

Azure Backup, Azure Site Recovery Workshop

2018-12-03

RVE

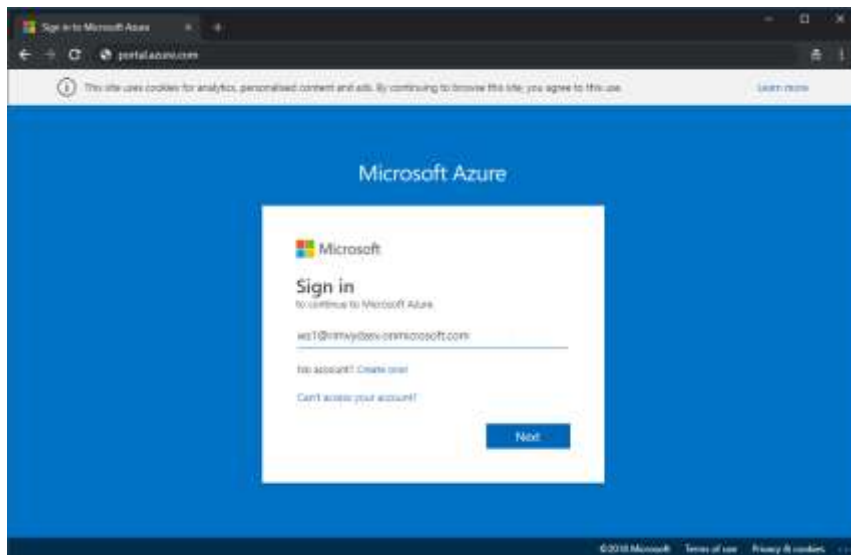
1. Azure Portal

<http://portal.azure.com>

Username: wsX@rimvydasv.onmicrosoft.com

Password: Vuhu3395

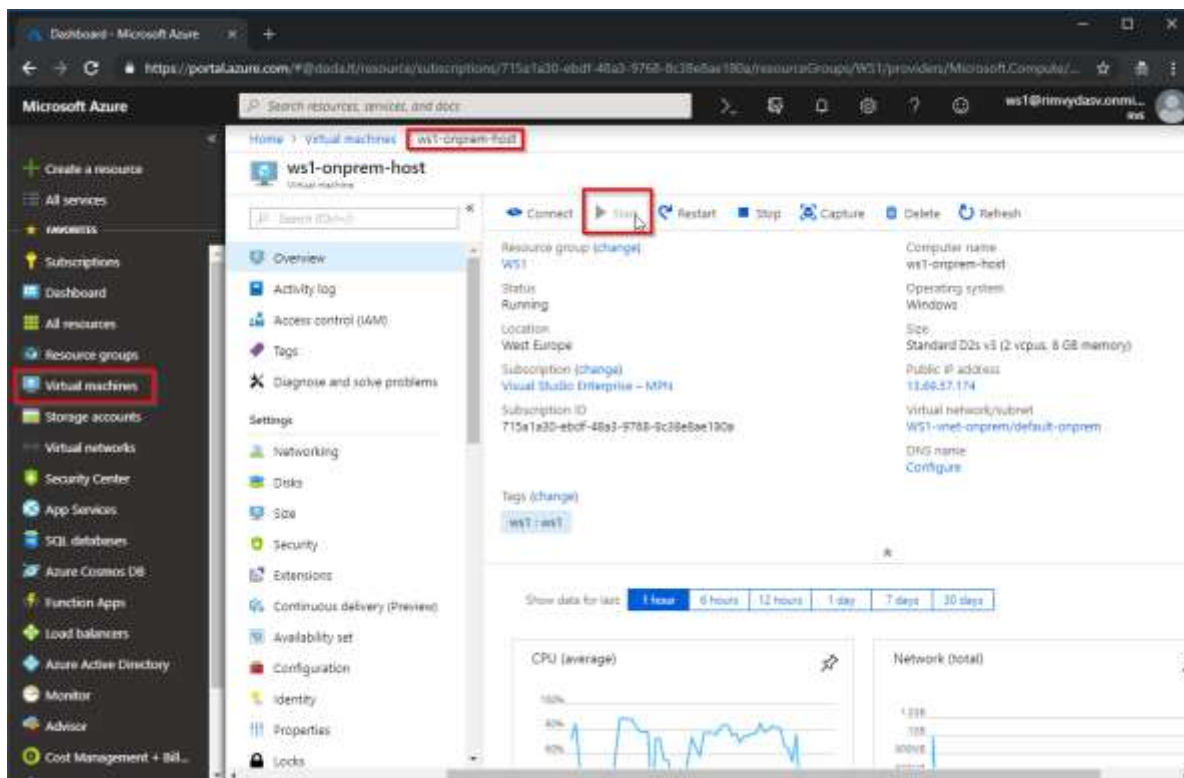
X – workshop pradžioje Jums suteiktas skaičius.



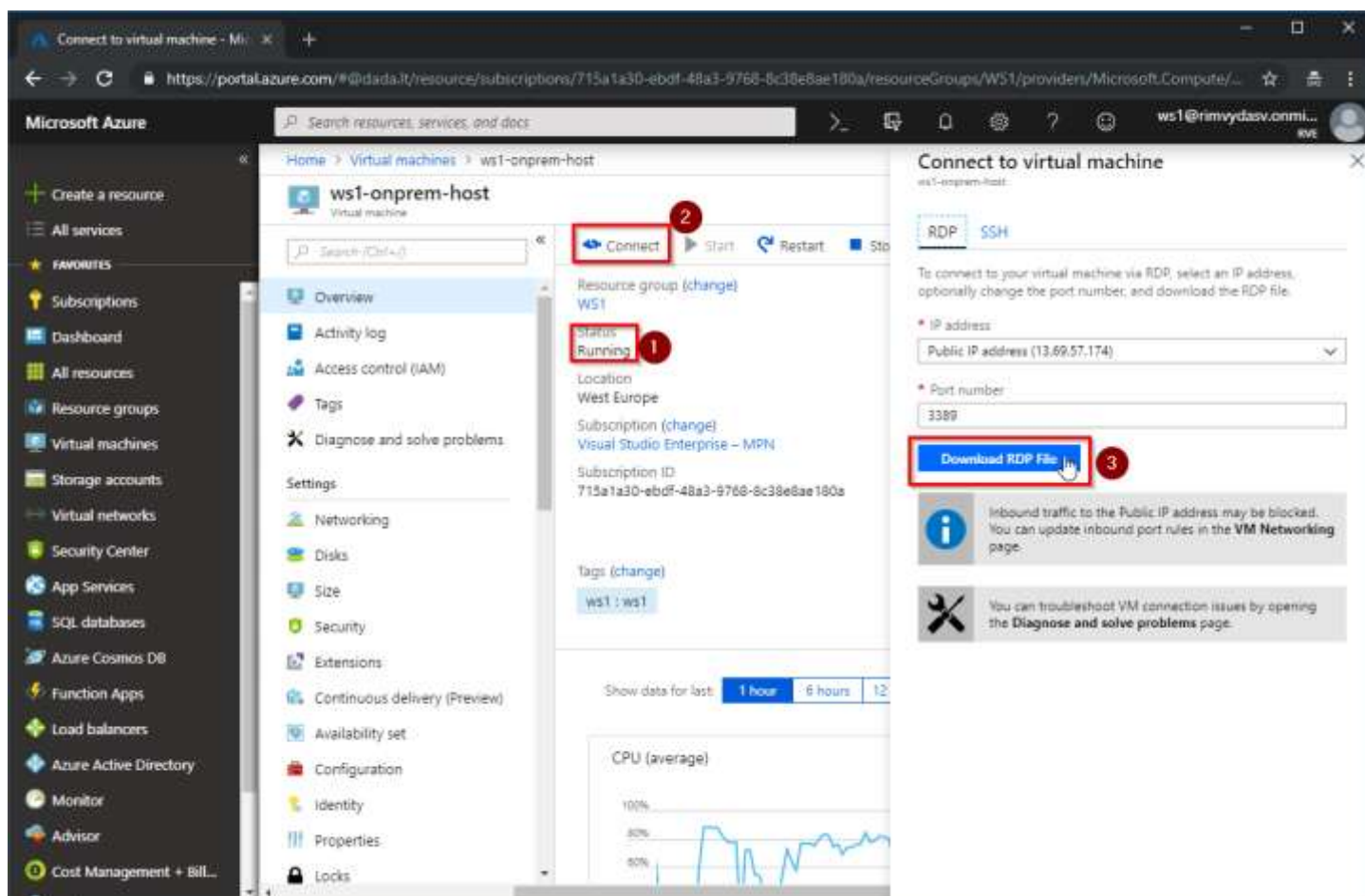
2. Resursų paruošimas, prisijungimas

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:

Username:	ws1
Password:	Vuhu33953395

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):

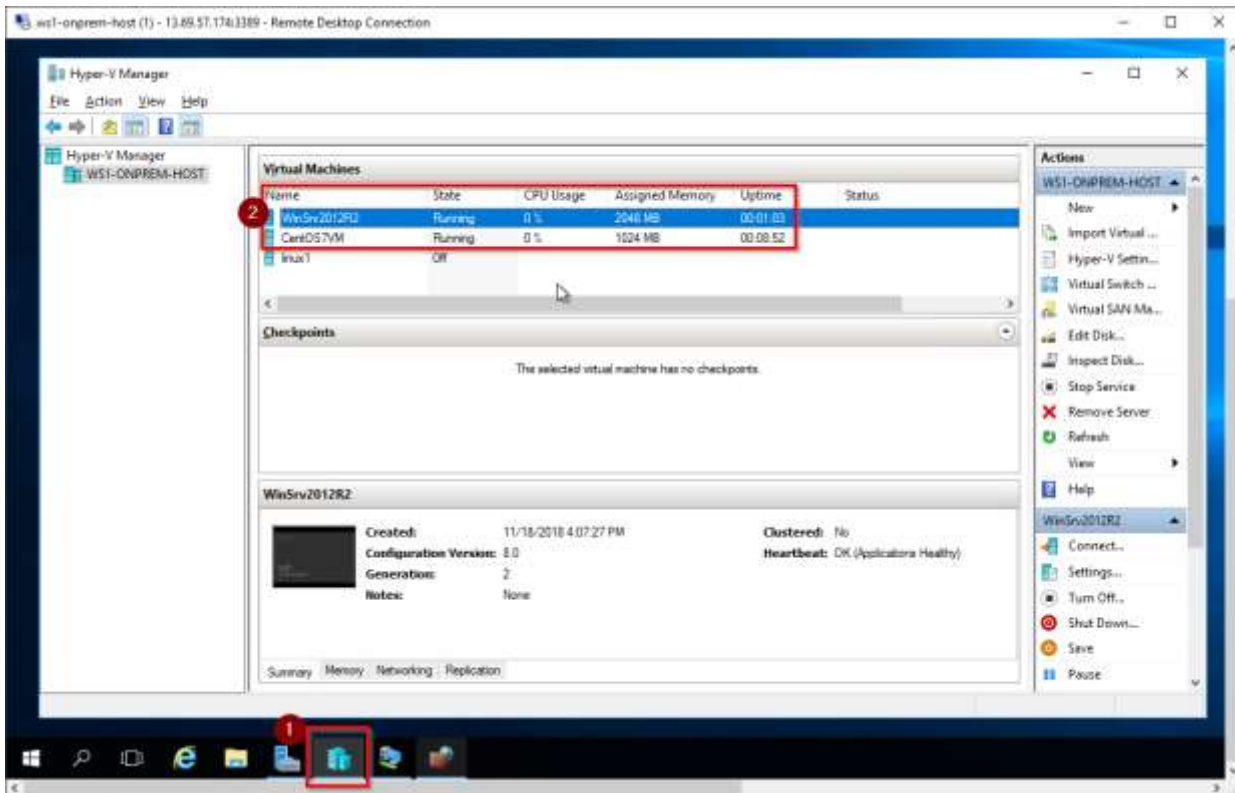
Username:	Administrator
Password:	Vuhu3395

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):

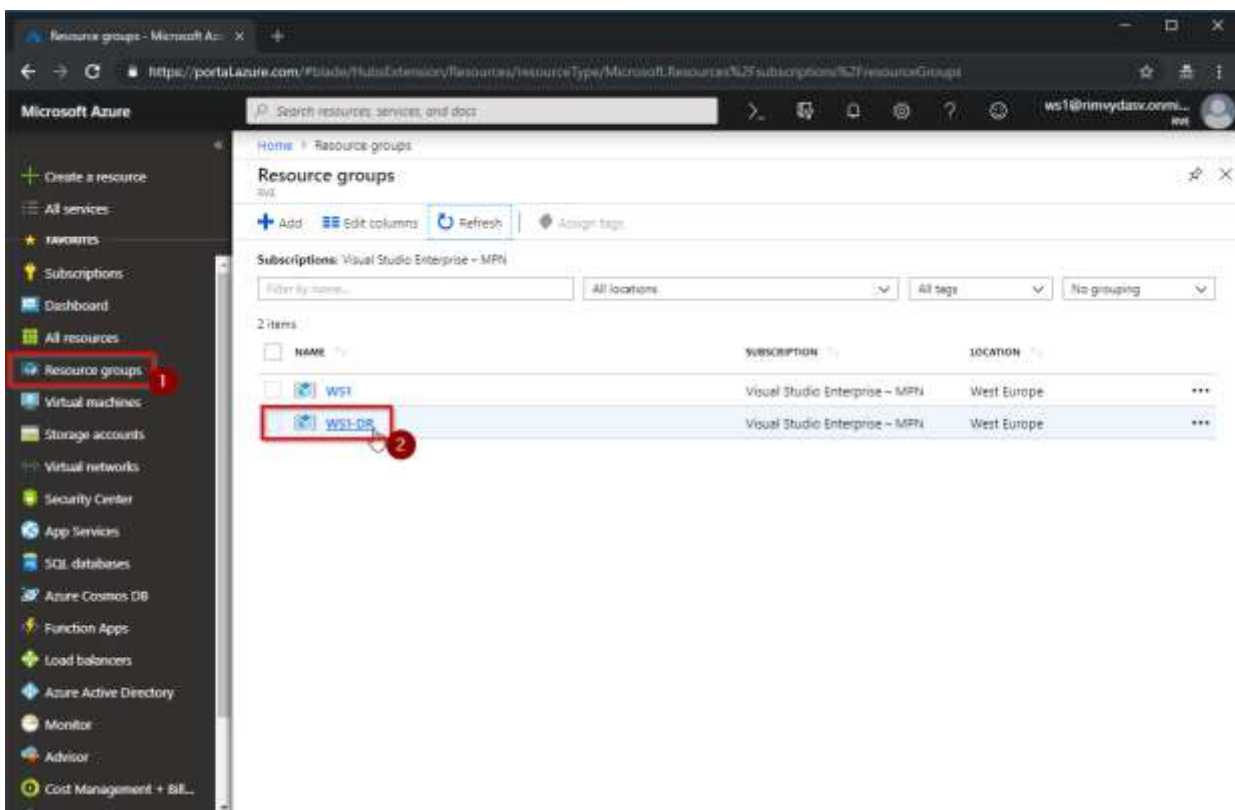
Root username:	ws
Password:	Vuhu3395

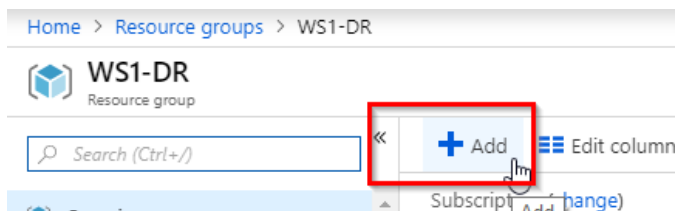
Pabandykite prisijungti prie abiejų VM Hyper-V konsolėje, įsitikinkite, kad jos veikia.



