunkite prie jau egzistuojančio virtualaus tinklo:



## NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

\* Virtual network ⓘ WS1-Cloud-VNet ▼  
[Create new](#)

\* Subnet ⓘ WS1-Cloud (10.10.0.0/24) ▼  
[Manage subnet configuration](#)

Public IP ⓘ (new) Srv2016-WS1-ip ▼  
[Create new](#)

Network security group ☒ Basic ☐ Advanced

\* Public inbound ports ⓘ ☐ None ☒ Allow selected ports

\* Select inbound ports RDP ▼

5.5.

Ijunkite Backup dar kurdami VM. Pasirinkite prieš tai sukurtą Recovery Services Vault. Sukurkite naują Policy su kitokia konfigūracija:

[Basics](#) [Disks](#) [Networking](#) **[Management](#)** [Guest config](#) [Tags](#) [Review + create](#)

Configure monitoring and management options for your VM.

**MONITORING**

Boot diagnostics ⓘ ☐ On ☒ Off

OS guest diagnostics ⓘ ☐ On ☒ Off

**IDENTITY**

System assigned managed identity ⓘ ☐ On ☒ Off

**AUTO-SHUTDOWN**

Enable auto-shutdown ⓘ ☐ On ☒ Off

**BACKUP**

Enable backup ⓘ ☒ On ☐ Off

\* Recovery Services vault ⓘ ☐ Create new ☒ Use existing

WS1-Vault ▼

\* Backup policy DefaultPolicy ▼  
[Create new](#)  
[View policy details](#)

5.6.

5.7. Nueikite iki "Review+create", sukurkite VM.

5.8. Naujai sukurta VM iškart apsaugota pagal jūsų sukurtą policy. Patikrinkite skiltį "Backup" prie VM valdymo:

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20181120000835 - Overview > Srv2016-WS1 - Backup

**Srv2016-WS1 - Backup**  
Virtual machine

Search (Ctrl+/)

Locks  
Automation script  
Operations  
Auto-shutdown  
**Backup**  
Disaster recovery

Backup now Restore VM File Recovery Stop backup Resume backup Dele

**Alerts and Jobs**  
[View all Alerts](#) (last 24 hours)  
[View all Jobs](#) (last 24 hours)

**Backup status**  
Backup Pre-Check ✓ Passed  
Last backup status ⚠ Warning(Initial backup pending)

**Restore points**  
This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, [click here](#).

## 6. Onprem VM backup konfigūravimas

- 6.1. Recovery services Vault pasirinkite Azure Backup. “Where your workload is running” pasirinkite “On-Premises”, “What to backup” pasirinkite “Files and Folders” ir “System State”. Atsisiųskite agentą ir prisijungimo duomenis (vault credentials):

The screenshot shows the 'Prepare infrastructure' wizard in the Azure Backup portal. The left sidebar has 'Getting started' and 'Backup' highlighted. The main area has two dropdowns: 'Where is your workload running?' set to 'On-Premises' and 'What do you want to backup?' set to '2 selected'. A 'Prepare Infrastructure' button is visible. On the right, the 'Recovery Services Agent' section lists five steps, with the first step 'Install Recovery Services agent' highlighted, showing a 'Download' button.

- 6.2. Failų perkėlimui panaudosime Azure File Share ir išbandysime jos prijungimą. Nueikite į resursų grupę „WSX“. Spauskite „+ Add“, suraskite ir pridėkite naują „Storage account“.

The screenshot shows the 'Storage account - blob, file, table, queue' page in the Azure portal. The page displays a list of storage accounts, including 'Storage account - blob, file, table, queue' which is highlighted. The right sidebar shows details for the selected storage account, including the publisher 'Microsoft' and useful links like 'Documentation', 'Service overview', and 'Pricing'. A 'Create' button is visible at the bottom right.

- 6.3. Pasirinkite savo resursų grupę „WSX“, pavadinkite „wsXfilesX“, „Standart“, „LRS“:

## Create storage account

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

\* Subscription

\* Resource group

[Create new](#)

### INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

\* Storage account name

\* Location

Performance ☒ Standard ☐ Premium

Account kind

Replication

Access tier (default) ☐ Cool ☒ Hot

[Review + create](#)

[Previous](#)

[Next : Advanced >](#)

## 6.4. Sukurtame “storage account” pasirinkite “Files”, sukurkite naują File Share:

Home > Microsoft.StorageAccount-20181119111241 - Overview > ws1files1

**ws1files1**  
Storage account

Search (Ctrl+J)

Open in Explorer → Move Delete Refresh

Tags (change)  
[Click here to add tags](#)

Services

- Blobs**  
REST-based object storage for unstructured data  
[Explore data using OAuth preview](#)  
[Learn more](#)
- Files**  
File shares that use the standard SMB 3.0 protocol  
[Learn more](#)
- Tables**  
Tabular data storage  
[Learn more](#)
- Queues**  
Effectively scale apps according to traffic  
[Explore data using OAuth preview](#)  
[Learn more](#)

File share Refresh

Storage account File share

## 6.5. Suteikite File Share pavadinimą ir nustatykite dydį:

**File share**

\* Name

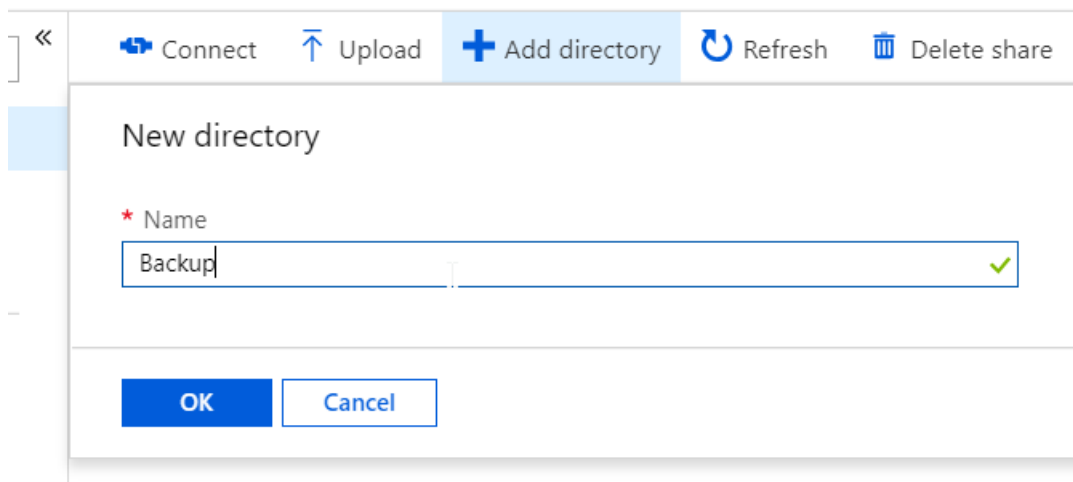
Quota

GB

[Create](#) [Discard](#)

[Create](#)

Sukurkite direktoriją:



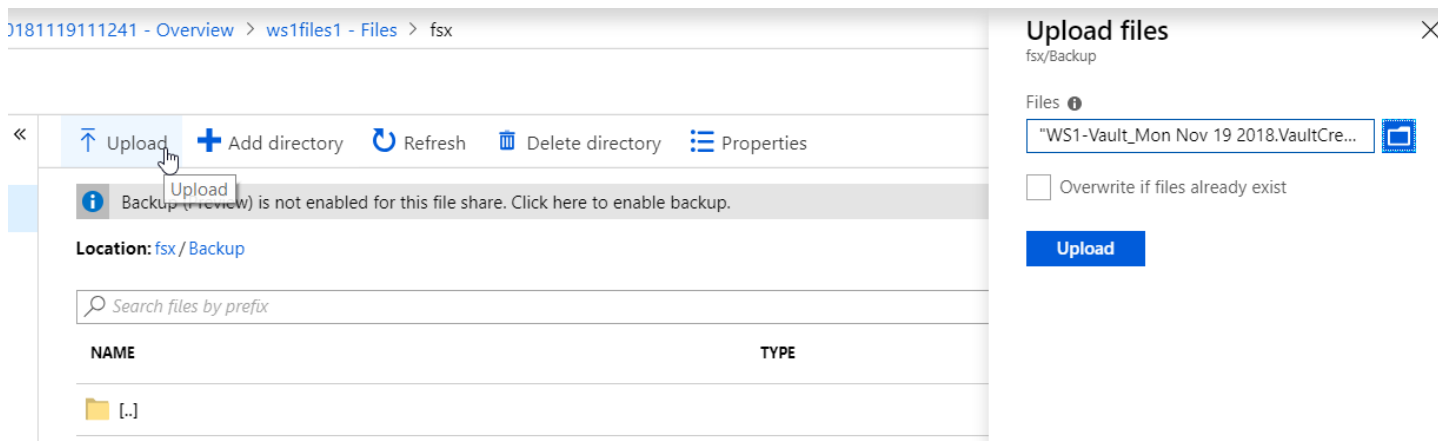
New directory

\* Name

Backup

OK Cancel

6.6. Įkelkite anksčiau parsisiųstus 2 backup konfigūravimo failus. Pasirinkite „Upload“:



181119111241 - Overview > ws1files1 - Files > fsx

Upload files

fsx/Backup

Files

"WS1-Vault\_Mon Nov 19 2018.VaultCre..."

