

Lab network

Our on-premises network consists of a Windows 2008 server and a phone system running on windows 7 both of which are physical servers.

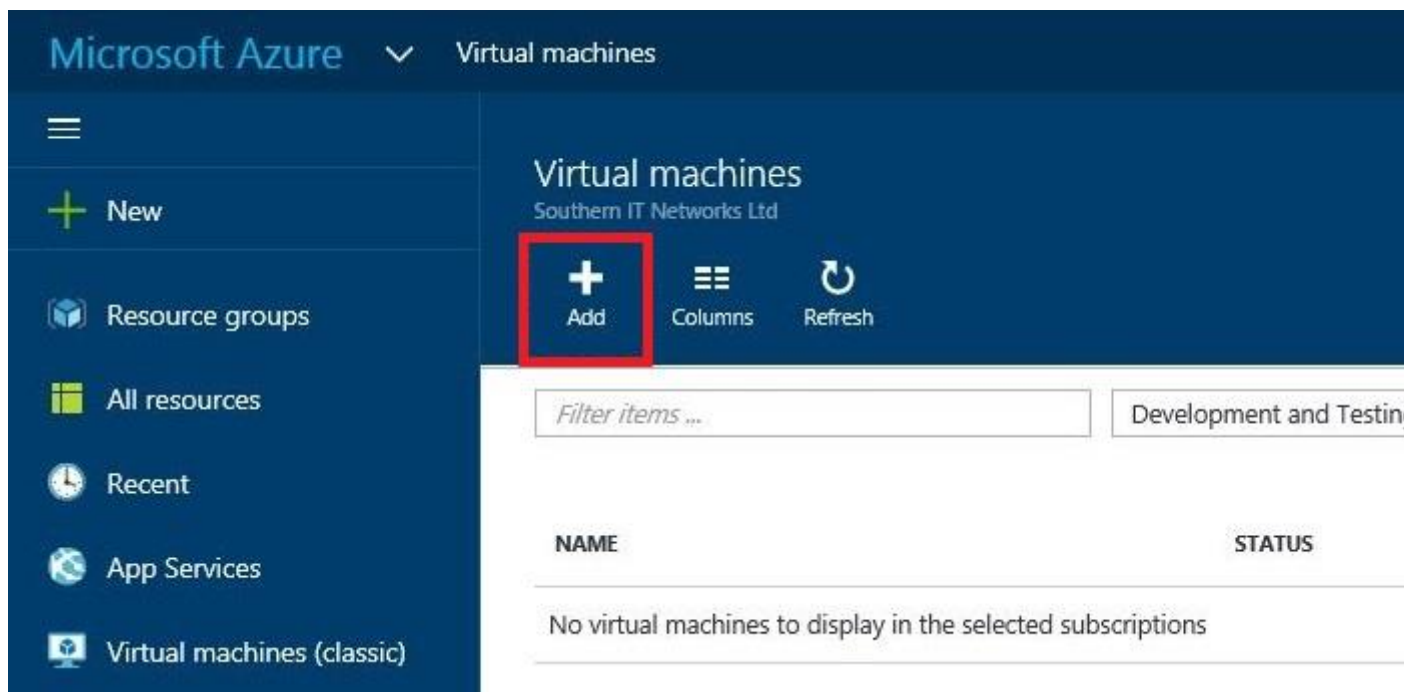
Goal

Our goal is to backup both of these machines and have a local and offsite copy ready to boot up within a moments notice.

Setup Guide

First thing we need to do is create a new VM which will run the recovery console and pull down the latest backups and save the data into VHD's. This does mean you are required to have at least one VM running at all times to manage the system.