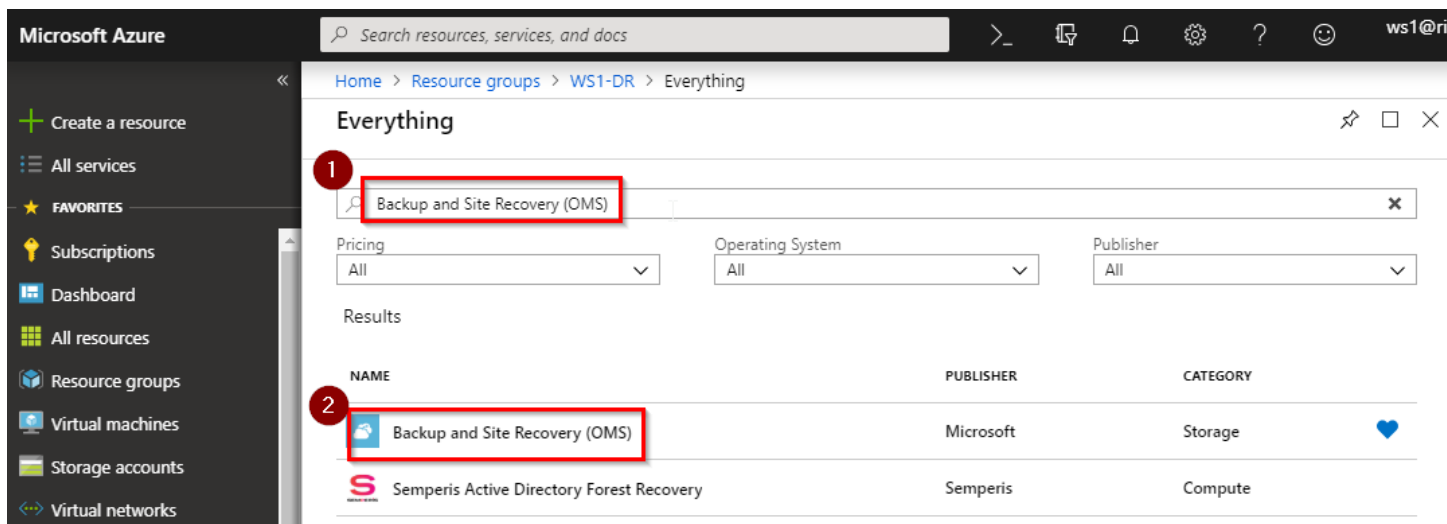
3. DR Vault sukūrimas:

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

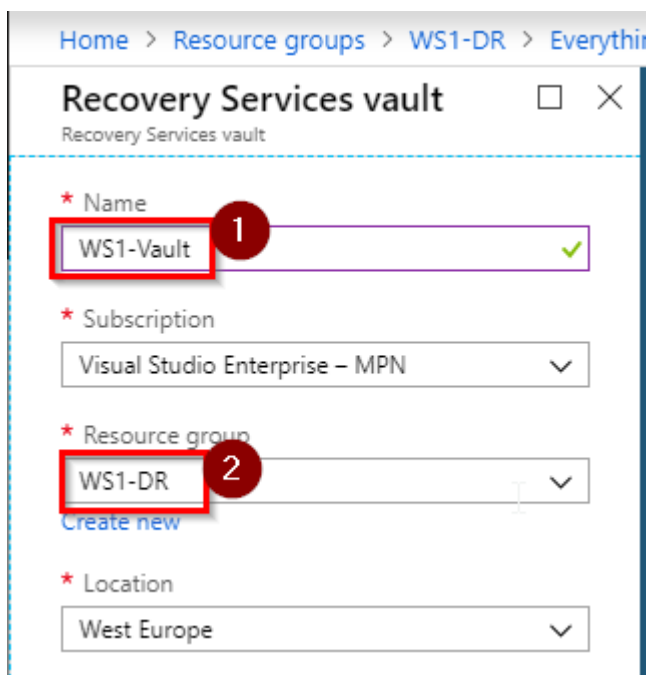




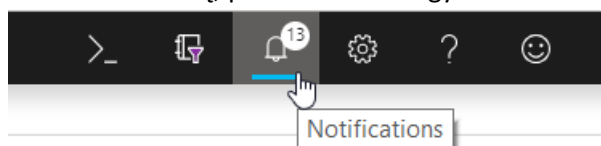
3.2. Azure Marketplace suraskite ir pasirinkite „Backup and Site Recovery (OMS):



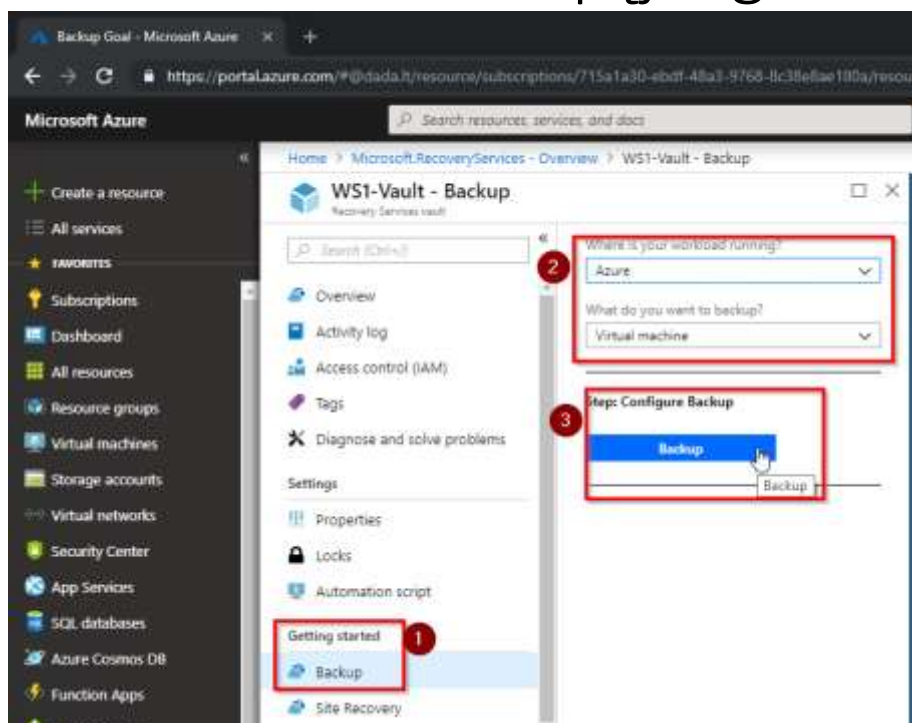
3.3. Pavadinkite „WSX-Vault“ (kur X jums suteiktas skaičius). Būtinai pasirinkite „WSX-DR“ resursų grupę. Spauskite „Create“.



3.4. Stebėkite statusą, palaukite kol saugykla bus sukurta.

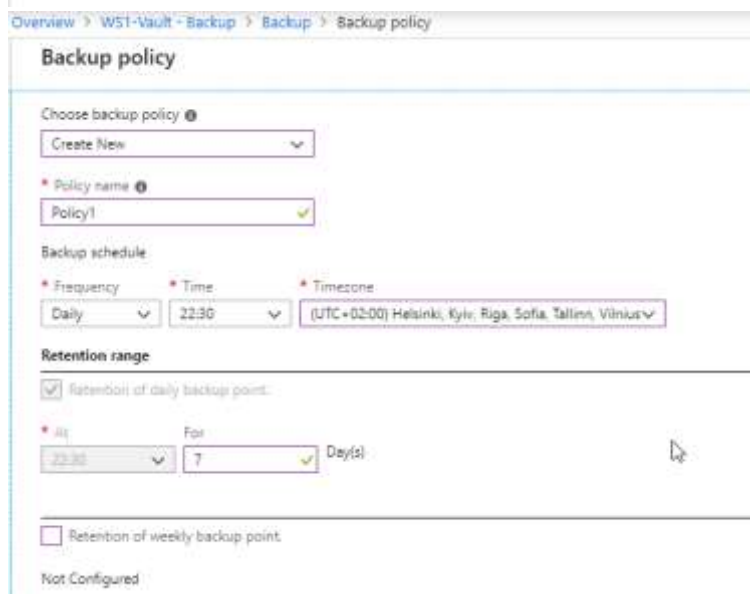


4. Azure VM backup įjungimas ir konfigūravimas

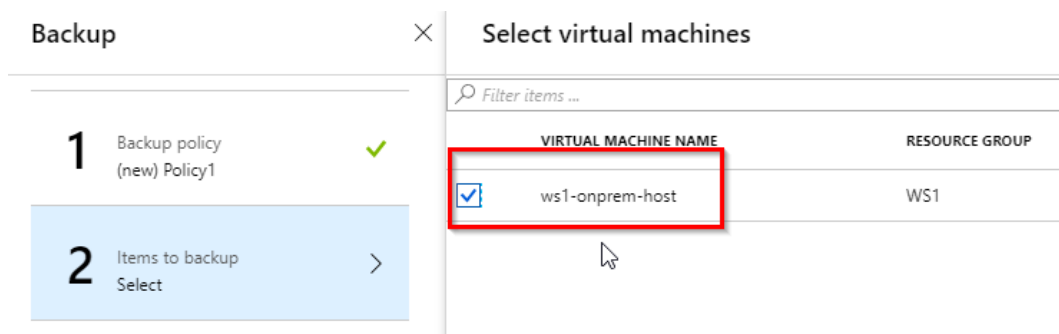


4.1. Sukurto Recovery Services Vault pasirinkite Backup skiltį. Nurodykite, kad jūsų virtuali mašiną kurią norite apsaugoti yra laikoma Azure.

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

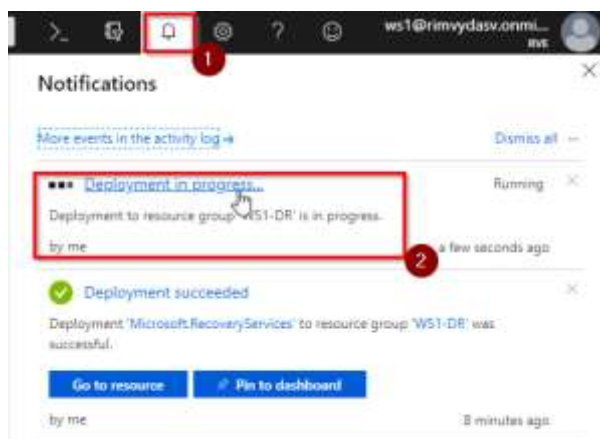


4.2. Pasirinkite kurią VM apsaugosite:

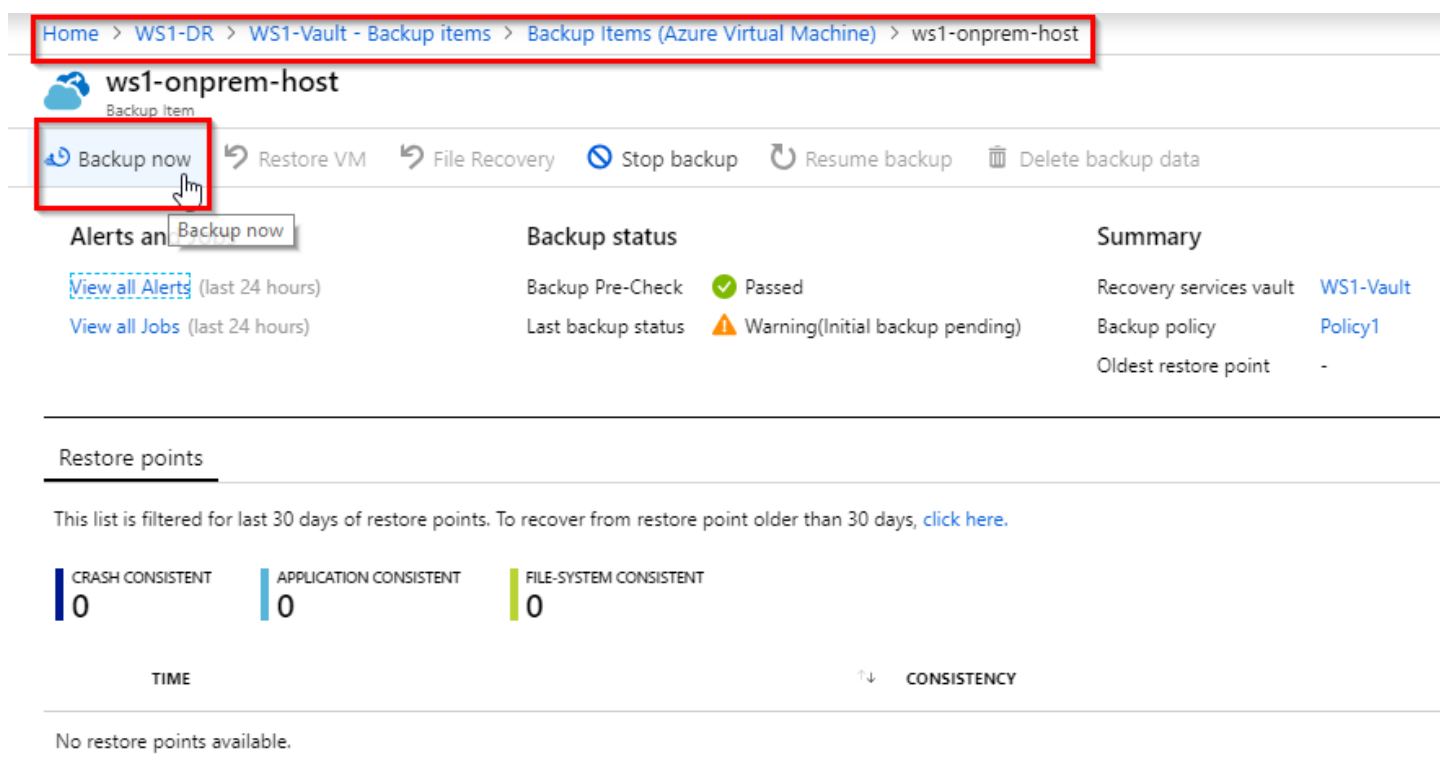


VIRTUAL MACHINE NAME	RESOURCE GROUP
<input checked="" type="checkbox"/> ws1-onprem-host	WS1

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



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 notifications
[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](#).

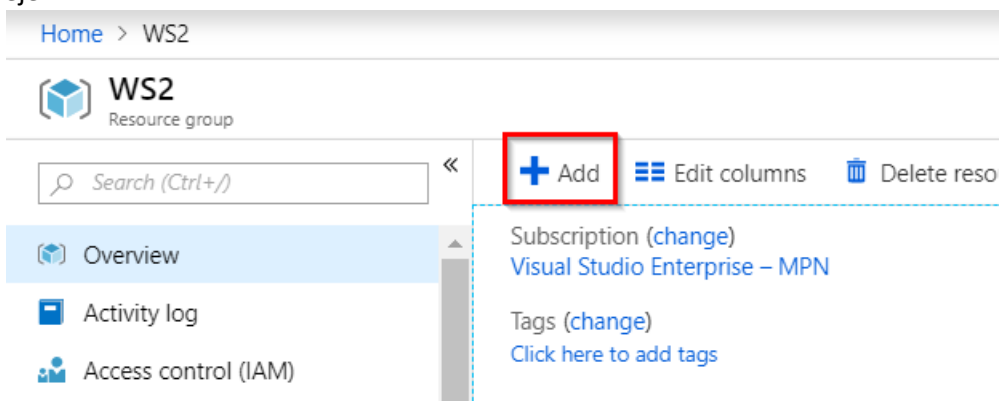
CRASH CONSISTENT	APPLICATION CONSISTENT	FILE-SYSTEM CONSISTENT
0	0	0

TIME CONSISTENCY

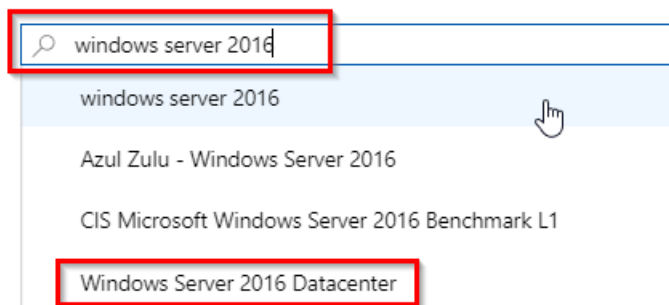
No restore points available.