☐ Overwrite if files already exist

Upload

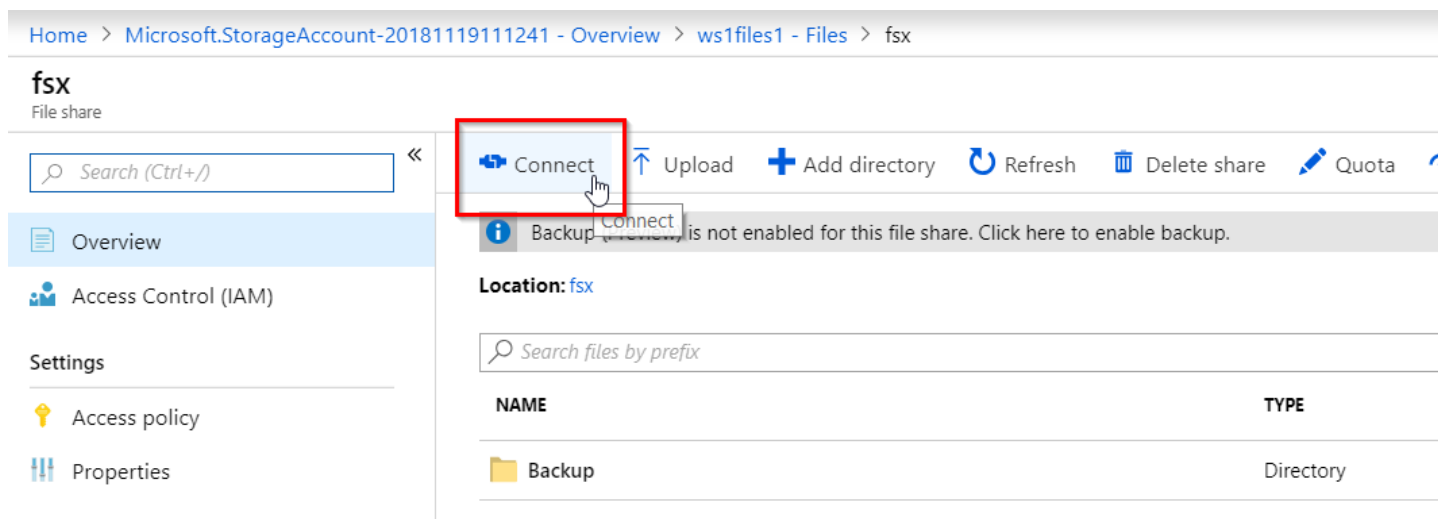
Backup (Preview) is not enabled for this file share. Click here to enable backup.

Location: fsx / Backup

Search files by prefix

NAME	TYPE
[.]	

6.7. Prijunkite File share prie **WinSrv2012R2** virtualios mašinos (onprem host viduje). Norėdami gauti prisijungimo komandą ir raktus pasirinkite „Connect“:



Home > Microsoft.StorageAccount-20181119111241 - Overview > ws1files1 - Files > fsx

fsx

File share

Search (Ctrl+/)

Overview

Access Control (IAM)

Settings

Access policy

Properties

Connect

Backup (Preview) is not enabled for this file share. Click here to enable backup.

Location: fsx

Search files by prefix

NAME	TYPE
Backup	Directory

Nustatykite norimą disko raidę, pasirinkite Powershell ar CMD komandos šabloną, jį nukopijuokite:

## Connect

fsx

### Connecting from Windows

Drive letter

1

To connect to this file share from a Windows computer, run these PowerShell commands:

```
$acctKey = ConvertTo-SecureString -String  
"ZftvVFdJyx6+kWBrPxl5aBa0eQhaivKnVqymG5wt7YJ4e  
t4ngeb+pQBtiuJCXuhE3sVSODlc3k0xZjJAbsYA==" -  
AsPlainText -Force  
$credential = New-Object
```



Alternatively, run this command if the key doesn't begin with a forward slash:

```
net use F: \\ws1files1.file.core.windows.net\fsx  
/u:AZURE\ws1files1  
ZftvVFdJyx6+kWBrPxl5aBa0eQhaivKnVqymG5wt7YJ4et4n  
geb+pQBtiuJCXuhE3sVSODlc3k0xZjJAbsYA==
```

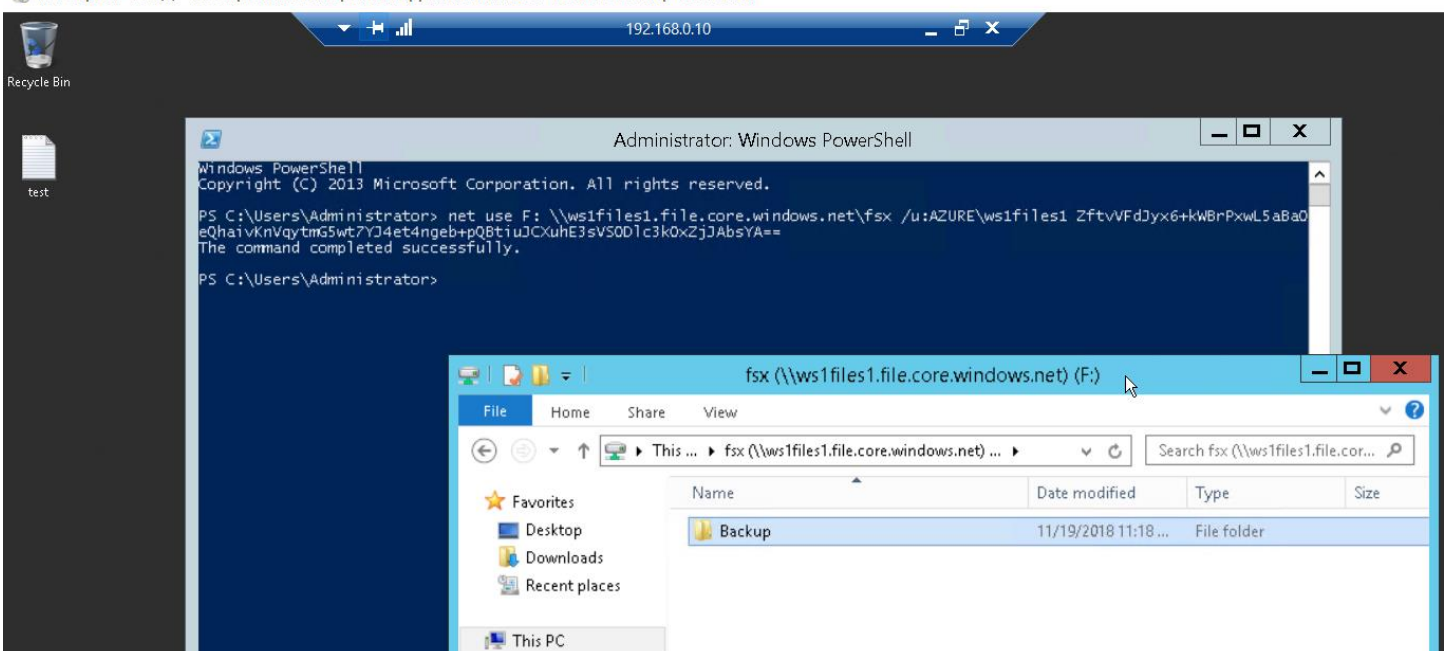
2



When connecting from a computer from outside Azure, remember to open outbound TCP port 445 in your local network. Some Internet service providers may block port 445. Check with your service provider for details.

- 6.8. Grįžkite į virtualią mašiną. Iš **wsX-onpremhst** VM per RDP prisijunkite prie **WinSrv2012R2** (192.168.0.10)
- 6.9. Įvykdysite anksčiau nukopijuotą komandą, po keleto sekundžių turėtų būti prijungtas papildomas tinklo diskas.


ws1-onprem-host(1) - ws1onprem.westeurope.cloudapp.azure.com:3389 - Remote Desktop Connection



Prijungtame diske matysite anksčiau įkeltus failus. Nukopijuokite į turinį į E:\ diską.

- 6.10. Sudiekite Azure Backup agentą ir užregistruokite (panaudodami Vault Credentials failą):

Microsoft Azure Recovery Services Agent Setup Wizard



Installation Settings

Installation Stages

Installation Settings

Proxy Configuration

Microsoft Update Opt-In

Installation

Installation Folder

Microsoft Azure Recovery Services Agent will be installed in the following folder. To choose a different installation folder, click Browse. The location specified must have at least 1 GB of free space.

C:\Program Files\Microsoft Azure Recovery Services Agent

Browse

Cache Location

Microsoft Azure Recovery Services Agent can use this to keep track of files being backed up from your computer. The location specified must have free space which is atleast 5% of the backup data.

C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch


Browse

< Back

Next >

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\Administrator\Desktop\WS1-Vault\_Mon Nov 19 2018.Vau

Browse

Backup Vault:

WS1-Vault

Region:

westeurope

Subscription Identifier:

715a1a30-ebdf-48a3-9768-8c38e8ae180a

< Previous

Next >

Finish

Cancel

Generuojamas ir išsaugomas užšifravimo raktas (reikalingas atstatymui):

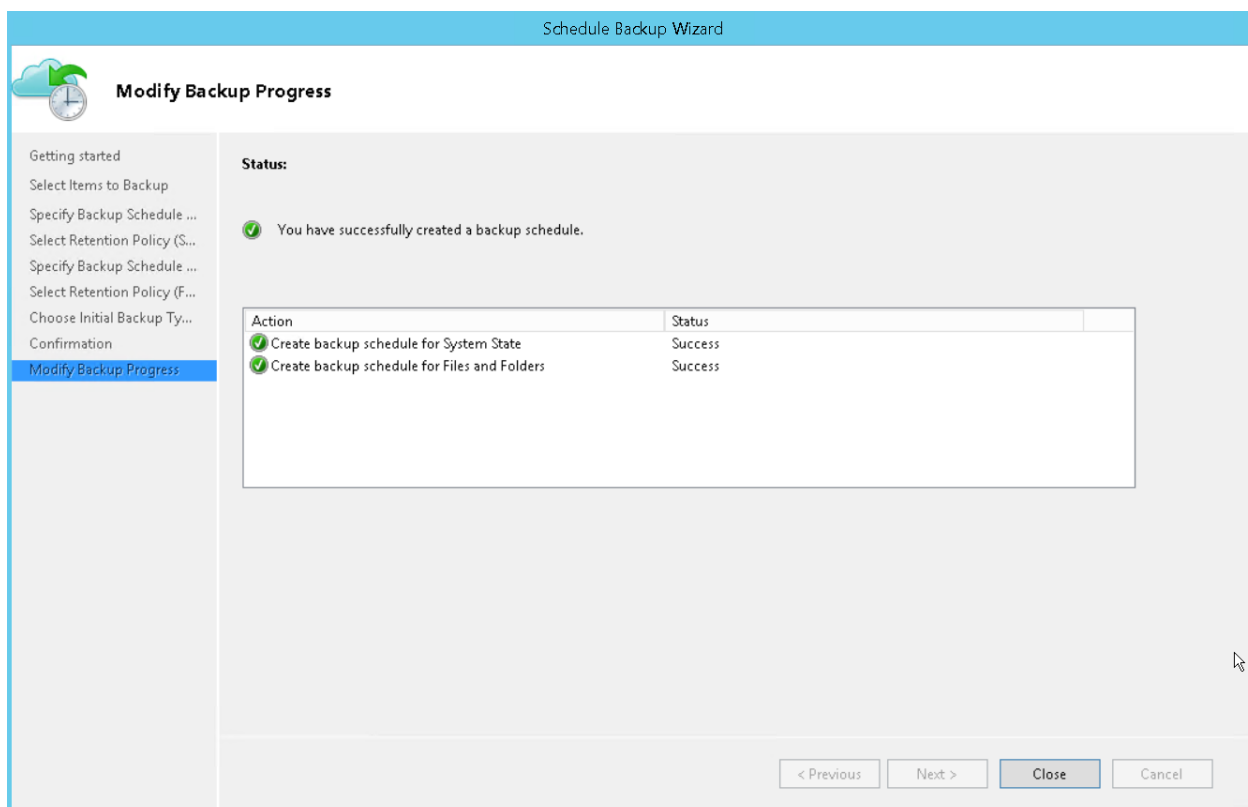
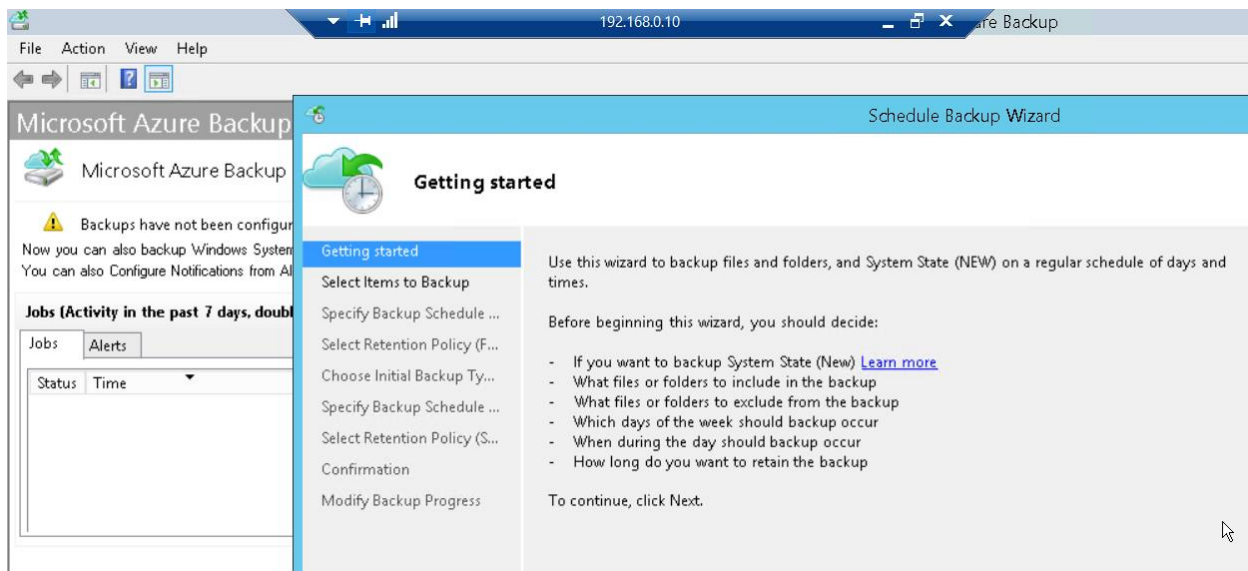
The screenshot shows the 'Encryption Setting' step of the 'Register Server Wizard'. The left sidebar has three items: 'Vault Identification', 'Encryption Setting' (which is highlighted), and 'Server Registration'. The main area contains the following text and controls:

- Header: **Encryption Setting**
- Text: Backups are encrypted to protect the confidentiality of your data.
- Text: Generate or type a passphrase to encrypt and decrypt backups from this server.
- Text: Enter Passphrase (minimum of 16 characters)
- Text input field: Contains 16 asterisks, followed by '(36)'.
- Text: Confirm Passphrase
- Text input field: Contains 16 asterisks, followed by '(36)'.
- Text: Enter a location to save the passphrase
- Text input field: Contains 'F:\', followed by a dropdown arrow.
- Text: Browse
- Text: If your passphrase is lost or forgotten, the data cannot be recovered. Microsoft Online Services does not save or manage this passphrase. It is strongly recommended you save your passphrase to an external location like a USB drive or network drive.
- Buttons: < Previous, Next >, Finish, Cancel.

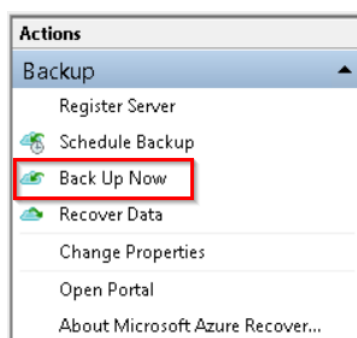
The screenshot shows the 'Server Registration' step of the 'Register Server Wizard'. The left sidebar has three items: 'Vault Identification', 'Encryption Setting', and 'Server Registration' (which is highlighted). The main area contains the following text and controls:

- Header: **Server Registration**
- Text: Microsoft Azure Backup is now available for this server.
- Text: The passphrase was saved to the following file :  
<F:\Microsoft Azure Recovery Services Agent 11 19 2018 11 32 47.txt>
- Text: Before your server is backed up you must configure and schedule backup options.
- Text: ☒ Launch Microsoft Azure Recovery Services Agent
- Buttons: < Previous, Next >, Close, Cancel.

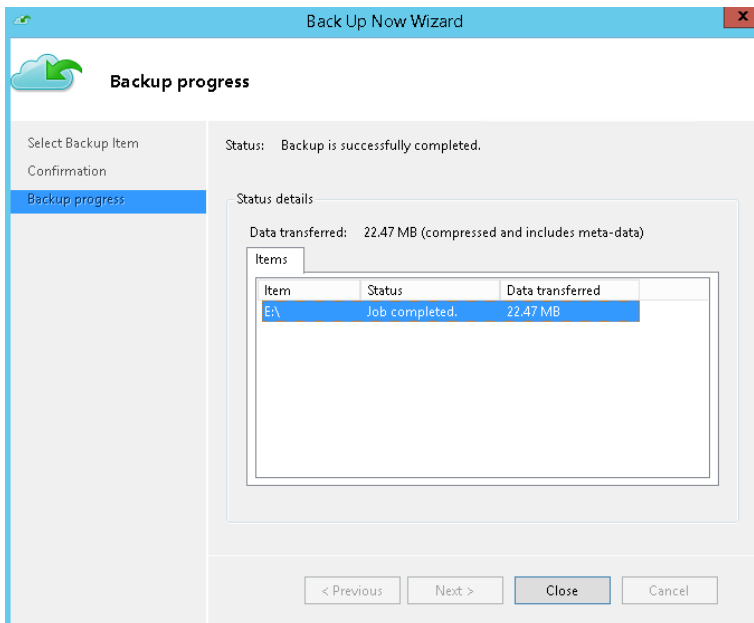
- 6.11. Pasirinkite „Schedule Backup“ ir panagrinėkite galimus variantus, sukurkite keletą skirtingų taisyklių „Files and Folders“ atsarginėms kopijoms ir „System State“ atsarginėms kopijoms:



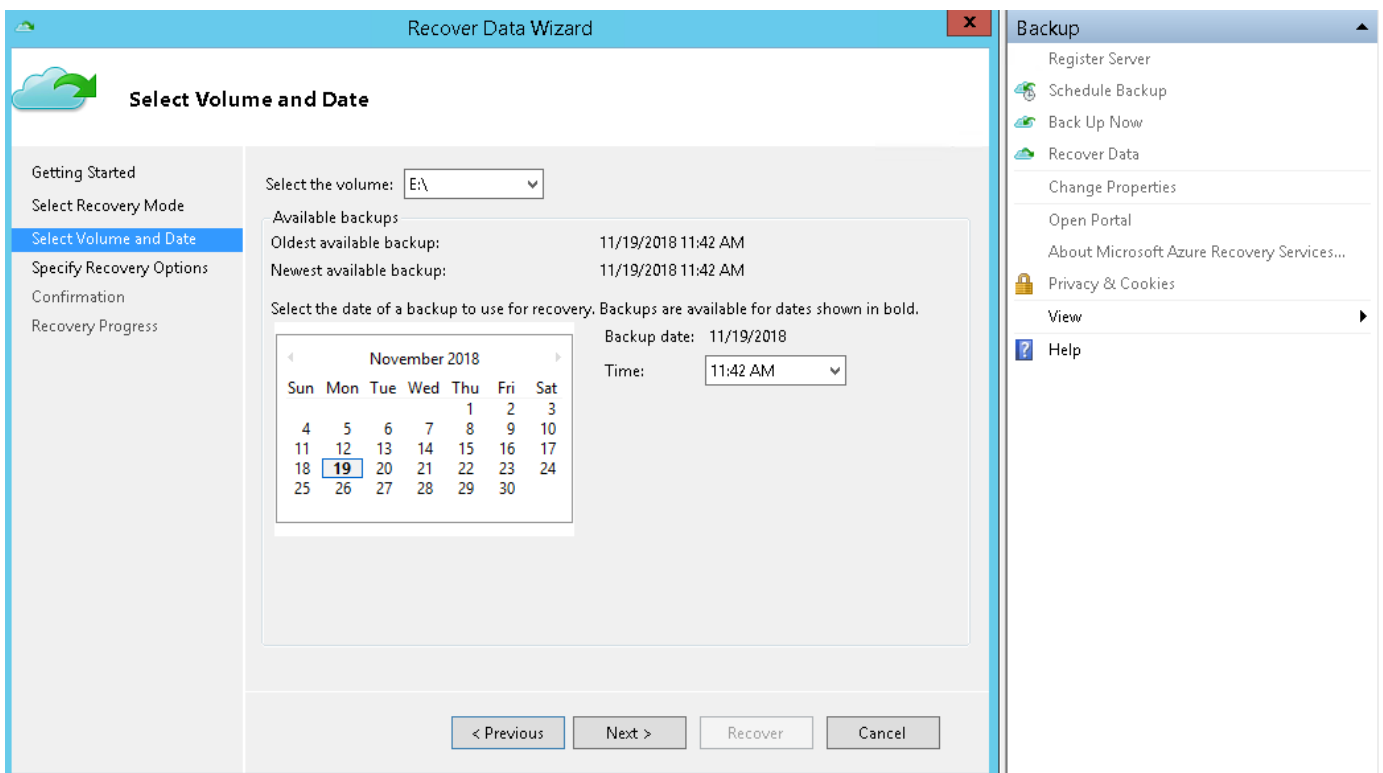
Sukūrę savo Backup politiką pasirinkite „Backup Now“:



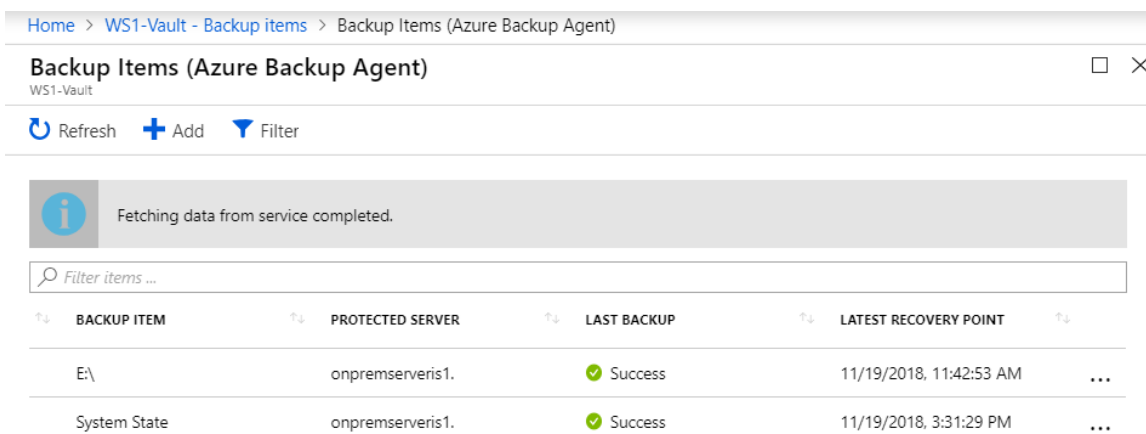




Pabandykite ištrinti ir atstatyti atsitiktinį failą/us. Pasirinkite „Recover Data“, atstatymo tašką. Panagrinėkite kokie yra atstatymo būdai ir kuo jie skiriasi.



Azure Backup saugomus objektus galite rasti Azure Portal, Recovery Services Vault, Backup Items:



## 7. Azure Site Recovery infrastruktūros paruošimas.

\*Deployment planner: <http://aka.ms/asr-deployment-planner> (Jei liks laiko)

7.1. Paruošiame nustatymus: workshop'o atveju serverio lokacija "onprem", su Hyper-V, be VMM:

The screenshot shows the Azure Site Recovery console for a Recovery Services vault named 'WS1-Vault'. The left sidebar shows the 'Site Recovery' menu item highlighted with a red box and a red circle '1'. The main area is divided into three panes. The first pane, 'WS1-Vault - Site Recovery', shows a list of settings with 'Prepare Infrastructure' highlighted by a red box and a red circle '2'. The second pane, 'Prepare infrastructure', shows a list of tasks with '1 Protection goal Select' highlighted by a red box and a red circle '3'. The third pane, 'Protection goal', shows a list of questions with 'On-premises' selected for 'Where are your machines located?' (red box and circle '4'), 'To Azure' selected for 'Where do you want to replicate your machines to?' (red box and circle '5'), 'Yes, with Hyper-V' selected for 'Are your machines virtualized?' (red box and circle '6'), and 'No' selected for 'Are you using System Center VMM to manage your Hyper-V hosts?' (red box and circle '7').

7.2. Deployment planning žingsnyje pasirenkame "I've done it" ir praleidžiame.

7.3. Sukuriame "Hyper-V Site".

The screenshot shows the Azure Site Recovery console for the same Recovery Services vault. The first pane, 'Prepare infrastructure', shows a list of tasks with '3 Source Prepare' highlighted by a red box. The second pane, 'Prepare source', shows a list of tasks with '+ Hyper-V Site' highlighted by a red box. The third pane, 'Create Hyper-V site', shows a list of tasks with 'Name' highlighted by a red box and the value 'OnpremDC' entered in the text field.

7.4. Pridedame Hyper-V host'ą, sekite instrukcijas, atsisiųskite agentą, registracijos raktą ir juos nukopijuokite į "WSX-Onprem-Host" VM. Sudiekite pagal instrukciją.

### Prepare infrastructure

WS1-Vault

These are long running tasks done on-premises.

- Protection goal  
Hyper-V VMs to Azure ✓
- Deployment planning  
I have done it ✓
- Source  
Prepare >
- Target  
Prepare >
- Replication settings  
Prepare >

### Prepare source

WS1-Vault

+ Hyper-V Site + **Hyper-V Server**

**✓ Step 1: Select Hyper-V site**

\* Hyper-V Site  
OnpremDC

**→ Step 2: Ensure Hyper-V servers are added**

0 Found... Click on +Hyper-V server in top command bar to add a Hyper-V server to the site. This may take approximately 15 min to 30 min.

### Add Server

WS1-Vault

Server type  
Hyper-V server

**i** Adding Hyper-V server may take 15 minutes to 30 minutes

Register your Hyper-V host(s)  
On-premises

- Make sure the host is running Windows Server 2012 R2 or above. [Learn more.](#)
- Configure Proxy setting and ensure each host can access the [Service URLs](#)
- Download the installer for the Microsoft Azure Site Recovery Provider.**
- Download the vault registration key to register the host in a Hyper-V site**  
OnpremDC  
**Download**
- Install the Provider on the Hyper-V host and use the registration key to register the host in the vault. [Learn more.](#)

7.5. Nukopijuokite du parsijstus failus į hostą, sudiekite Azure Site Recovery agentą:

ws1-onprem-host (1) - 13.69.57.174:3389 - Remote Desktop Connection

Recycle Bin

ream

ASR

File Home Share View Manage

ASR

Name	Date modified	Type	Size
AzureSiteRecoveryProvider (3)	11/18/2018 6:05 PM	Application	52,914 KB
WS1-Vault_OnpremDC_Sun Nov 18 2018.VaultCredentials	11/18/2018 6:05 PM	VAULTCREDENTIAL...	5 KB

2 items 1 item selected 51.6 MB

Azure Site Recovery Provider Setup (Hyper-V server)

### Provider Installation

● Microsoft Update

● **Installation**

Specify where you want to install the Microsoft Azure Site Recovery Provider. This setup will install Azure Site Recovery Provider and Azure Recovery Services Agent on this computer.

Installation Location C:\Program Files\Microsoft Azure Site Recovery Provider **Browse**

Installing Azure Recovery Services Agent

✓ Configuring Service

**Install** **Finish**

7.6. Užregistruokite hostą su VaultCredentials failu:

Microsoft Azure Site Recovery Registration Wizard

## Vault Settings...

Select the registration key file you downloaded from the Azure Site Recovery portal and specify vault settings. [Learn More](#)

Key file: WS1-Vault\_OnpremDC\_Sun Nov 18 2018.VaultCredentials Browse

Subscription: 715a1a30-ebdf-48a3-9768-8c38e8ae180a

Vault name: WS1-Vault

Hyper-V site name: OnpremDC

7.7. Hoste atidarykite “Microsoft Azure Backup”, nustatykite išsiunčiamų duomenų greičio apribojimus darbo valandomis:

Microsoft Azure Backup

File Action View Help

Microsoft Azure Backup supports scheduled backups of files and folders to an c

Click on "Register Server" in the Actions pane to register server using your Microsoft Azure Backup account

Actions: Backup, Register Server, **Change Properties**, View

Microsoft Azure Backup Properties

Encryption Proxy Configuration **Throttling**

☒ Enable internet bandwidth usage throttling for backup operations

Work hours: 300.0 Mbps

Non-work hours: 1000.0 Mbps

Work hours: 9 AM 5 PM

Work days: ☐ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday

7.8. Per 5-15 minučių jūsų “onprem” hostas turi atsirasti sąrašė:

Prepare infrastructure WS1-Vault

These are long running tasks done on-premises.