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:

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

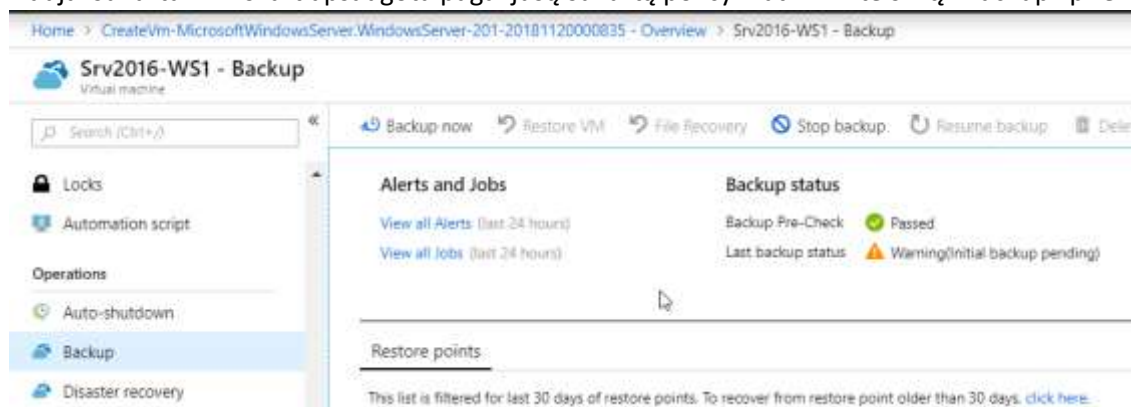
WS1-Vault ▼

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

5.6.

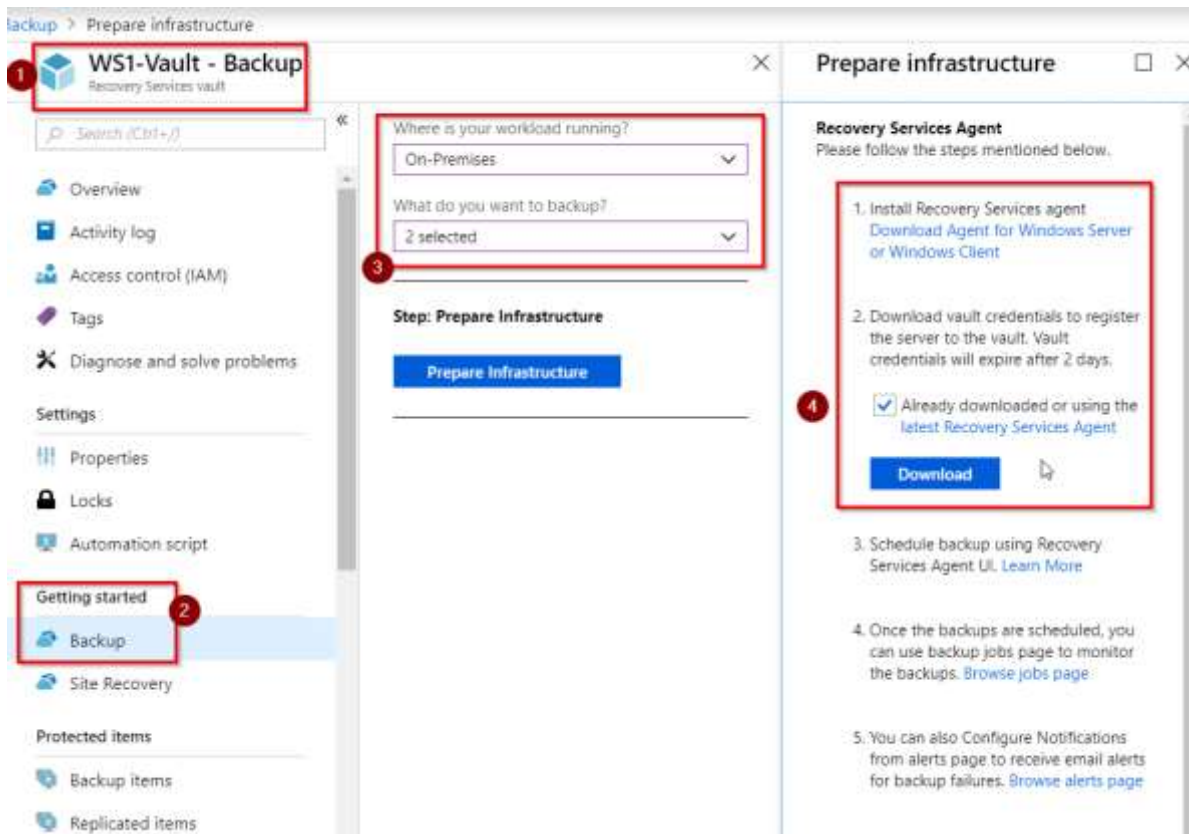
5.7. Nueikite iki "Review+create", sukurkite VM.

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

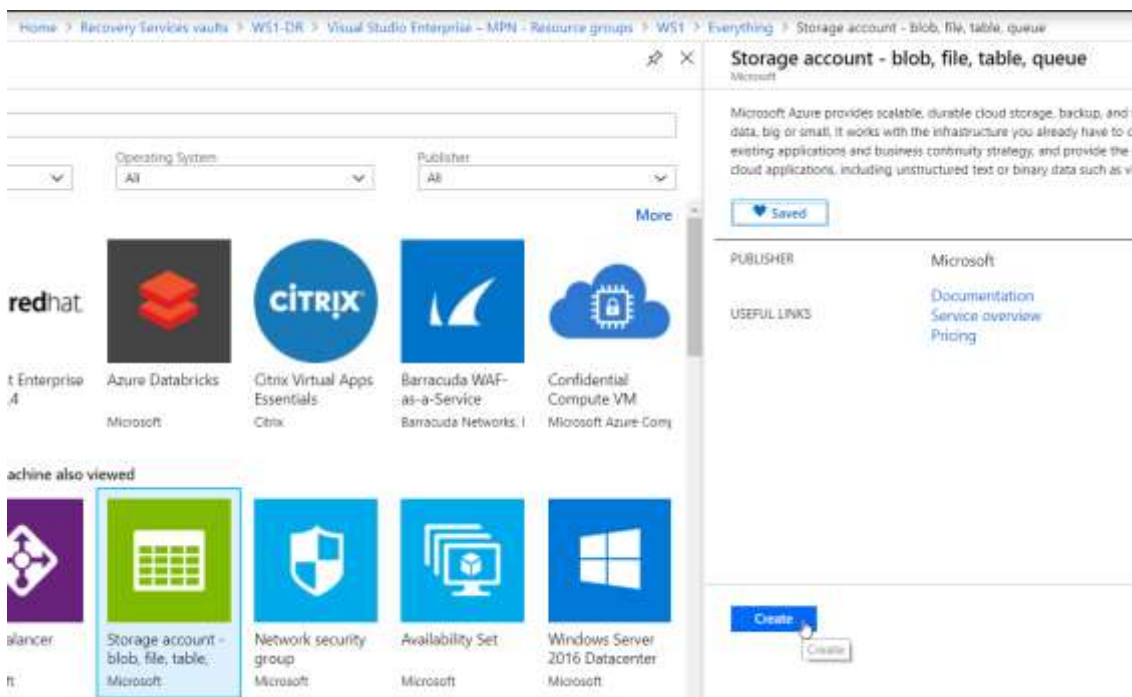


6. Onprem VM backup konfigūravimas

- 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”. Atsiųskite agentą ir prisijungimo duomenis (vault credentials):



- 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“.



- 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

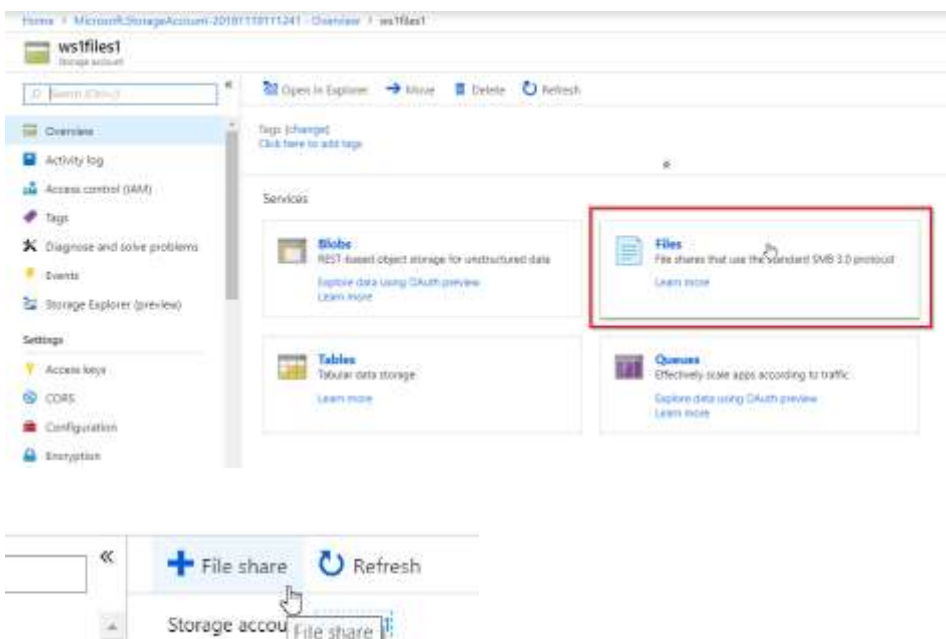
Account kind

Replication

Access tier (default) ☐ Cool ☒ Hot

[Review + create](#) [Previous](#) [Next : Advanced >](#)

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



6.5. Suteikite File Share pavadinimą ir nustatykite dydį:

File share ✕

* Name

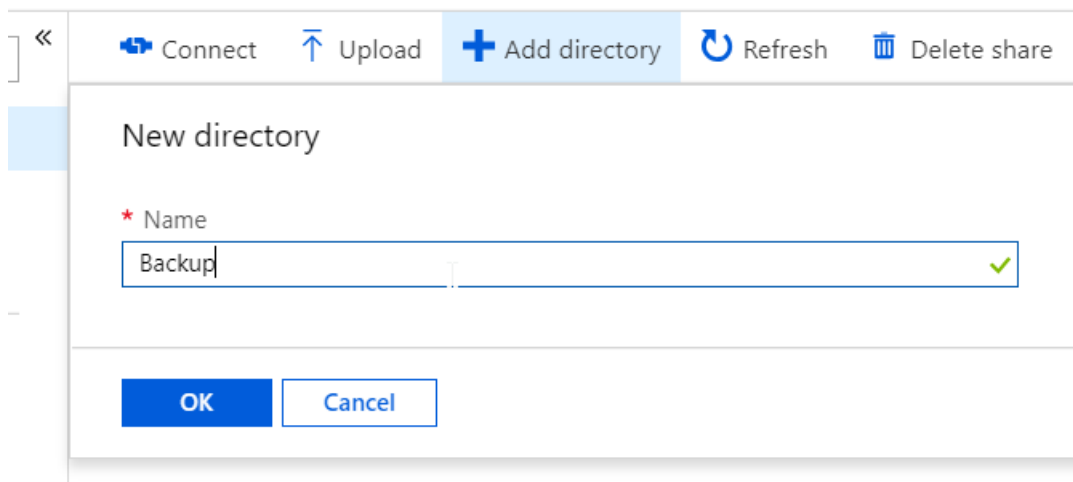
Quota

GB

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

[Create](#)

Sukurkite direktoriją:



« Connect Upload **Add directory** Refresh Delete share

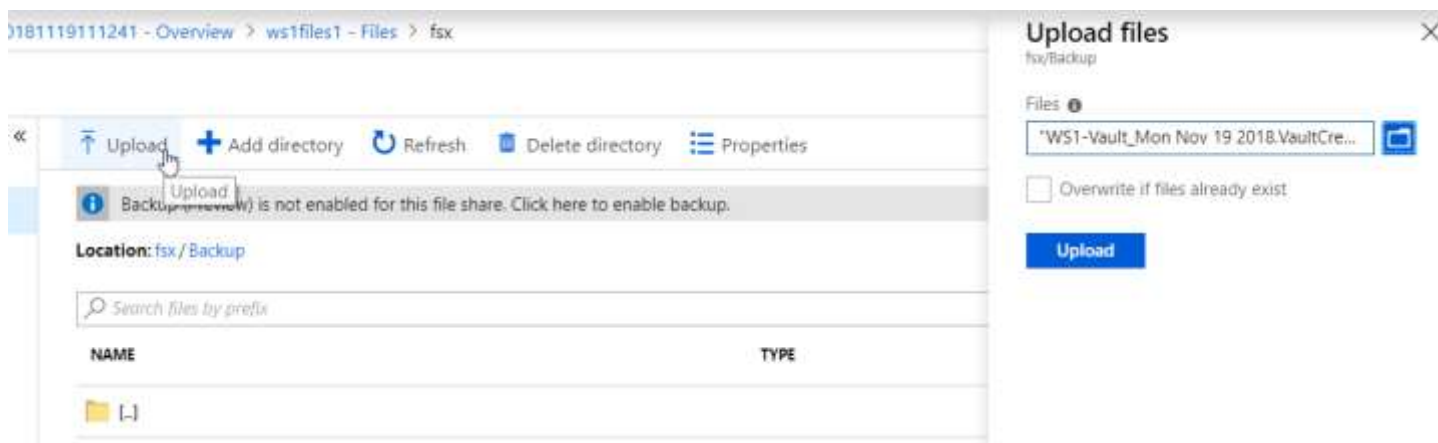
New directory

* Name

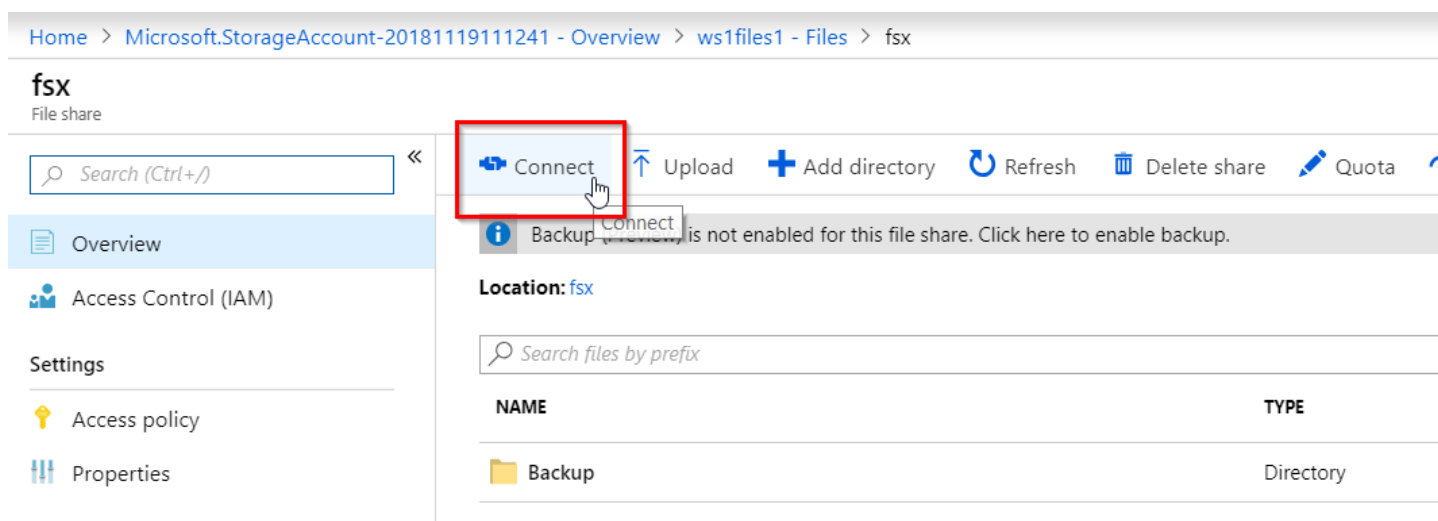
Backup ✓

OK Cancel

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



6.7. Prijunkite File share prie **WinSrv2012R2** virtualios mašinos (**onprem host viduje, PER RDP IP 192.168.0.10**) Norėdami gauti prisijungimo prie File Share komandą ir raktus pasirinkite „Connect“:



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+kWBrPxxL5aBa0eQhaivKnVqymG5wt7YJ4e  
t4ngeb+pQBtiuJCXuhE3sVSODlc3k0xZjJAbsYA==" -  
AsPlainText -Force  
$credential = New-Object
```



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

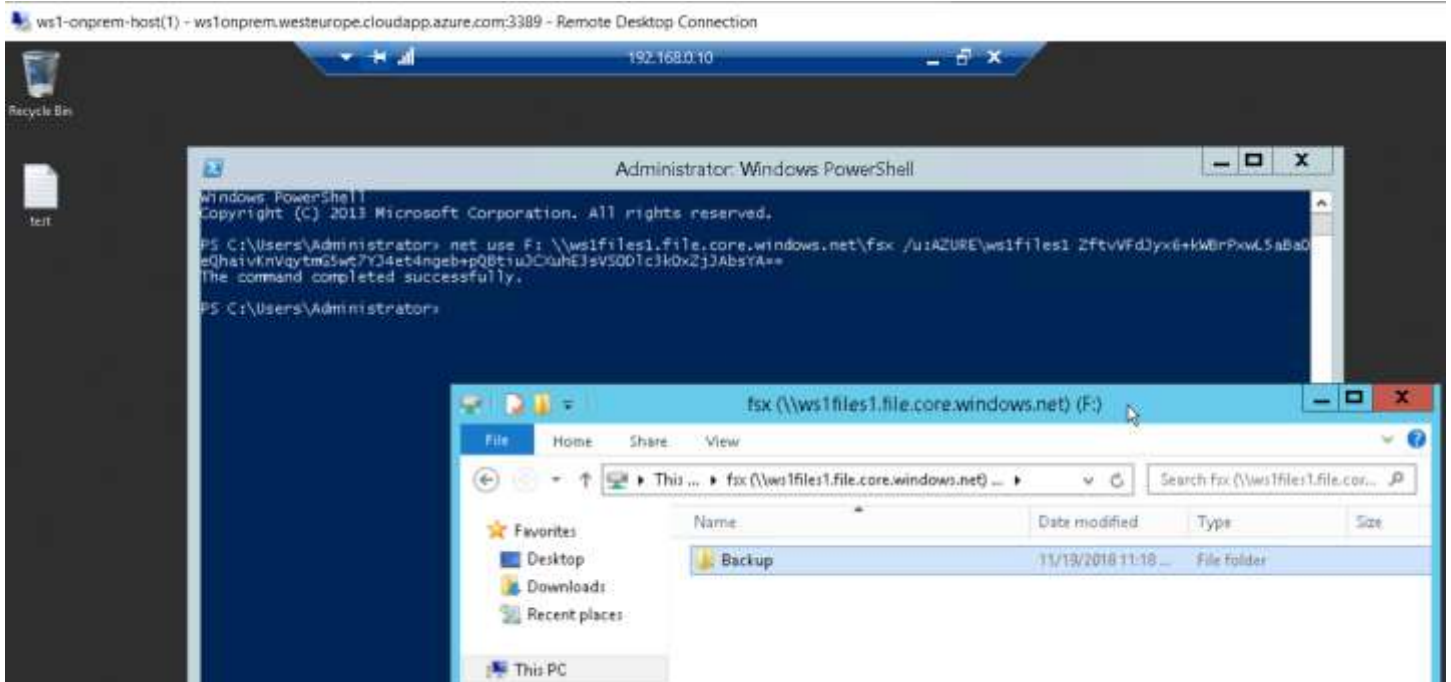
```
net use F: \\ws1files1.file.core.windows.net\fsx  
/u:AZURE\ws1files1  
ZftvVFdJyx6+kWBrPxxL5aBa0eQhaivKnVqymG5wt7YJ4et4n  
geb+pQBtiuJCXuhE3sVSODlc3k0xZjJAbsYA==
```

2



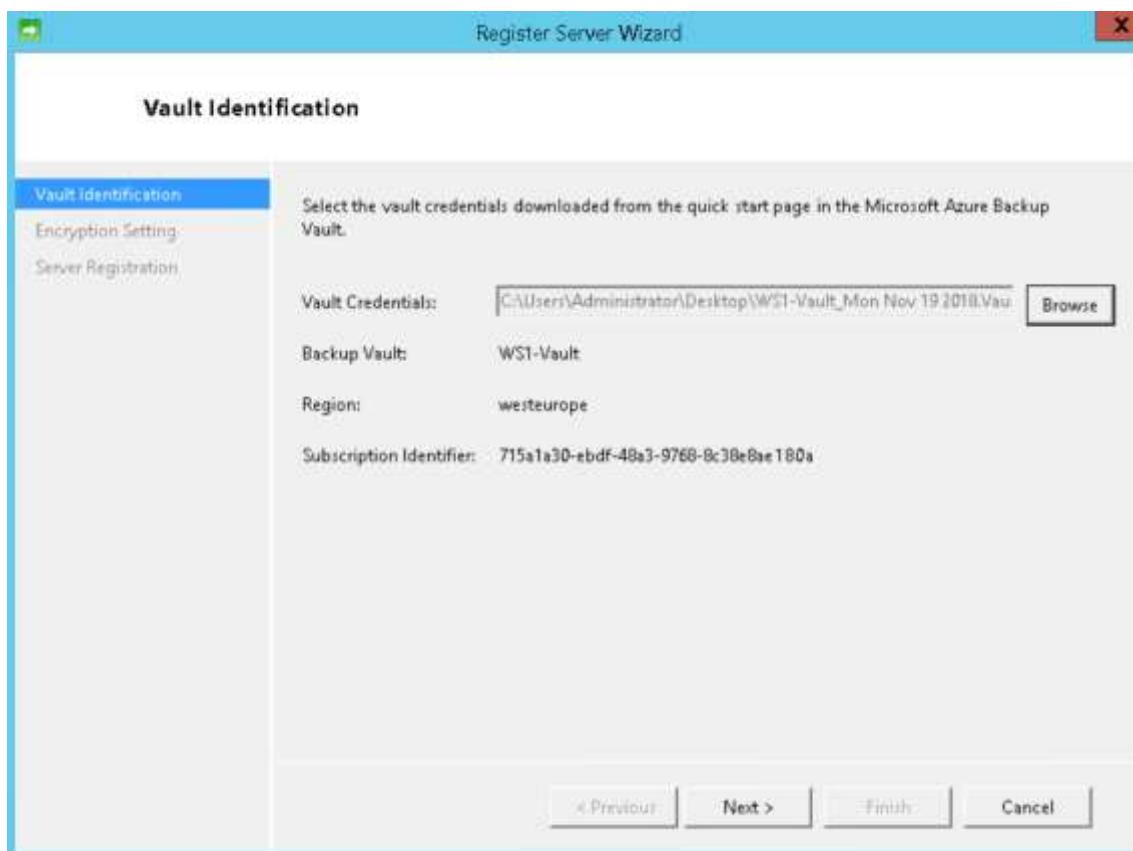
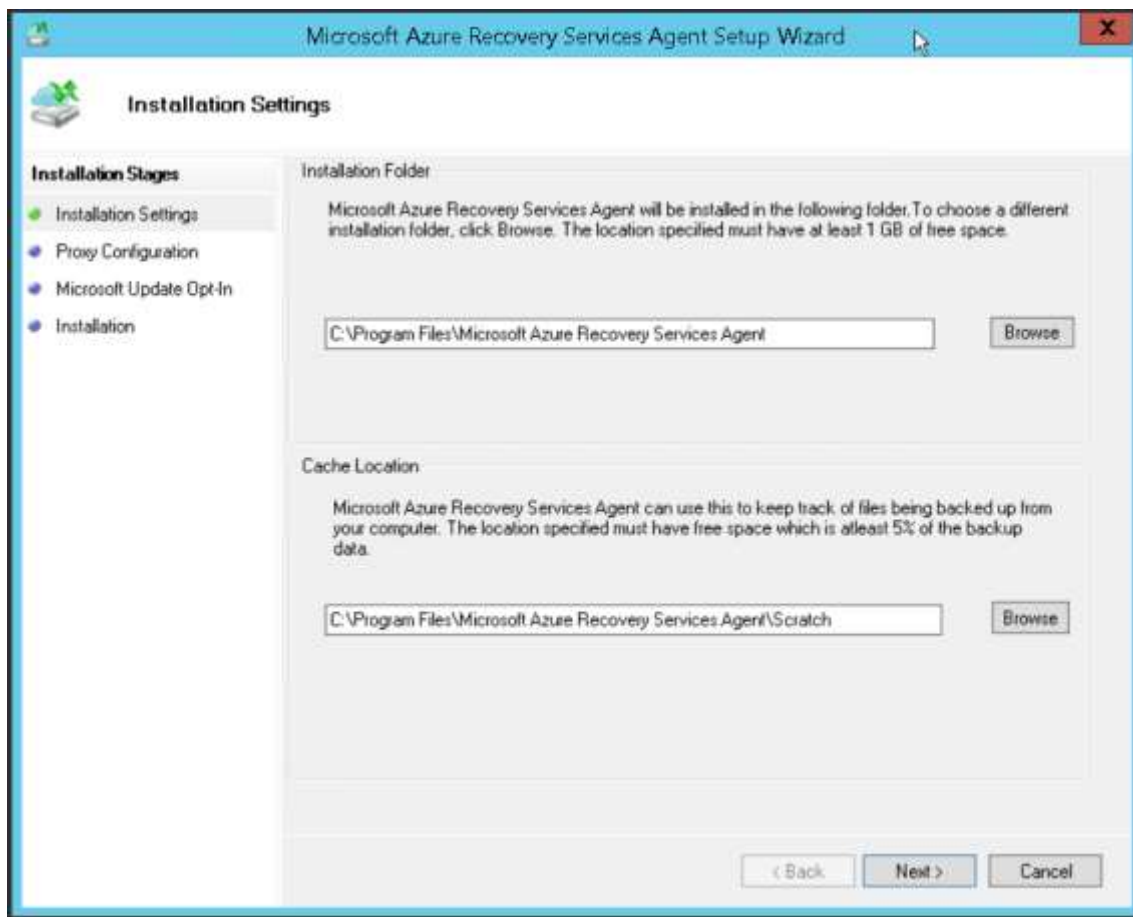
When connecting from a computer from outside Azure, remember to open outbound TCP port 445 in your local network. Some Internet service providers may block port 445. Check with your service provider for details.

- 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.



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

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

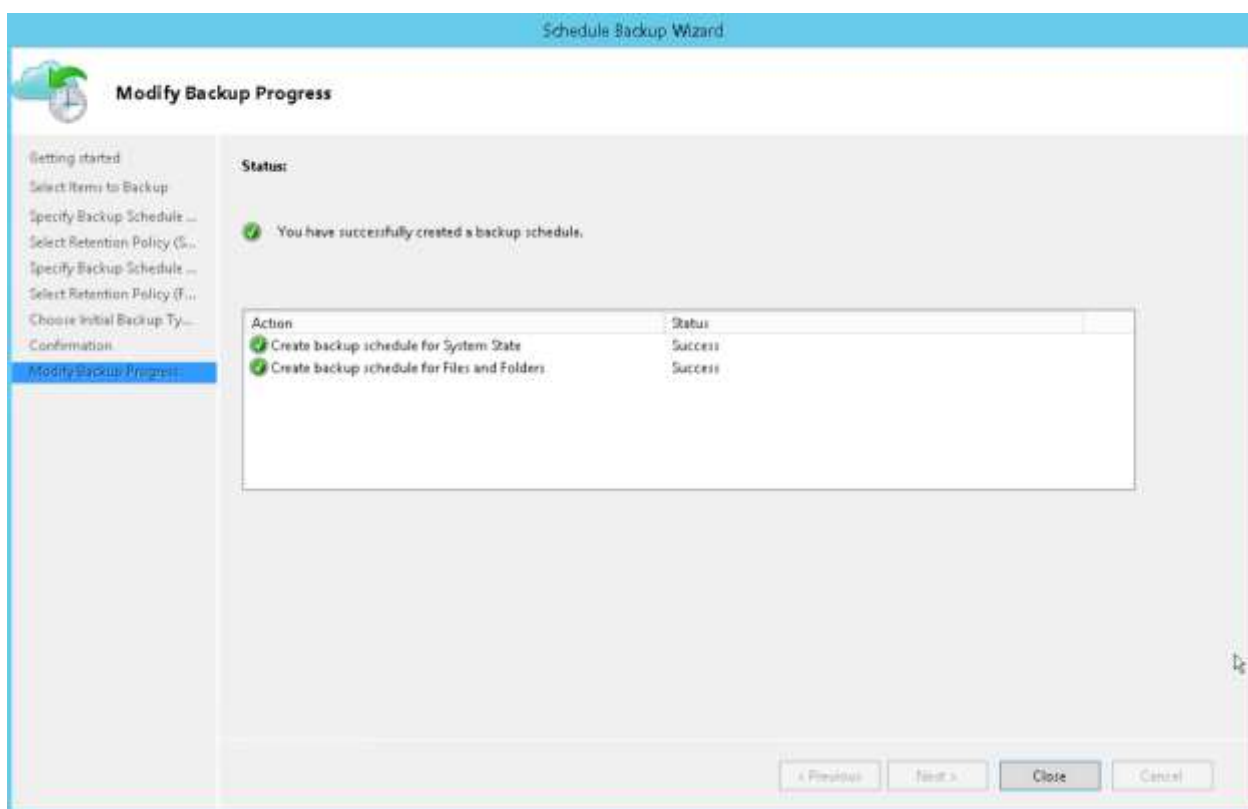
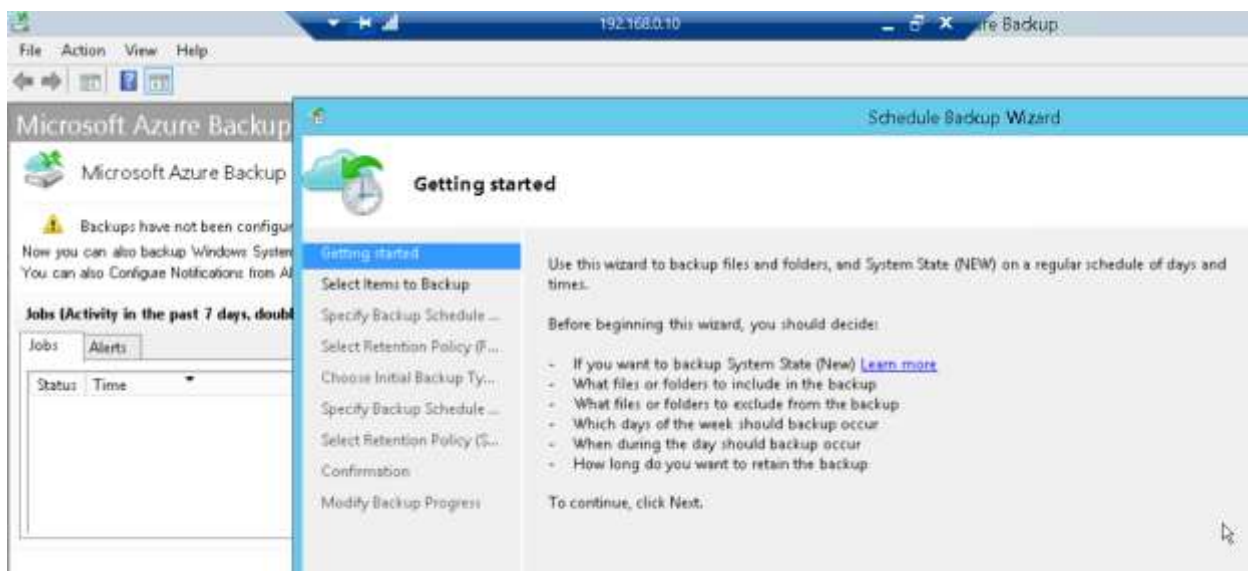


Generuojamas ir išsaugomas užšifravimo raktas (reikalingas atstatymui):

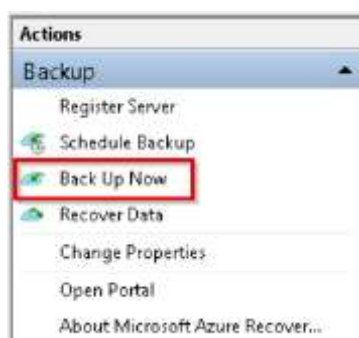
The screenshot shows the 'Register Server Wizard' window with the 'Encryption Setting' step selected in the left sidebar. The main area contains instructions: 'Backups are encrypted to protect the confidentiality of your data. Generate or type a passphrase to encrypt and decrypt backups from this server.' It includes two text boxes for 'Enter Passphrase (minimum of 16 characters)' and 'Confirm Passphrase', both showing masked characters and a '(36)' character count. A 'Generate Passphrase' button is to the right. Below is a text box for 'Enter a location to save the passphrase' with 'F:\' entered and a 'Browse' button. A warning icon and text state: '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.' At the bottom are buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

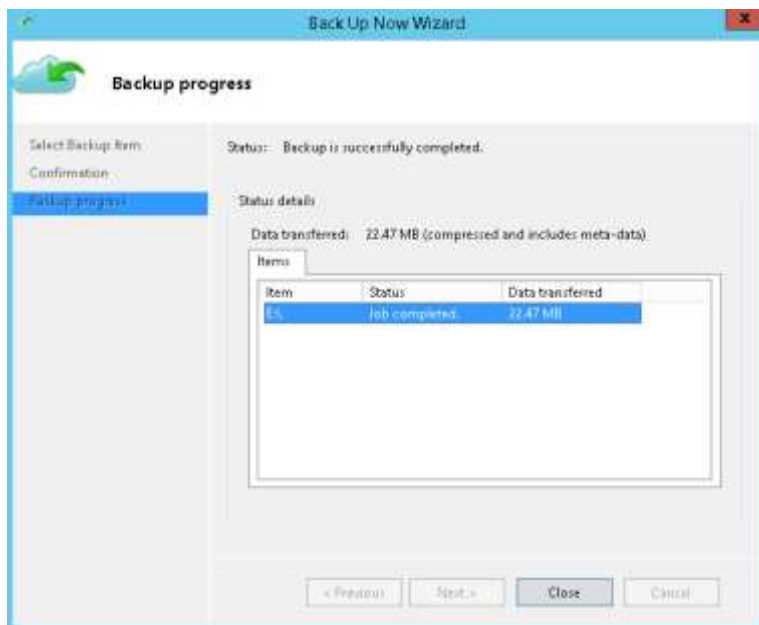
The screenshot shows the 'Register Server Wizard' window with the 'Server Registration' step selected in the left sidebar. The main area displays a green checkmark icon and the text: 'Microsoft Azure Backup is now available for this server.' It follows with 'The passphrase was saved to the following file : [F:\Microsoft Azure Recovery Services Agent.11.19.2018.11.32.47.txt](\"#\")'. Below this, it says 'Before your server is backed up you must configure and schedule backup options.' and has a checked checkbox for 'Launch Microsoft Azure Recovery Services Agent'. At the bottom are buttons: '< Previous', 'Next >', 'Close', and 'Cancel'.

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

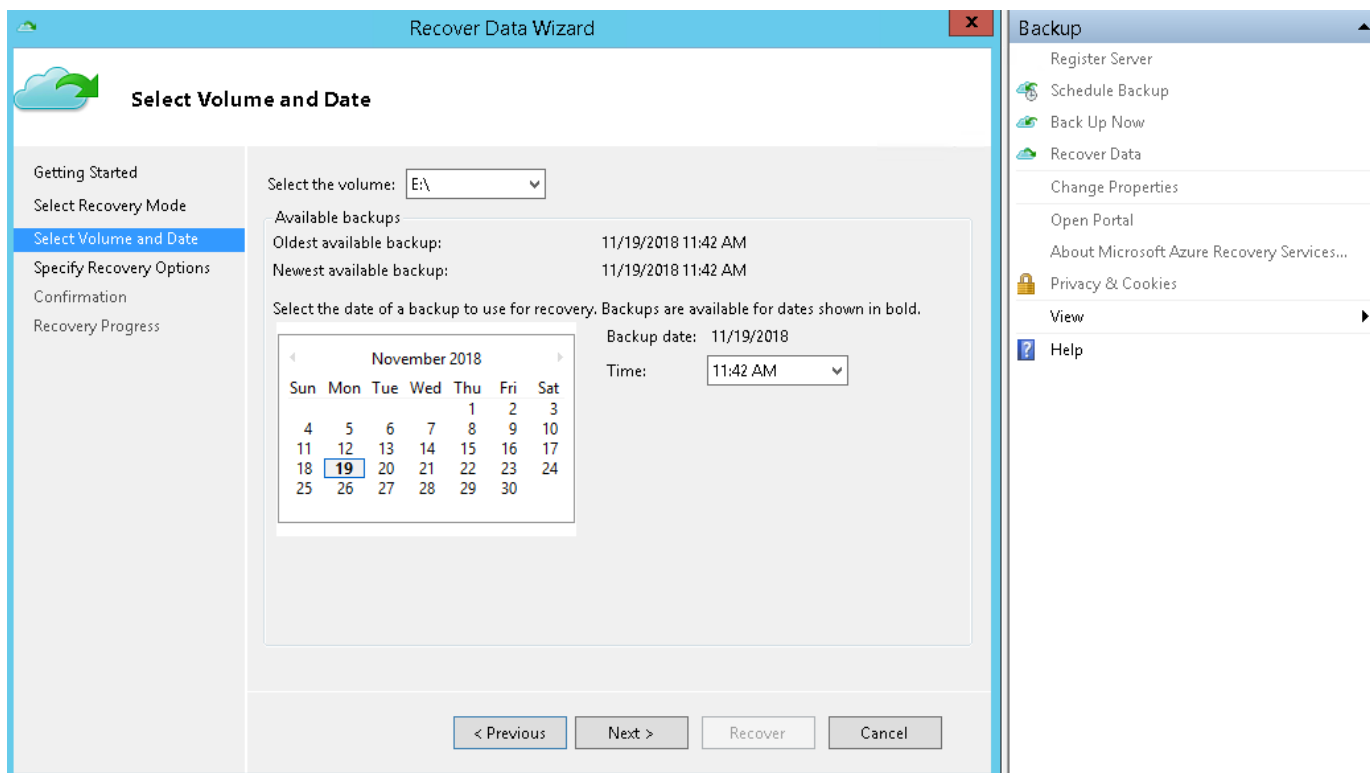


Sukūrę savo Backup politiką pasirinkite „Backup Now“:

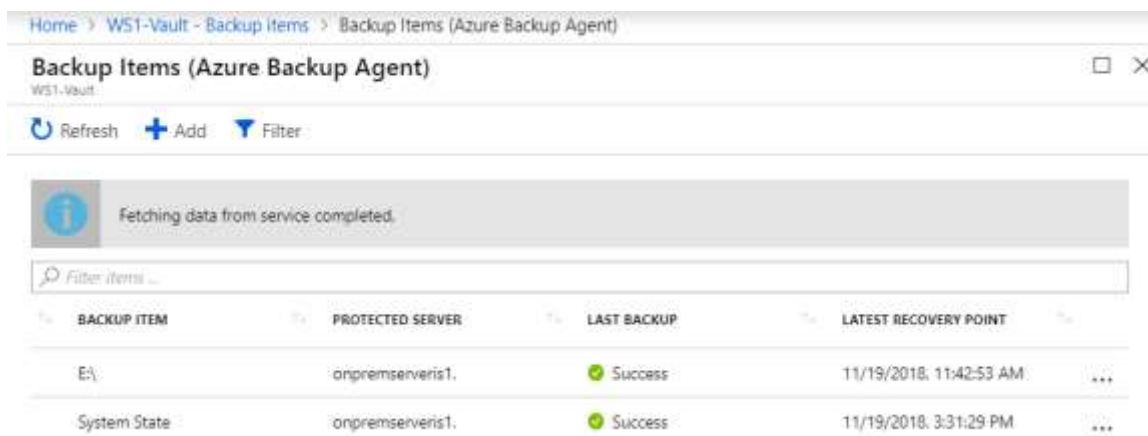




Pabandykite ištrinti ir atstatyti atsitiktinį failą/us. Pasirinkite „Recover Data“, atstatymo tašką. Panagrinėkite kokie yra atstatymo būdai ir kuo jie skiriasi.



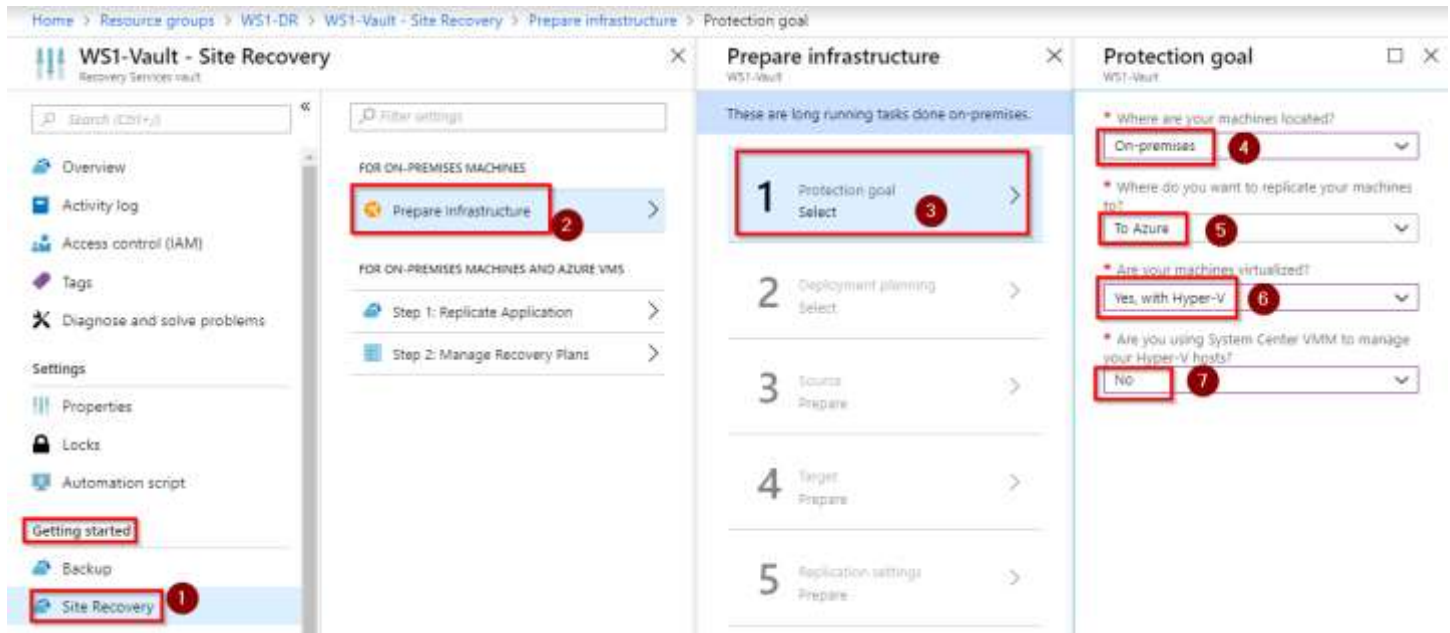
Azure Backup saugomus objektus galite rasti Azure Portal, Recovery Services Vault, Backup Items:



7. Azure Site Recovery infrastruktūros paruošimas.

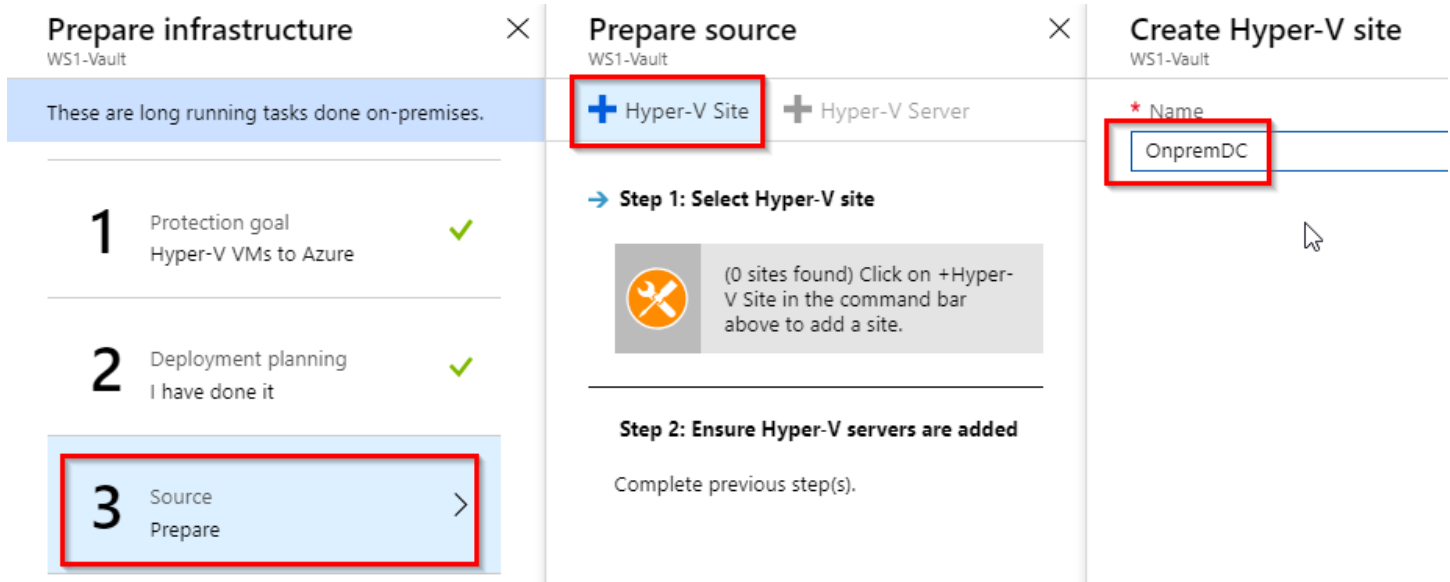
*Deployment planner: <http://aka.ms/asr-deployment-planner> (Jei liks laiko)

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



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

7.3. Sukuriame "Hyper-V Site".



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

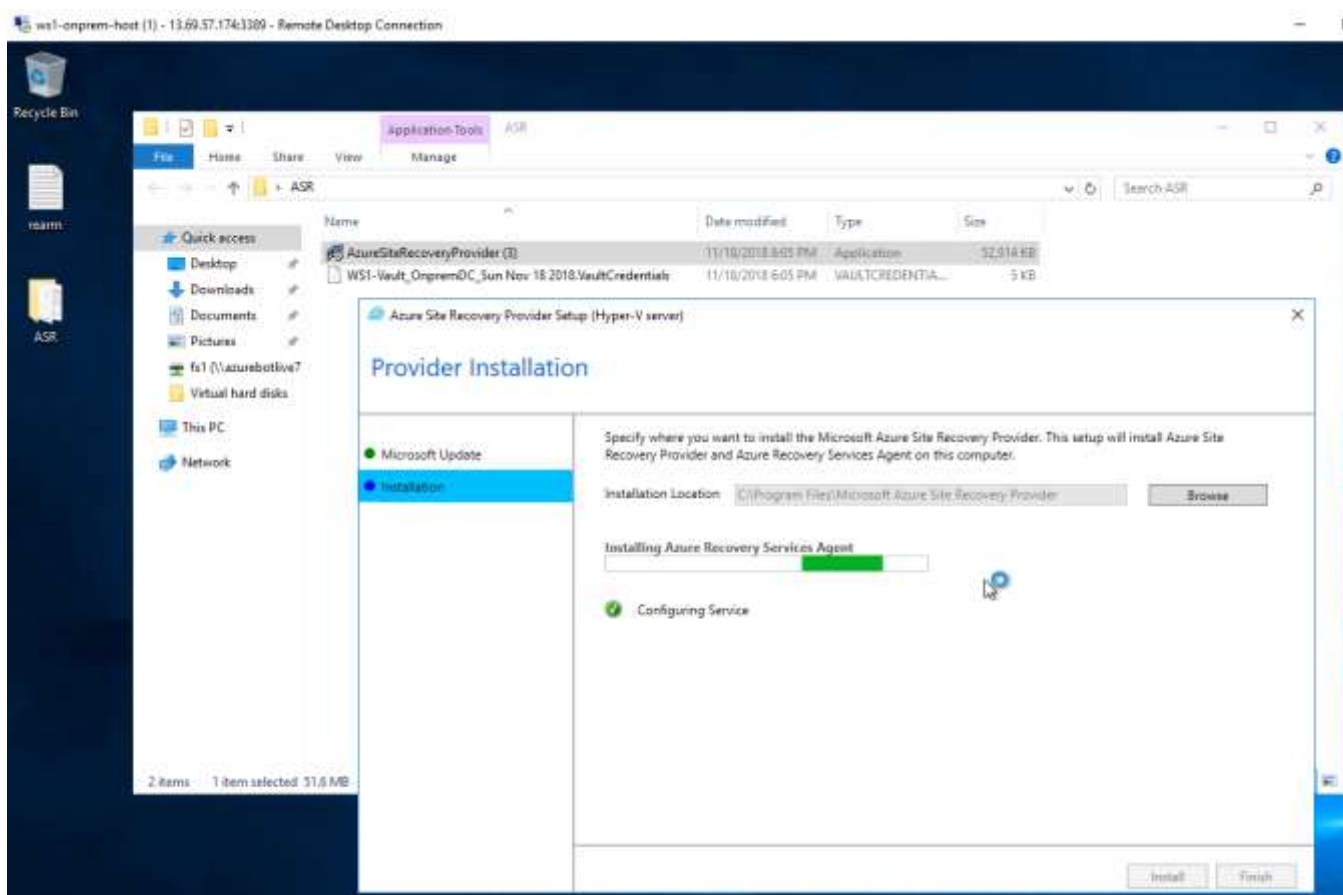
Hyper-V server