1 Protection goal Hyper-V VMs to Azure ✓

2 Deployment planning I have done it ✓

3 Source Prepare >

Prepare source WS1-Vault

+ Hyper-V Site + Hyper-V Server

✓ Step 1: Select Hyper-V site

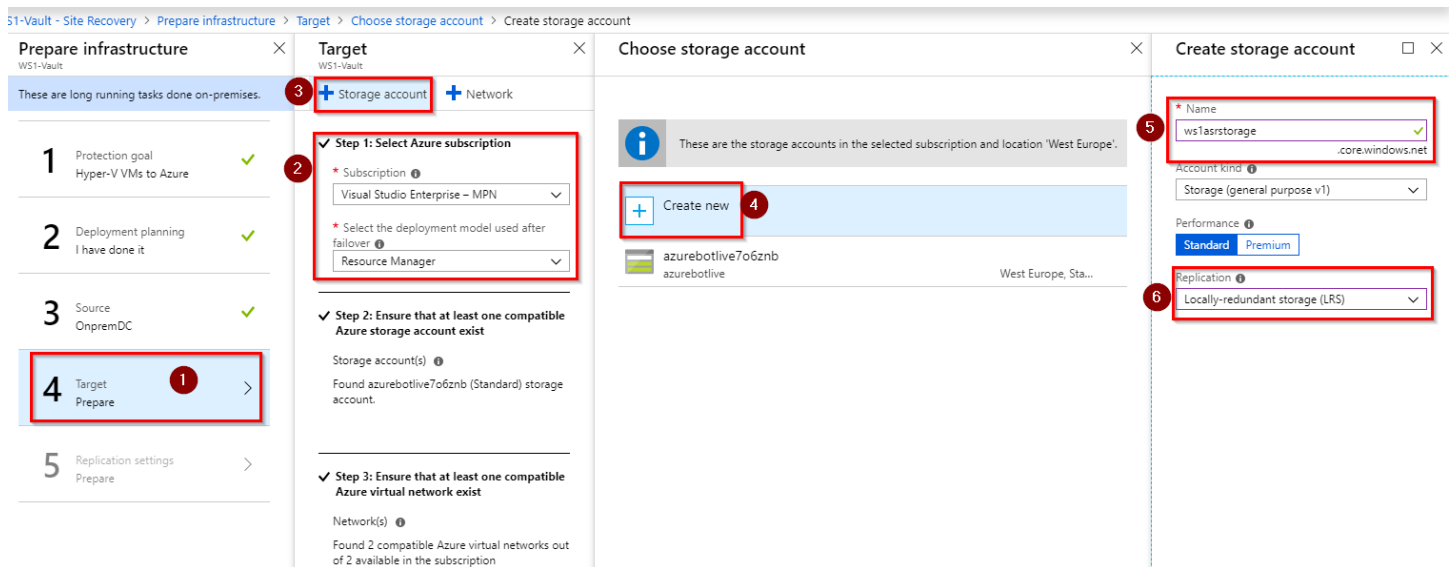
\* Hyper-V Site

OnpremDC

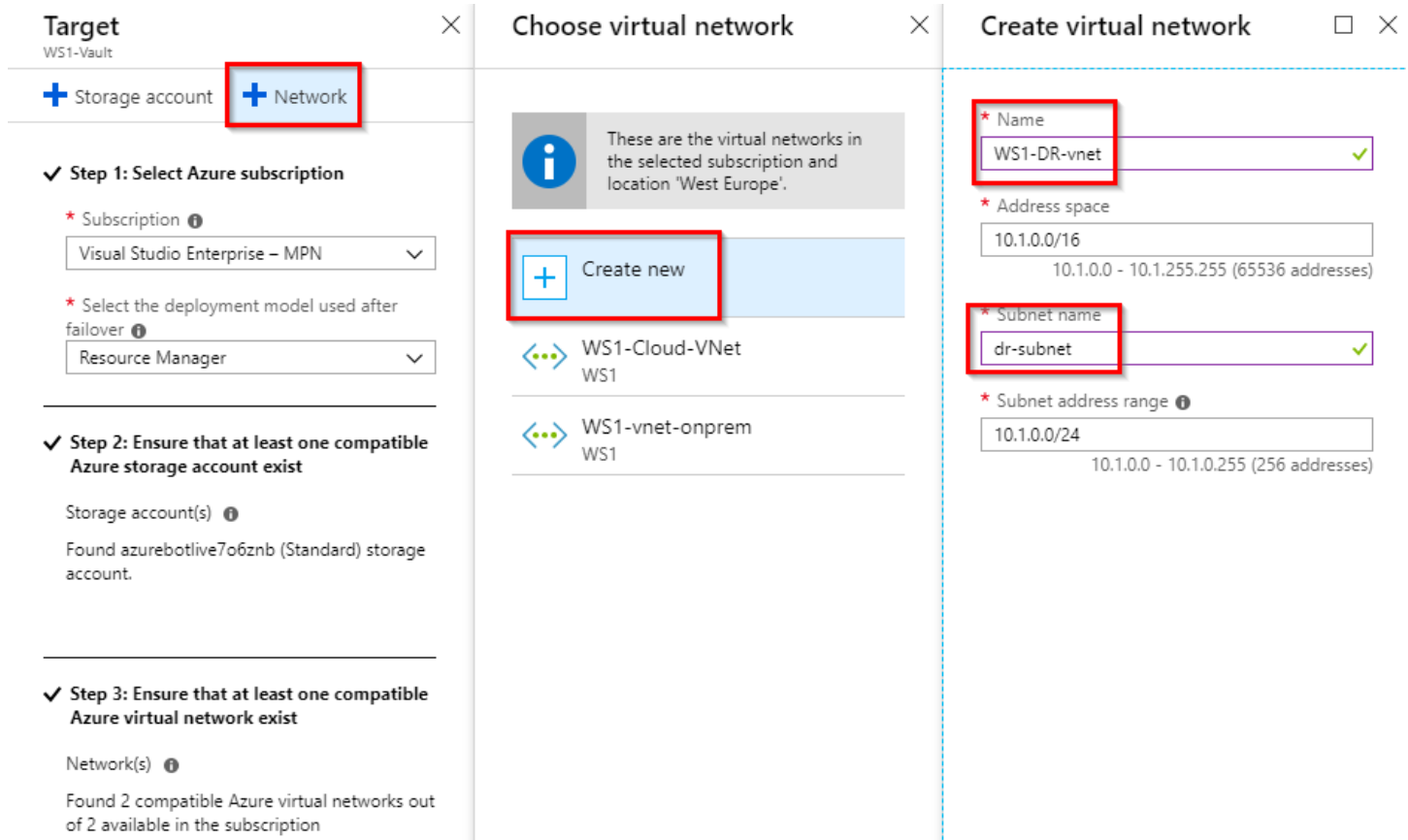
✓ Step 2: Ensure Hyper-V servers are added

ws1-onprem-host

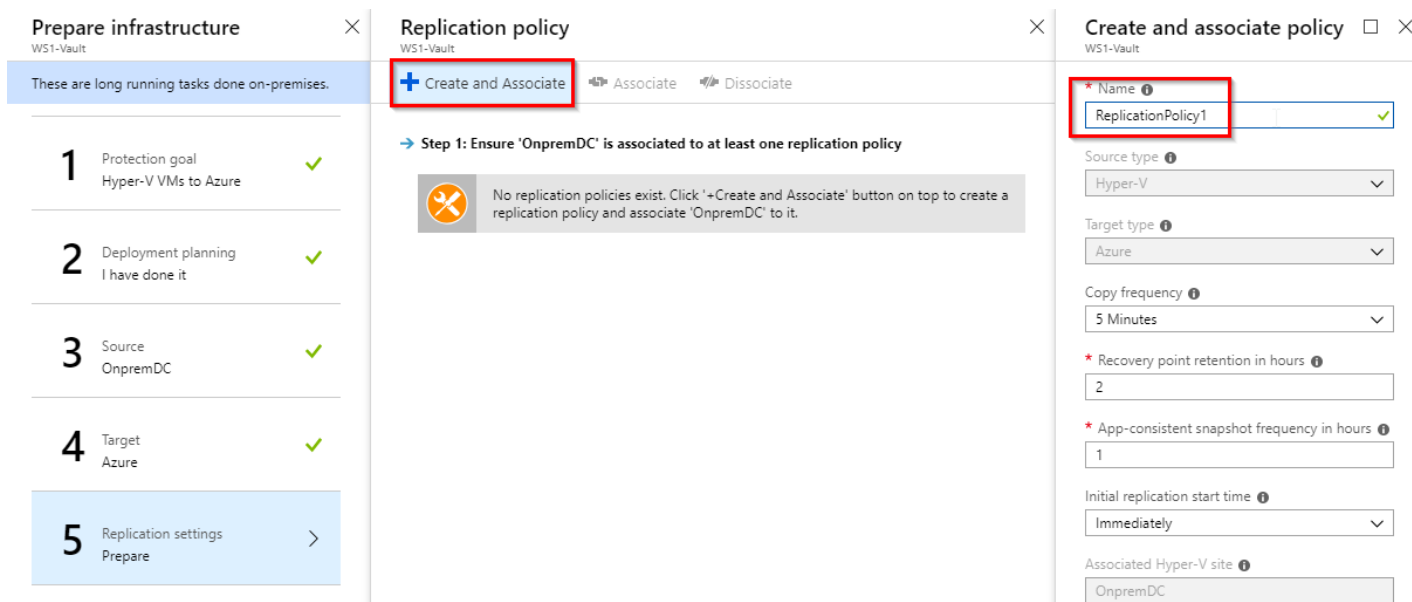
7.9. Ketvirtame paruošimo žingsnyje pridėkite papildomą “Storage account” kur bus saugomi replikuojami VM duomenys. Pavadinkite “wsXasrstorage”, pasirinkite LRS.