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**
- 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:



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:

- Protection goal Hyper-V VMs to Azure
- Deployment planning I have done it
- Source Prepare

Prepare source WS1-Vault

+ Hyper-V Site + Hyper-V Server

✓ Step 1: Select Hyper-V site

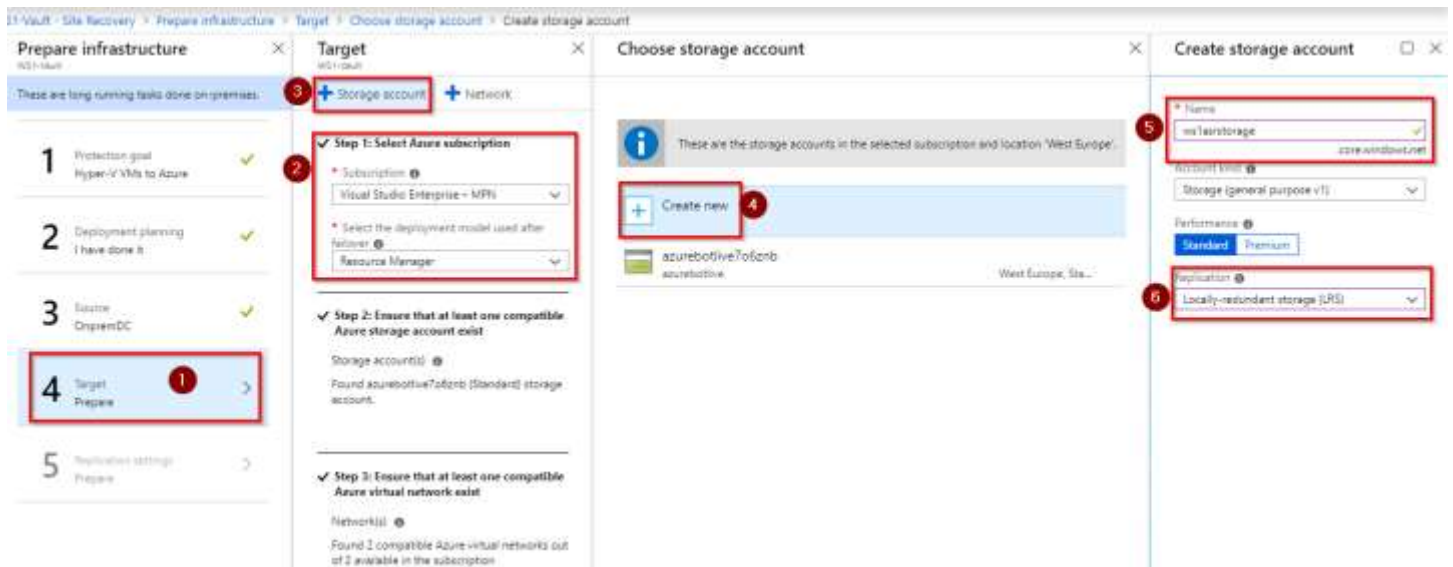
* Hyper-V Site

OnpremDC

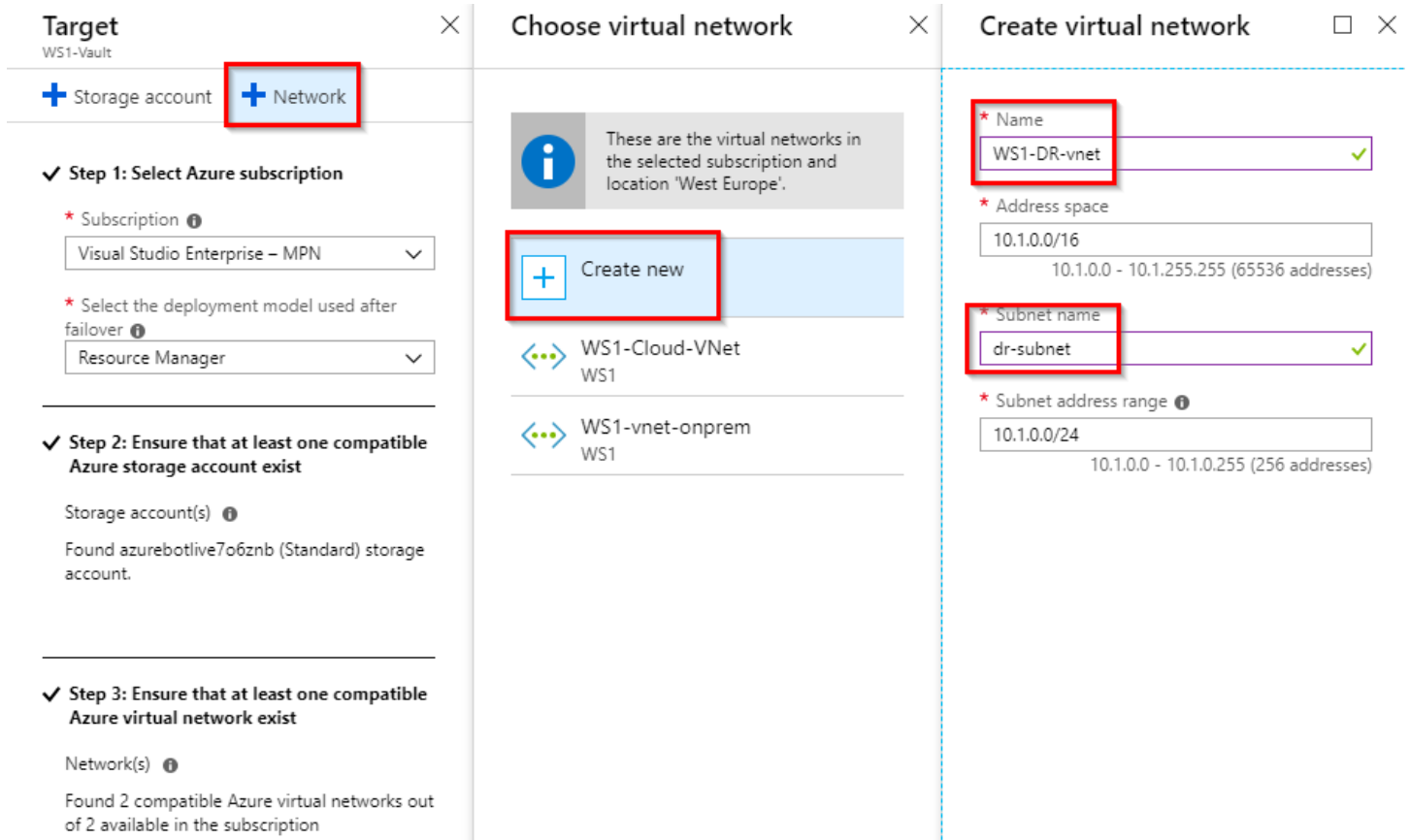
✓ Step 2: Ensure Hyper-V servers are added

ws1-onprem-host

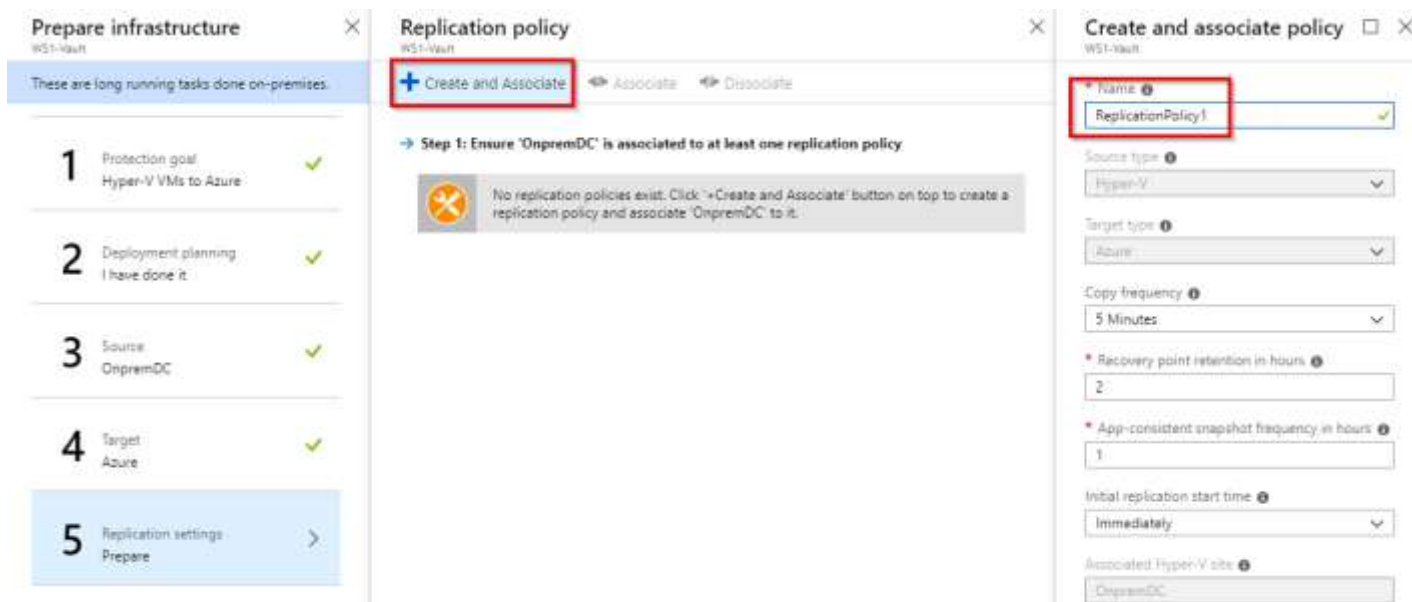
7.9. Ketvirtame paruošimo žingsnyje pridėkite papildomą “Storage account” kur bus saugomi replikuojami VM duomenys. Pavadinkite “wsXasrstorage”, pasirinkite LRS.



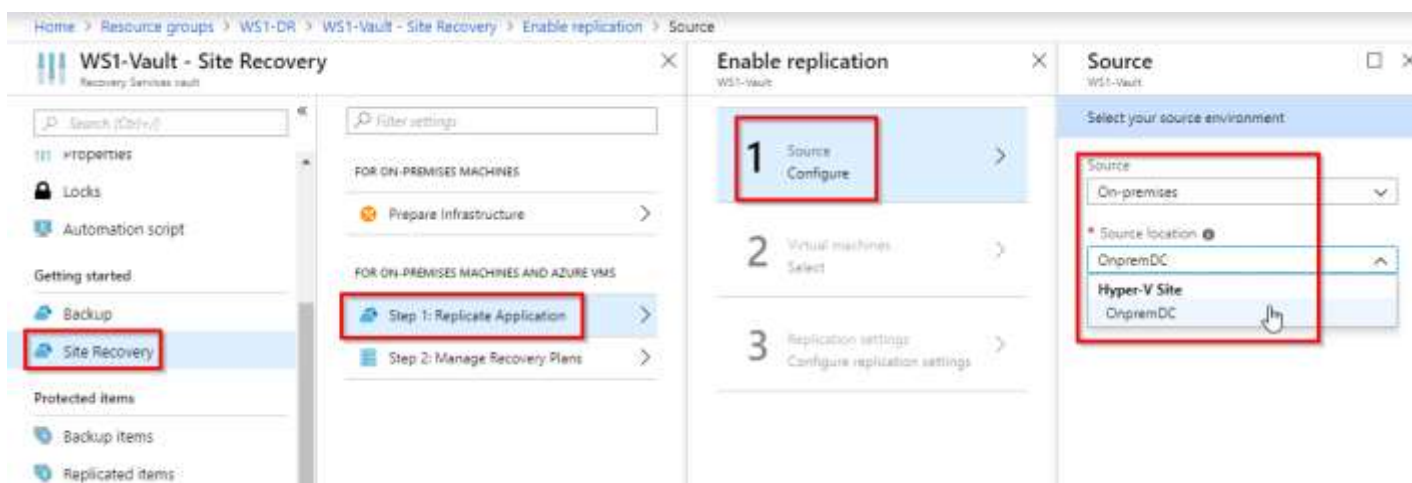
7.10. Pridėkite Azure virtualų tinklą, kurį naudos atstatomos VM. Pavadinkite “wsX-DR-vnet”. Address space ir subnet neturėtų kirstis su “onprem” tinklo režiais.



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



7.12. Jjunkite 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

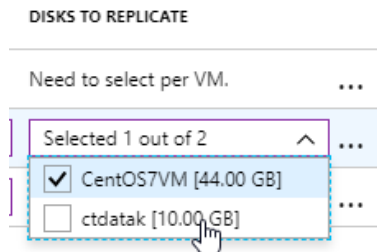
7.15. Nurodykite VM OS tipą, OS diską:

Recovery > Enable replication > Configure properties

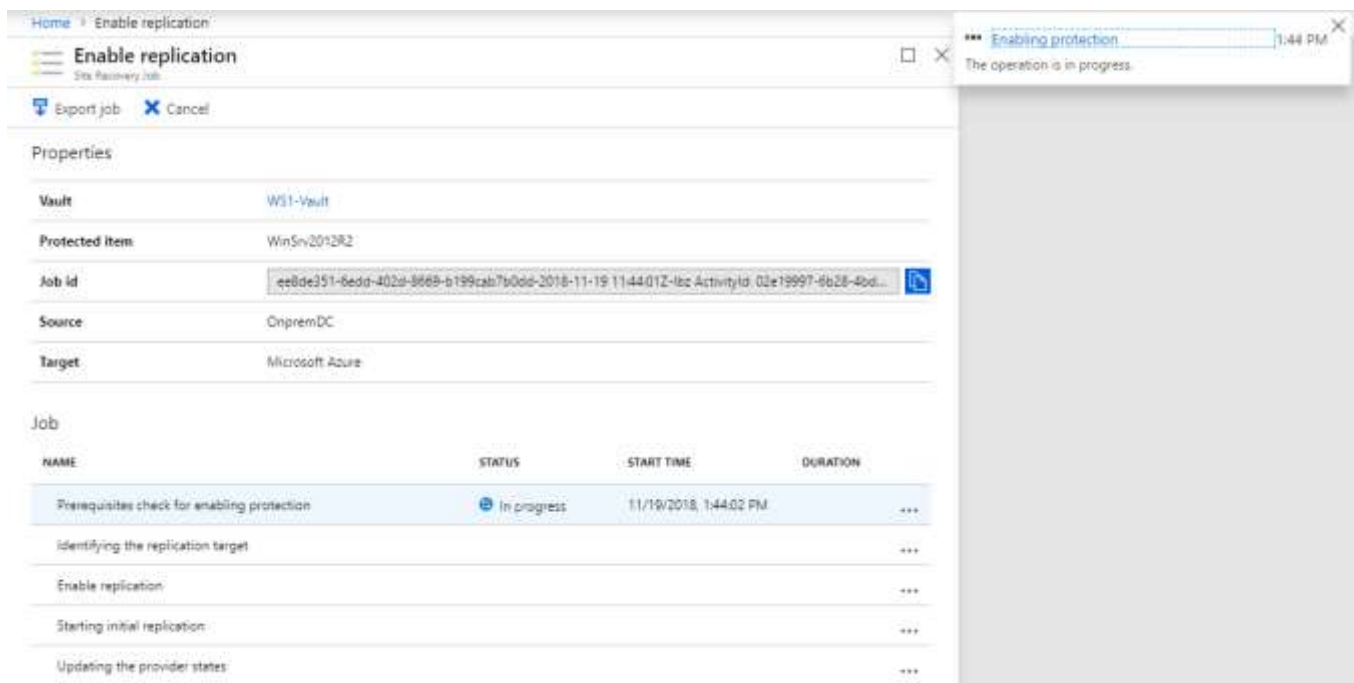
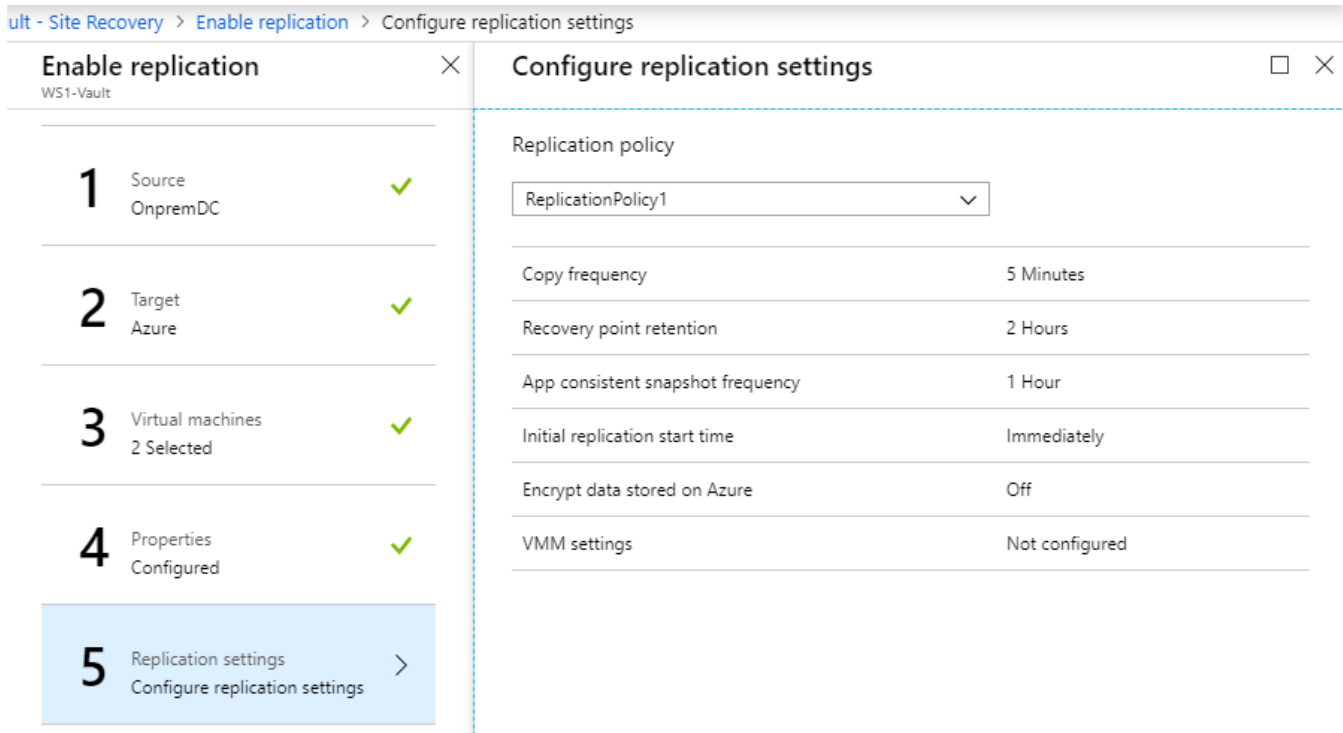
Configure properties

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+F)

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 HEALTH	STATUS	ACTIVE LOCATION	REPLICATION POLICY	RPO	OPERATING SYSTEM	DAILY DATA CH...	IP ADDRESS
WinSrv2012R2	Healthy	0% synchron...	OnpremDC	ReplicationPo...	-	Windows	-	...
CentOS7VM	Healthy	0% synchron...	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 HEALTH	STATUS	ACTIVE LOCATION	REPLICATION POLICY	RPO	OPERATING SYSTEM
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 item

Search (Ctrl+F)

Overview

General

Properties

Compute and Network

Disks

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 set in the resource group
Use managed disks	-	No

Network properties

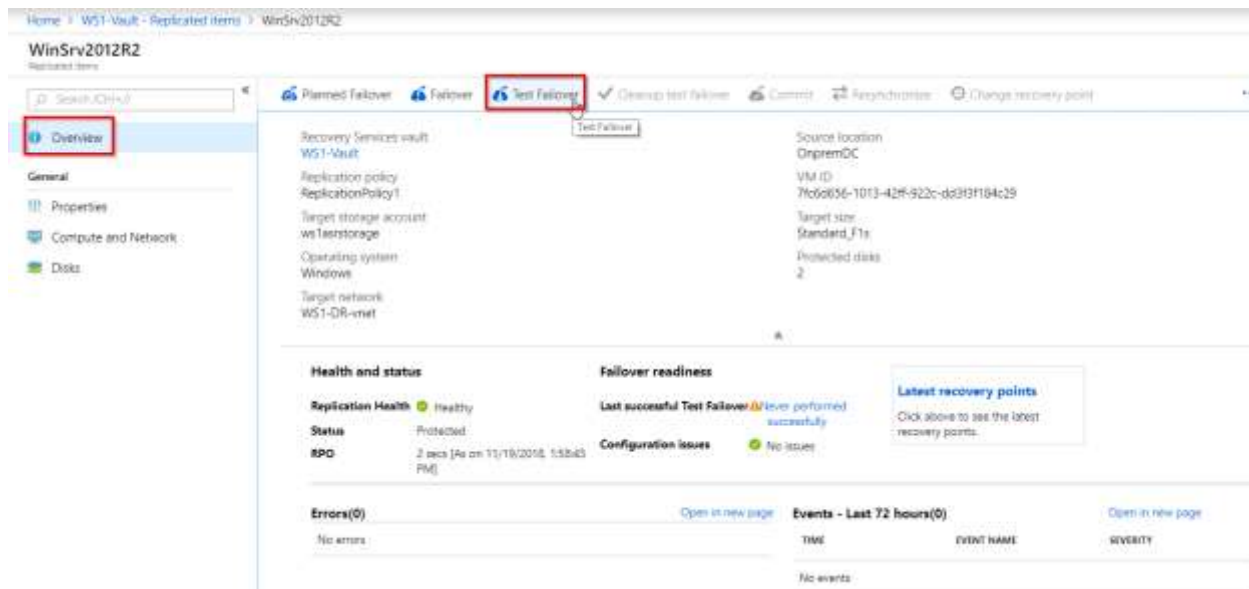
PROPERTIES	TARGET NETWORK
Virtual network	WS1-DR-vnet

Network interfaces

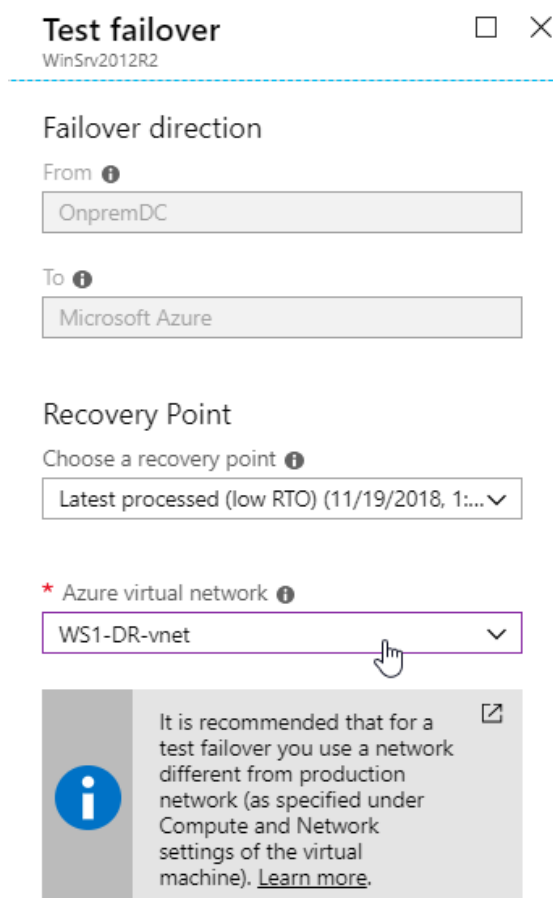
ON-PREMISES NETWORK NAME	TARGET SUBNET	TARGET IP	TARGET NETWORK INTERFACE TYPE
InternalNATSwitch	dr-subnet	DHCP assigned	Primary

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

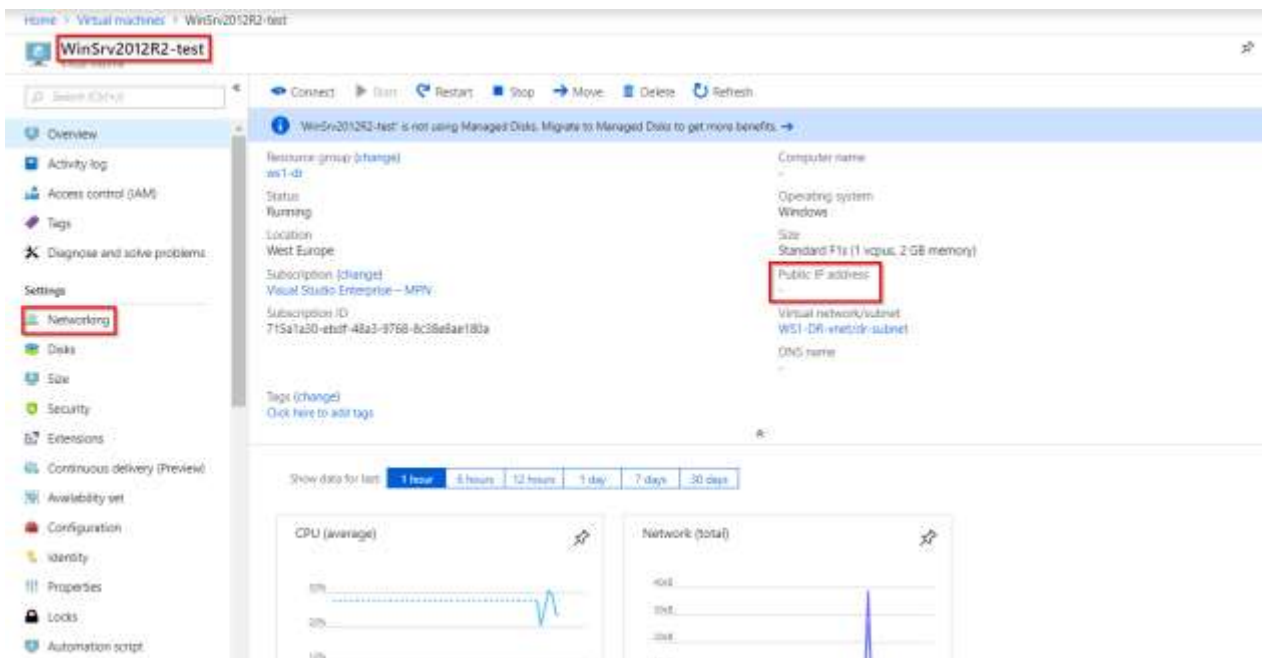
8.1. Vault'e pasirinkite apsaugotą VM, pasirinkite „Test Failover“:



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



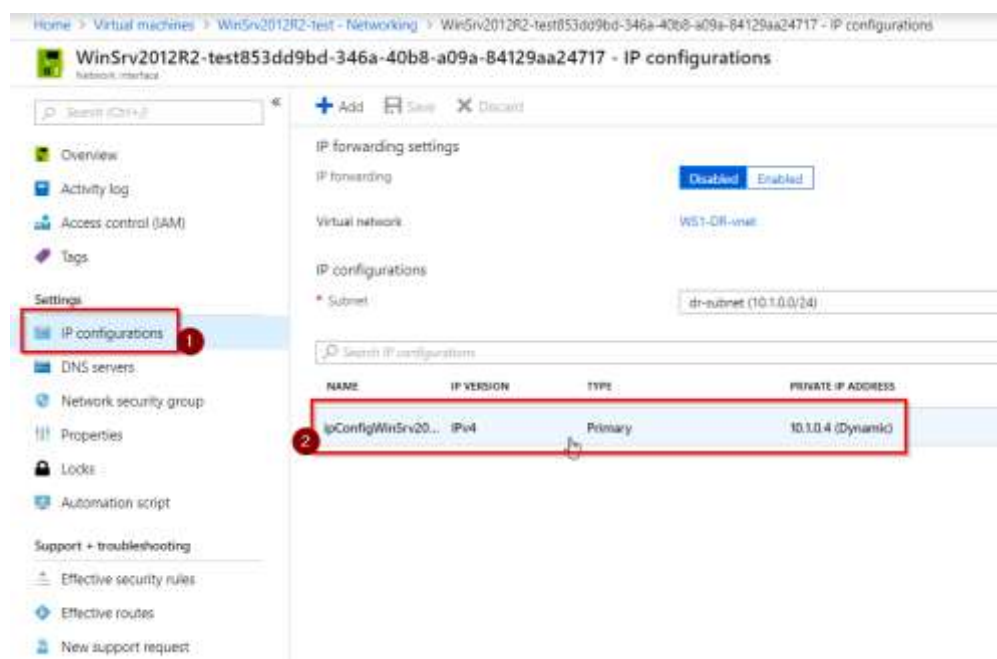
8.3. Po kurio laiko turime testinės mašinos kopiją debesyje. Suraskite mašiną prie visų Azure virtulių mašinų kairiajame portalo meniu „Virtual Machines“. Norėdami prisijungti šiai VM priskirkite Public IP:



8.4. Pasirinkite tinklo adapterio nustatymus:



8.5. Pasirinkite "IP configurations":



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

- 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.

Open in new page

Events - Last 72 hours(1)

Open in new page

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

for the virtual machine has.

every supported limits:

rt-limits.

bytes/sec) of the virtual machine is

covery supported limits for the

grage type.

every supported limits

Table view

Azure

Azure Site Recovery

Test failover cleanup

WinSrv2012R2

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.

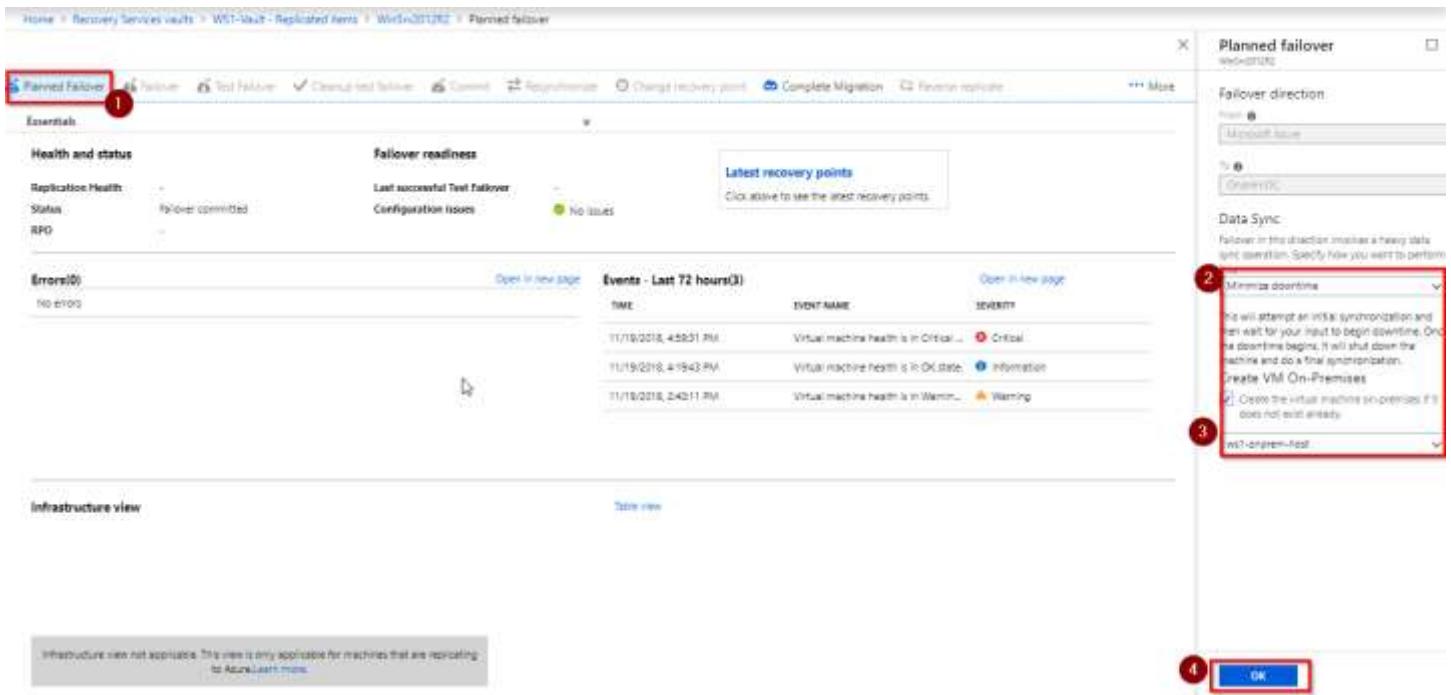