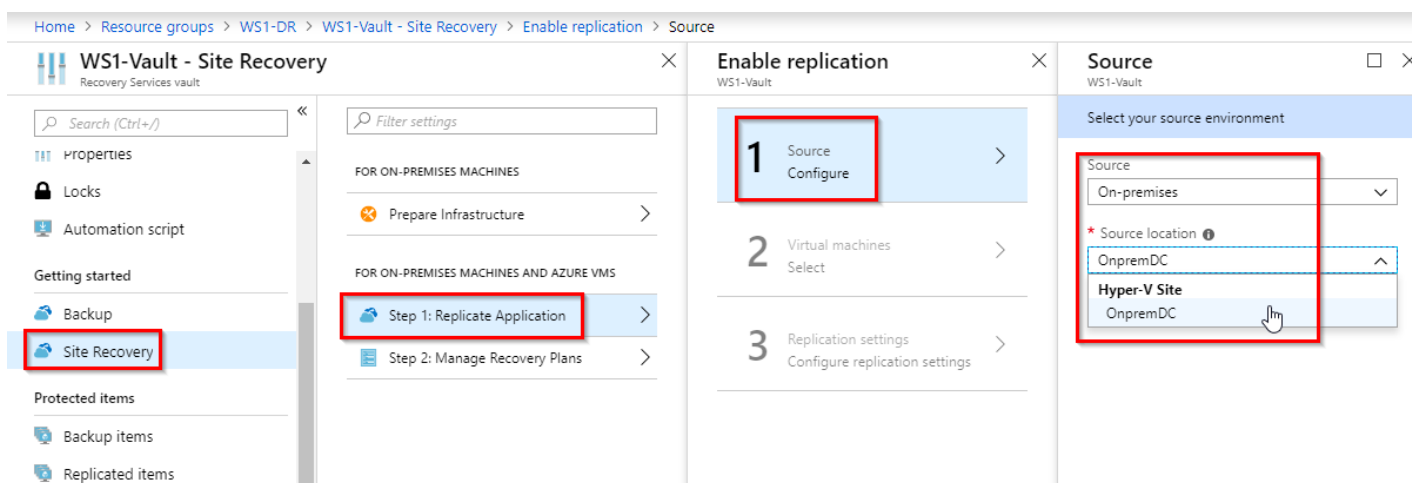
7.10. Pridėkite Azure virtualų tinklą, kurį naudos atstatomos VM. Pavadinkite “wsX-DR-vnet”. Address space ir subnet neturėtų kirstis su “onprem” tinklo režiais.



7.11. Penktame žingsnyje kuriate “Replication policy”. Sukurkite taisyklės pavadinimą, kitas reikšmes palikite kokios yra.



## 7.12. Ljunkite replication:



## 7.13. Postfailover grupę pasirinkite WSX-DR, Storage account ws1asrstorage (arba sukurkite naują), virtualus tinklas kurį naudos VM – WSX-DR-vnet:

Enable replication

WS1-Vault

1 Source

OnpremDC

✓

2 Target

Configure

>

3 Virtual machines

Select

>

4 Properties

Configure properties

>

5 Replication settings

Configure replication settings

>

Enable replication

Target

WS1-Vault

Select your target settings for recovery

\* Target

Azure

\* Subscription

Visual Studio Enterprise – MPN

Post-failover resource group

WS1-DR

\* Post-failover deployment model

Resource Manager

\* Storage account

ws1asrstorage

Azure network

Configure now for selected machines.

Post-failover Azure network

WS1-DR-vnet

Subnet

dr-subnet (10.1.0.0/24)

OK

7.14. Pasirinkite VM, kurias replikuosite (nesirinkite tik „linux1“ vm):

Enable replication

WS1-Vault

1 Source

OnpremDC

✓

2 Target

Azure

✓

3 Virtual machines

Select

>

Select virtual machines

Finished retrieving data.

Filter items...

linux1

☒ WinSrv2012R2

☒ CentOS7VM

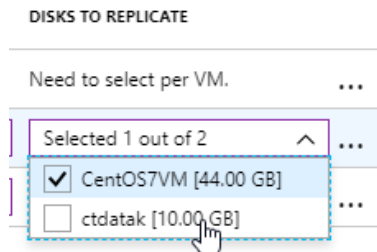
7.15. Nurodykite VM OS tipą, OS diską:

Recovery > Enable replication > Configure properties

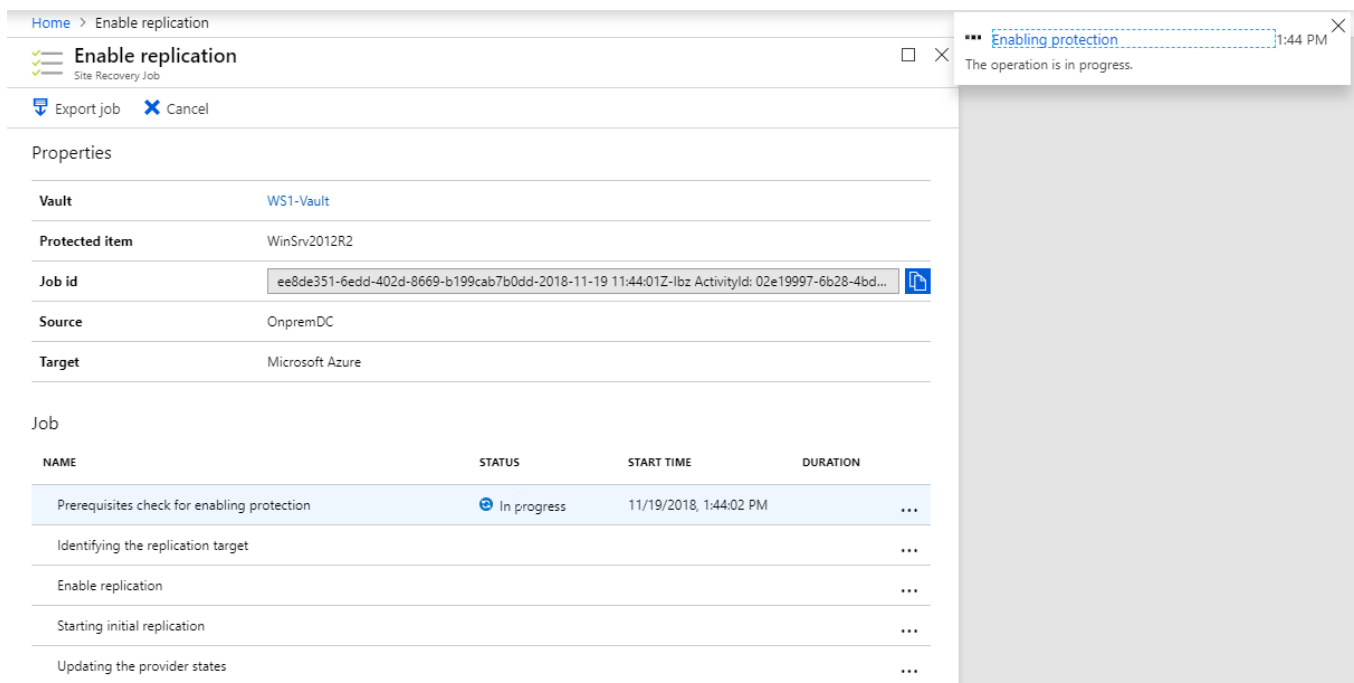
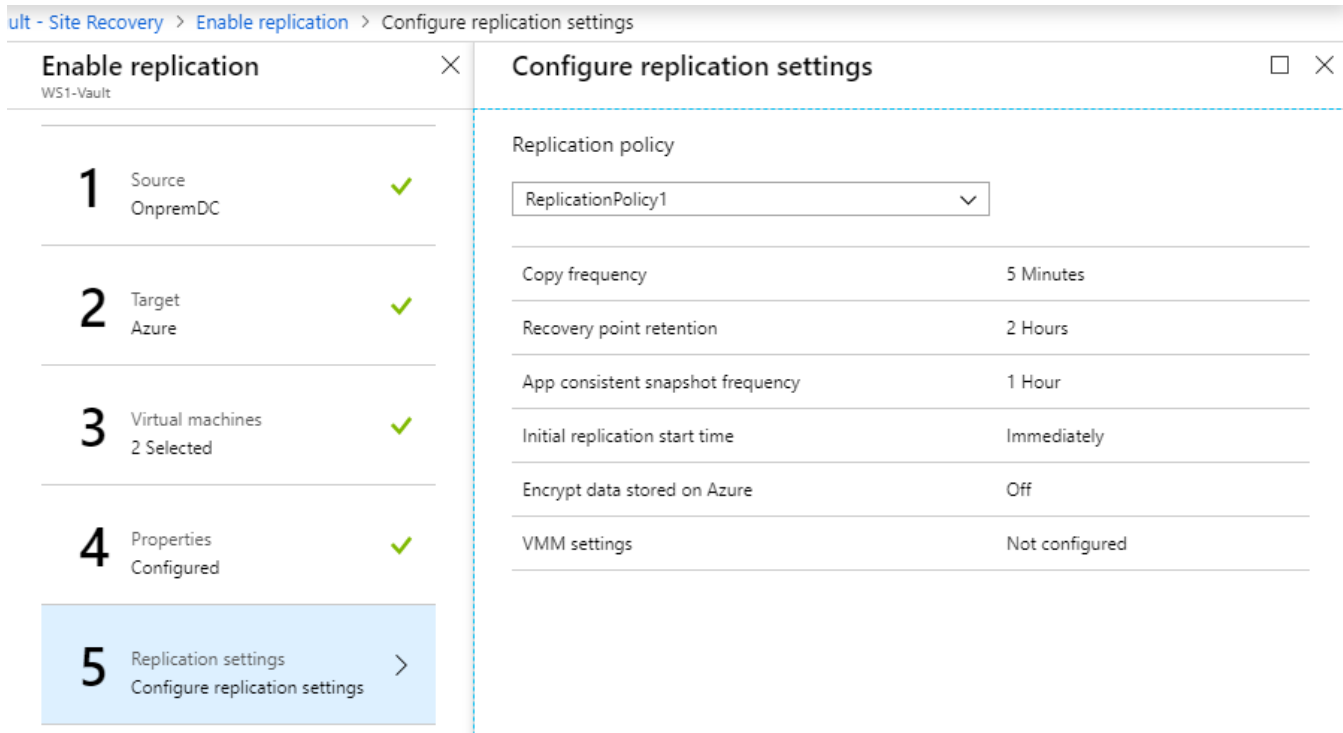
Configure properties

NAME	OS TYPE	OS DISK	DISKS TO REPLICATE
Defaults	Select	Need to select per VM.	Need to select per VM. ...
CentOS7VM	Linux	CentOS7VM	All Disks [2] ...
WinSrv2012R2	Windows	VM2-ws2012r2	All Disks [2] ...