The screenshot shows the Azure Site Recovery console for a Windows VM. The 'Planned Failover' tab is selected, and the 'Failover' button is highlighted with a red box. The 'Essentials' section shows 'Health and status' as 'Healthy' and 'Protected'. The 'Failover readiness' section shows 'Last successful Test Failover' on 11/18/2018. The 'Events' table shows two events: 'Virtual machine health is in OK...' and 'Virtual machine health is in Warning...'. The 'Recovery Point' section on the right shows 'Latest processed (see RPO) (11/19/2018, 4:00 PM)' and a checkbox for 'Shut down virtual machine and synchronize the latest data...' which is checked. The 'OK' button is highlighted with a red box.

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

The screenshot shows the Azure Site Recovery console for a CentOS7 VM. The 'Commit' button is highlighted with a red box. The 'Essentials' section shows 'Health and status' as 'Planned failover finished'. The 'Failover readiness' section shows 'Last successful Test Failover' as 'No issues'. The 'Events' table is empty.

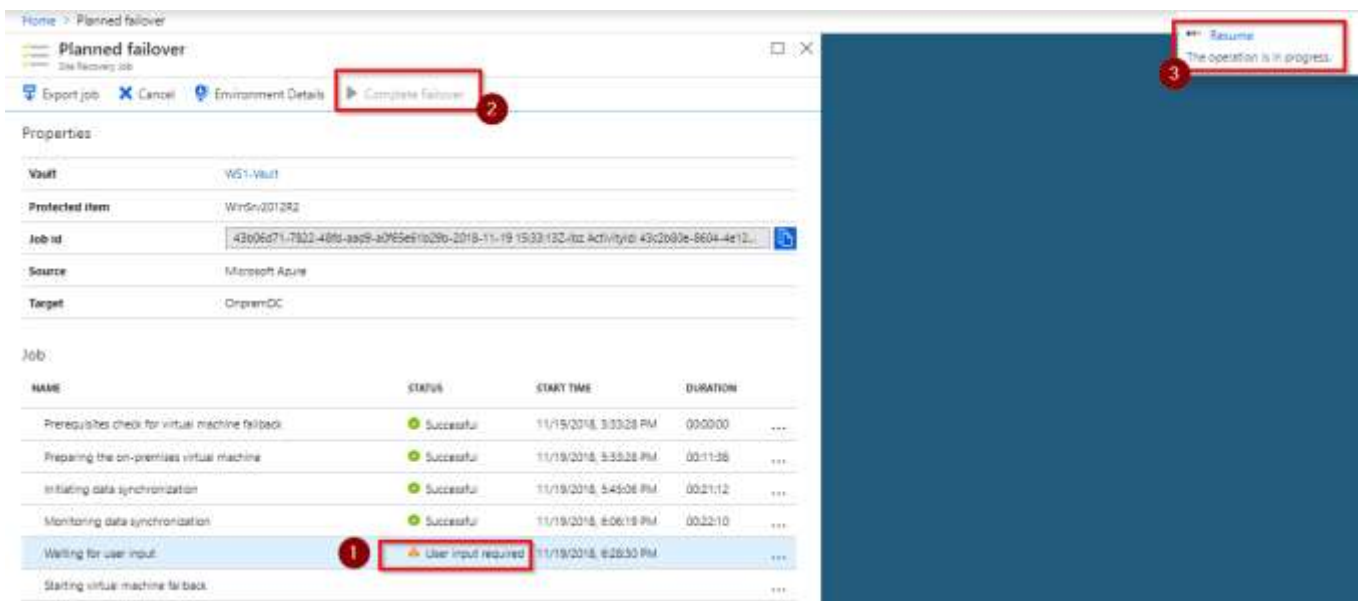
Patikrinkite atstatytą Azure VM, pabandykite prisijungti.

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:



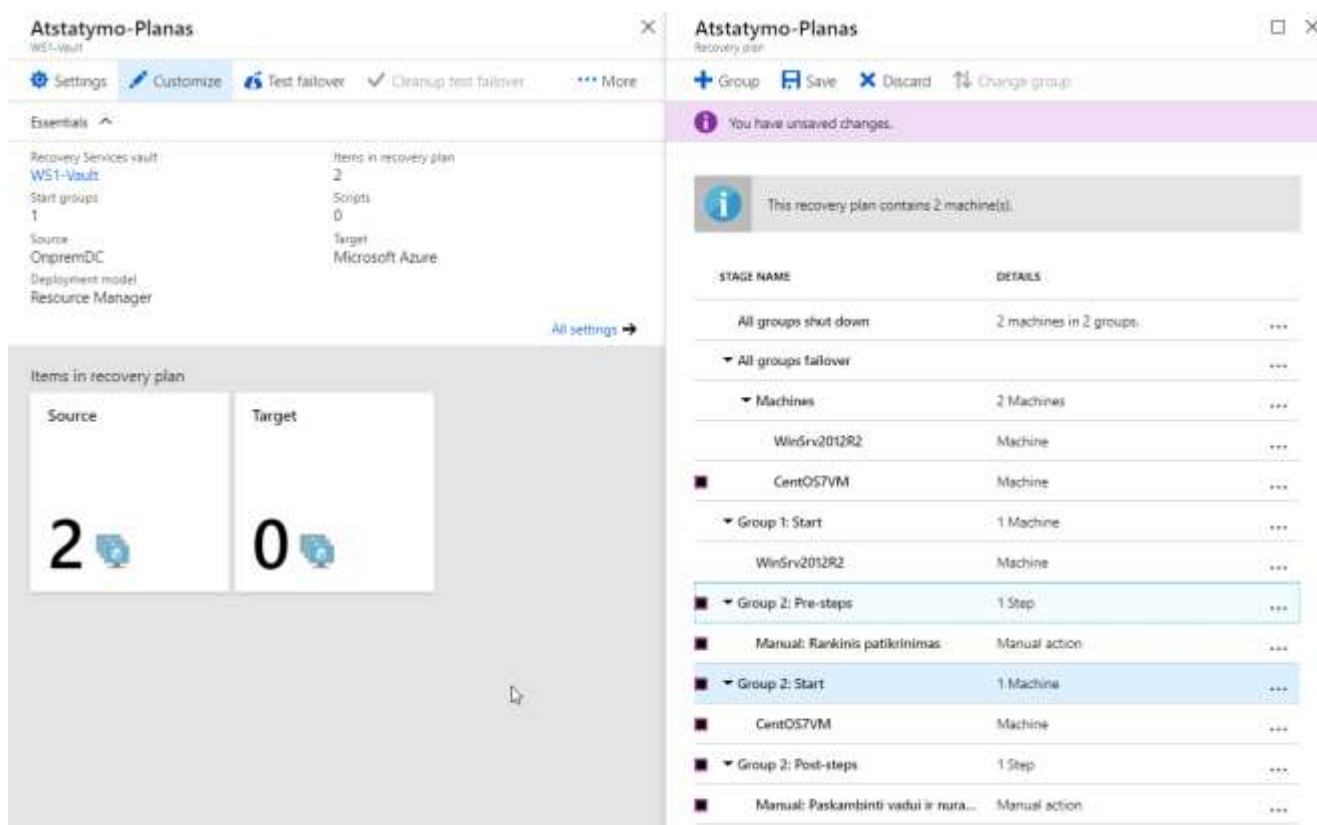
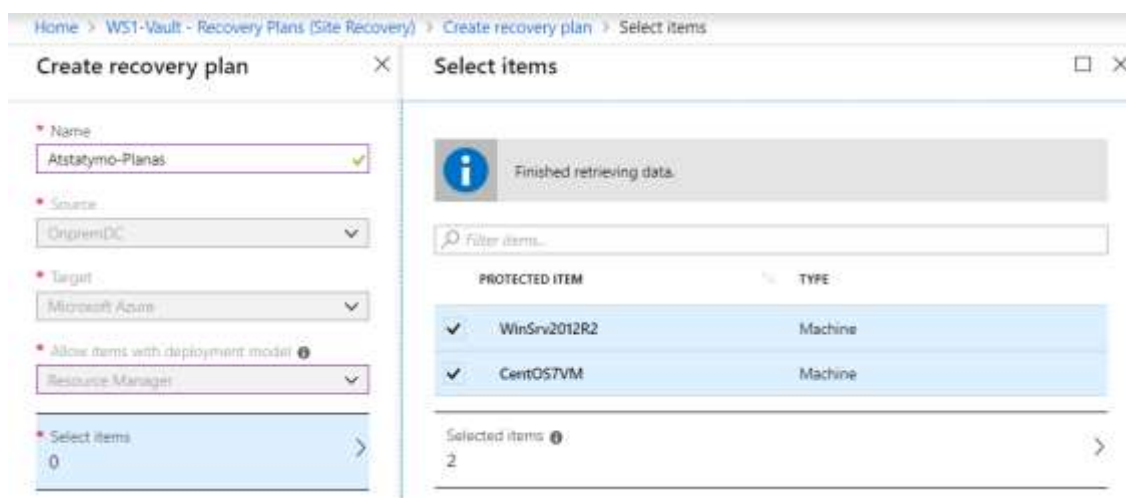
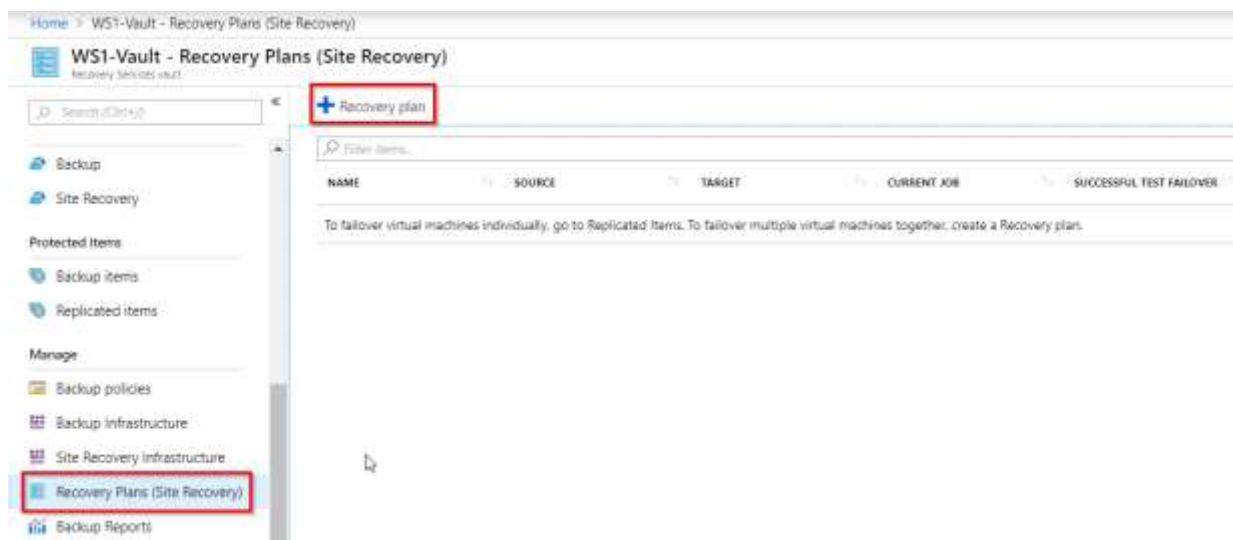
Kai VM atstatoma į Hyper-V lieka patvirtinti paspaudžiant “Commit”. Tuomet vėl replikuojama iš Onprem į Azure.

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

Cleanup test failover

Commit

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




11. Azure to Azure ASR

Replikavimas į kitą regioną:

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

Configure disaster recovery



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 - MRM	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