7.16. Yra galimybė pasirinkti kuris diskas nebus replikuojamas:



7.17. Priskirkite Replication Policy kurią sukūrėte anksčiau ir įjunkite apsaugą:



7.18. Stebėkite replikavimo būseną:



Home > WS1-Vault - Replicated items

## WS1-Vault - Replicated items

Recovery Services vault

Search (Ctrl+/)

Refresh Replicate Columns Filter

You can run your machines on managed disks after a failover or migration from on-premises to Azure. Set the option to use managed disks in Replicated item -> Settings -> Compute and Network.

Last refreshed at: 11/19/2018, 1:45:48 PM

Finished loading data from service.

Filter items...

NAME	REPLICATION H...	STATUS	ACTIVE LOCATI...	REPLICATION P...	RPO	OPERATING SY...	DAILY DATA CH...	IP ADDRESS
WinSrv201...	Healthy	0% synchroni...	OnpremDC	ReplicationPo...	-	Windows	-	...
CentOS7VM	Healthy	0% synchroni...	OnpremDC	ReplicationPo...	-	Linux	-	...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Properties

Locks

Automation script

Getting started

Backup

Site Recovery

Protected items

Backup items

Replicated items

7.19. Nusipelnėte pertraukos. Pailsėkite 5 minutes.

7.20. Pasibaigus pradiniam replikavimui statusas turi pasikeisti į „Protected“:

NAME	REPLICATION HEAL...	STATUS	ACTIVE LOCATION	REPLICATION POLI...	RPO	OPERATING SYS
WinSrv2012R2	Healthy	Protected	OnpremDC	ReplicationPolicy1	3 seconds	Windows
CentOS7VM	Healthy	Protected	OnpremDC	ReplicationPolicy1	2 seconds	Linux

7.21. Apsaugotai VM galima pakeisti nustatymus: dydį, tinklą, pavadinimą ir t.t. Pakeiskite VM dydį į F1s

Home > WS1-Vault - Replicated items > WinSrv2012R2 - Compute and Network

## WinSrv2012R2 - Compute and Network

Replicated items

Save Discard

Compute properties

PROPERTIES	ON-PREMISES	MICROSOFT AZURE
Name	WinSrv2012R2	WinSrv2012R2
Resource group	-	WS1-DR
Size	2 cores, 2.00 GB memory, 1 NICs	F2s_v2 (2 cores, 4 GB memory, 1 NICs)
Availability set	-	No applicable availability sets in the resource group
Use managed disks	-	No

Network properties

PROPERTIES	TARGET NETWORK
Virtual network	WS1-DR-vnet

Network interfaces

ON-PREMISES NETWORK NAME	TARGET SUBNET	TARGET IP	TARGET NETWORK INTERFACE TYPE
InternalNATSwitch	dr-subnet	DHCP assigned	Primary

Overview

General

Properties

Compute and Network

Disks

## 8. Test failover – VM atstatymas izoliuotoje aplinkoje nepaveikiant onprem VM

### 8.1. Vault'e pasirinkite apsaugotą VM, pasirinkite „Test Failover“:

The screenshot shows the Azure portal interface for a replicated VM named 'WinSrv2012R2'. The 'Test Failover' tab is selected and highlighted with a red box. The left sidebar shows the 'Overview' tab selected. The main content area displays the 'Test Failover' configuration, including the source location (OnpremDC), VM ID, target size (Standard\_F1s), and target network (WS1-DR-vnet). The 'Health and status' section shows the replication health as 'Healthy' and the status as 'Protected'. The 'Failover readiness' section shows the last successful test failover as 'Never performed successfully' and configuration issues as 'No issues'. The 'Errors' and 'Events' sections show no errors or events.

### 8.2. Pasirinkite vėliausią recovery point, priskirkite DR virtualų tinklą, startuokite Failover procesą:

The screenshot shows the 'Test failover' dialog box for the VM 'WinSrv2012R2'. The 'Failover direction' section shows the 'From' location as 'OnpremDC' and the 'To' location as 'Microsoft Azure'. The 'Recovery Point' section shows the chosen recovery point as 'Latest processed (low RTO) (11/19/2018, 1:...'.

**\* Azure virtual network**

WS1-DR-vnet

It is recommended that for a test failover you use a network different from production network (as specified under Compute and Network settings of the virtual machine). [Learn more.](#)

### 8.3. Po kurio laiko turime testinės mašinos kopiją debesyje. Suraskite mašiną prie visų Azure virtulių mašinų kairiajame portalo meniu „Virtual Machines“. Norėdami prisijungti šiai VM priskirkite Public IP:

Home > Virtual machines > WinSrv2012R2-test

**WinSrv2012R2-test**

Search (Ctrl+/)

Overview

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

Settings

- Networking**
- Disks
- Size
- Security
- Extensions
- Continuous delivery (Preview)
- Availability set
- Configuration
- Identity
- Properties
- Locks
- Automation script

Connect Start Restart Stop Move Delete Refresh

'WinSrv2012R2-test' is not using Managed Disks. Migrate to Managed Disks to get more benefits. →

Resource group (change) ws1-dr

Status Running

Location West Europe

Subscription (change) Visual Studio Enterprise – MPN

Subscription ID 715a1a30-ebdf-48a3-9768-8c38e8ae180a

Computer name -

Operating system Windows

Size Standard F1s (1 vcpu, 2 GB memory)

Public IP address -

Virtual network/subnet WS1-DR-vnet/dr-subnet

DNS name -

Tags (change) Click here to add tags

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

CPU (average)

Network (total)

#### 8.4. Pasirinkite tinklo adapterio nustatymus:

WinSrv2012R2-test - Networking

Virtual machine

Search (Ctrl+/)

Overview

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

Settings

- Networking**

Attach network interface Detach network interface

**Network Interface:** WinSrv2012R2-test853dd9bd-346a-40b8-a09a-84129aa24717 Effective security rules

Topology

Virtual network/subnet: WS1-DR-vnet/dr-subnet Public IP: None Private IP: 10.1.0.4 Accelerated networking: Disabled

This network interface does not contain network security groups

**APPLICATION SECURITY GROUPS**

Configure the application security groups

#### 8.5. Pasirinkite "IP configurations":

Home > Virtual machines > WinSrv2012R2-test - Networking > WinSrv2012R2-test853dd9bd-346a-40b8-a09a-84129aa24717 - IP configurations

**WinSrv2012R2-test853dd9bd-346a-40b8-a09a-84129aa24717 - IP configurations**

Network interface

Search (Ctrl+/)

Overview

- Activity log
- Access control (IAM)
- Tags

Settings

- IP configurations**
- DNS servers
- Network security group
- Properties
- Locks
- Automation script

Support + troubleshooting

- Effective security rules
- Effective routes
- New support request

+ Add Save Discard

IP forwarding settings

IP forwarding Disabled Enabled

Virtual network WS1-DR-vnet

IP configurations

\* Subnet dr-subnet (10.1.0.0/24)

Search IP configurations

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS
ipConfigWinSrv20...	IPv4	Primary	10.1.0.4 (Dynamic)

#### 8.6. Įjunkite "Public IP", sukurkite naują unikalų pavadinimą, išsaugokite nustatymus:

... > WinSrv2012R2-test853dd9bd-346a-40b8-a09a-84129aa24717 - IP configurations > ipConfigWinSrv2012R2-test853dd9bd-346a-40b8-a09a-84129aa24717 > Choose public IP address > Create public IP address

ipConfigWinSrv2012R2-test853dd9bd-346a-40b8-a09a-84129aa24717

Save Discard

Public IP address settings

Public IP address

Disabled Enabled

IP address

Configure required settings

Private IP address settings

Virtual network/subnet

WS1-DR-vnet/dr-subnet

Assignment

Dynamic Static

\* IP address

10.1.0.4

Choose public IP address

Dynamic public IP addresses that are not in use won't have an IP address assigned to them.

These are the public IP addresses in the selected subscription and location 'West Europe'.

Create new

ws1-onprem-host-ip  
WS1 137.117.137.138 ...

WS2-onprem-host-pip-f3c5b3ec7d43426aadb92cbf6a0b14e2  
WS2

WS3-onprem-host-pip-882db35f7b29425c91e91a4845c86548  
WS3

Create public IP address

\* Name

ip2012temp

SKU

Basic Standard

Assignment

Dynamic Static

## 8.7. Prisijunkite prie naujai sukurtos VM:

Home > Virtual machines > WinSrv2012R2-test

WinSrv2012R2-test

Virtual machine

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Disks

Size

Security

Connect Start Restart Stop Move Delete Refresh

"WinSrv2012R2-test" is not using Managed Disks. Migrate to Managed Disks to get more benefits. →

Resource group (change)  
ws1-dr

Status  
Running

Location  
West Europe

Subscription (change)  
Visual Studio Enterprise – MPN

Subscription ID  
715a1a30-ebdf-48a3-9768-8c38e8ae180a

Tags (change)  
Click here to add tags

Computer name  
-

Operating system  
Windows

Size  
Standard F1s (1 vcpu, 2 GB memory)

Public IP address  
137.117.246.92

Virtual network/subnet  
WS1-DR-vnet/dr-subnet

DNS name  
wsdrvm1.westeurope.cloudapp.azure.com

## 8.8. Patikrinkite ar pasiekiami IIS svetainė per VM Public IP.

## 8.9. Išvalykite Test Failover metu sukurtą VM ir jos resursus:

Home > Recovery Services vaults > WS1-Vault - Replicated items > WinSrv2012R2

WinSrv2012R2

Replicated items

Search (Ctrl+/)

Overview

General

Properties

Compute and Network

Disks

Planned Failover Failover Test Failover Cleanup test failover Commit Resynchronize Change recovery point

Cleanup test failover

Essentials

Health and status

Replication Health Warning

Status Cleanup test failover pending

RPO 2 secs [As on 11/19/2018, 3:31:43 PM]

Failover readiness

Last successful Test Failover -

Configuration issues No issues

Latest recovery points

Click above to see the latest recovery points.

ult - Replicated items > WinSrv2012R2 > Test failover cleanup

☒ Cleanup test failover
 Commit
 Resynchronize
 Change recovery point
 More

### Failover readiness

**Last successful Test Failover -**

**Configuration issues** ✓ No issues

**Latest recovery points**  
Click above to see the latest recovery points.

Events - Last 72 hours(1)

TIME	EVENT NAME	SEVERITY
11/19/2018, 2:40:11 PM	Virtual machine health is in...	Warning

Notes

Testas sėkmingas.

☒ Testing is complete. Delete test failover virtual machine(s).

OK

8.10. Patikrinkite ar prie VM sąrašo neliko testinės mašinos (Azure portale „Virtual Machines“ skiltis“).

## 9. Failover (avarijos imitacija).

Failover metu priešingai nei „Test failover“ yra paliečiamos ir „onprem“ esančios VM. Jos išjungiamos automatiškai (jei jos „avarijos atveju“ apskritai veikia“). Naudojama netikėto gedimo metu, VM atstatoma iš paskutinių turimų replikuotų duomenų.

Planned failover naudojamas atliekant profilaktikos darbus onprem. Kuomet yra galimybė tvarkingai perjungti, susinchronizuoti paskutinius duomenis.

### 9.1. Išbandykite Planner failover ir Failover scenarijus.

Home > WS1-Vault - Replicated items > WinSrv2012R2 > Failover

Planned Failover **Failover** Test Failover Cleanup test failover Commit Resynchronize Change recovery point Complete Migration

Essentials

**Health and status**

Replication Health: Healthy  
Status: Protected  
RPO: 2 secs [As on 11/19/2018, 4:21:40 PM]

**Failover readiness**

Last successful Test Failover: 11/19/2018, 2:04:24 PM  
Configuration issues: No issues

**Latest recovery points**

Click above to see the latest recovery points.

**Errors(0)**

No errors

**Events - Last 72 hours(2)**

TIME	EVENT NAME	SEVERITY
11/19/2018, 4:19:43 PM	Virtual machine health is in OK...	Information
11/19/2018, 2:40:11 PM	Virtual machine health is in Wa...	Warning

**Failover**

WinSrv2012R2

**Failover direction**

From: OnpremDC  
To: Microsoft Azure

**Recovery Point**

Choose a recovery point: Latest processed (low RTO) (11/19/2018, 4:21:40 PM)

☒ Shut down virtual machine and synchronize the latest data. If you do not select this option, or you select this option and the attempt fails, the latest recovery point will be used.

**OK**

### 9.2. Pasibaigus failover procesui, perjungimui, spauskite „Commit“:

Home > WS1-Vault - Replicated items > CentOS7VM

CentOS7VM

Replicated items

Search (Ctrl+J)

Planned Failover **Failover** Test Failover Cleanup test failover **Commit** Resynchronize Change recovery point Complete Migration Reverse replicate

**Overview**

General  
Properties  
Compute and Network  
Disks

**Essentials**

**Health and status**

Replication Health: -  
Status: Planned failover finished  
RPO: -

**Failover readiness**

Last successful Test Failover: -  
Configuration issues: No issues

**Latest recovery points**

Click above to see the latest recovery points.

**Errors(0)**

No errors

**Events - Last 72 hours(0)**

TIME	EVENT NAME	SEVERITY
No events		

Patikrinkite atstatytą Azure VM, pabandykite prisijungti.

9.3. Failback procesas. Jūsų VM veikia atstatyta debesyje, onprem buvusi problema išspręsta. Reikia sinchronizuoti naujausius duomenis ir atkurti VM lokaliame Hyper-V hoste. Tai atliekama pasirenkant “Planned failover” tik šiuo atveju visas procesas vyksta į kitą pusę – replikuojama iš Azure į Onprem.

Jei Hyper-V buvusi mašina buvo ištrinta – Planned failover metu ji gali būti automatiškai atkurta su visa buvusia konfigūracija.

9.4. Pastebėkite kas vyksta Hyper-V hoste, kas vyksta prie „Planner failover“ operacijos statuso:

NAME	STATUS	START TIME	DURATION
Prerequisites check for virtual machine failback	Successful	11/19/2018, 5:33:28 PM	00:00:00
Preparing the on-premises virtual machine	Successful	11/19/2018, 5:33:28 PM	00:11:38
Initiating data synchronization	Successful	11/19/2018, 5:45:06 PM	00:21:12
Monitoring data synchronization	Successful	11/19/2018, 6:06:19 PM	00:22:10
Waiting for user input	User input required	11/19/2018, 6:28:30 PM	
Starting virtual machine failback			

Kai VM atstatoma į Hyper-V lieka patvirtinti paspaudžiant “Commit”. Tuomet vėl replikuojama iš Onprem į Azure.

NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION	REPLICATION POLICY	RPO	OPERATING SYSTEM
WinSrv2012R2	Warning	Finalize failback pend...	OnpremDC	ReplicationPolicy1	-	Windows
CentOS7VM	Warning	Finalize failback pend...	OnpremDC	ReplicationPolicy1	-	Linux

10. Recovery Plans. Panagrinėkite atstatymo planų ir papildomų veiksmų konfigūravimo galimybes. Kaip automatizuoti keleto VM atstatymą, eigą, rankinį įsiterpimą.

Home > WS1-Vault - Recovery Plans (Site Recovery)

WS1-Vault - Recovery Plans (Site Recovery)

Recovery Services vault

Search (Ctrl+/)

+ Recovery plan

Backup

Site Recovery

Protected items

Backup items

Replicated items

Manage

Backup policies

Backup Infrastructure

Site Recovery Infrastructure

Recovery Plans (Site Recovery)

Backup Reports

Filter items...

NAME	SOURCE	TARGET	CURRENT JOB	SUCCESSFUL TEST FAILOVER
To failover virtual machines individually, go to Replicated Items. To failover multiple virtual machines together, create a Recovery plan.				

Home > WS1-Vault - Recovery Plans (Site Recovery) > Create recovery plan > Select items

Create recovery plan

Select items

Name

Atstatymo-Planas

Source

OnpremDC

Target

Microsoft Azure

Allow items with deployment model

Resource Manager

Select items

0

Finished retrieving data.

Filter items...

PROTECTED ITEM	TYPE
WinSrv2012R2	Machine
CentOS7VM	Machine

Selected items

2

Atstatymo-Planas

WS1-Vault

Settings

Customize

Test failover

Cleanup test failover

More

Essentials

Recovery Services vault

WS1-Vault

Start groups

1

Source

OnpremDC

Deployment model

Resource Manager

Items in recovery plan

2

Scripts

0

Target

Microsoft Azure

All settings

Items in recovery plan

Source

2

Target

0

Atstatymo-Planas

Recovery plan

+ Group

Save

Discard

Change group

You have unsaved changes.

This recovery plan contains 2 machine(s).

STAGE NAME	DETAILS
All groups shut down	2 machines in 2 groups.
All groups failover	
Machines	2 Machines
WinSrv2012R2	Machine
CentOS7VM	Machine
Group 1: Start	1 Machine
WinSrv2012R2	Machine
Group 2: Pre-steps	1 Step
Manual: Rankinis patikrinimas	Manual action
Group 2: Start	1 Machine
CentOS7VM	Machine
Group 2: Post-steps	1 Step
Manual: Paskambinti vadui ir nura...	Manual action




11. Azure to Azure ASR

Replikavimas į kitą regioną:

Home > Virtual machines > ws1-onprem-host > Configure disaster recovery

Configure disaster recovery

ws1-onprem-host



**Welcome to Azure Site Recovery**

You can replicate your virtual machines to another Azure region for business continuity and disaster recovery needs. You can conduct periodic DR drills to ensure you meet the compliance needs. The VM will be replicated with the specified settings to the selected region so that you can recover your applications in the event of outages in source region. [Learn more about Azure Site Recovery.](#)

\* Target region

North Europe

Target settings

	SOURCE	TARGET	
Subscription	Visual Studio Enterprise – MPN	Visual Studio Enterprise – M...	?
VM resource group	WS1	(new) WS1-asr	?
Availability set	Not Applicable	Not Applicable	?
Virtual network	WS1-vnet-onprem	(new) WS1-vnet-onprem-asr	?

Storage settings

[+] Show details

A new cache storage account and 1 replica managed disk(s) will be created.

Replication settings

[+] Show details

A new recovery services vault and recovery policy will be created.

Extension settings

[+] Show details

Site Recovery manages site recovery extension updates for all your replicated items. 1 new automation account will be created.



Source region (West Europe)

Selected target region (North Europe)

Available target regions