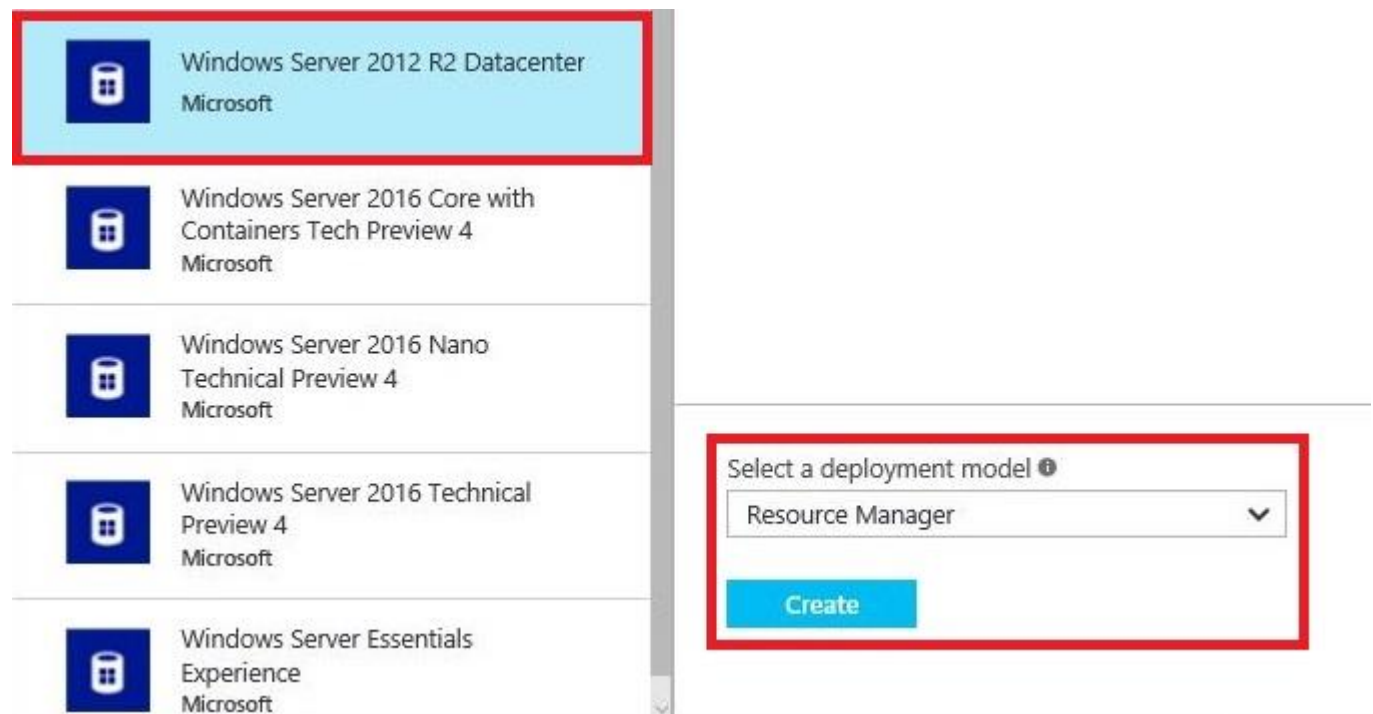
Go to Virtual Machines and press Add.



Select a windows server then Windows Server 2012R2 Datacenter.



Choose Resource Manager as the deployment model and select Create.



Give your VM a name, here we choose 'MaxBacukpMgmtVM', enter a username, password, resource group and location. Remember to keep all of your VM's in the same location then press Ok.

Create virtual machine

Basics

1 Basics
Configure basic settings >

2 Size
Choose virtual machine size >

3 Settings
Configure optional features >

4 Summary
Windows Server 2012 R2 Datacenter >

* Name
MaxBackupMgmtVM ✓

* User name
✓

* Password
✓

* Subscription
Development and Testing Credits >

* Resource group
MaxBackupResourceGroup ✓

Select existing

* Location
North Europe >

OK

Now select the size of the VM but it really doesn't need to be anything special if you are restoring only a few VM's. Here I select a basic DS1 and press Select.

1 Basics
Done

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Summary
Windows Server 2012 R2 Datacenter

Prices presented below are estimated retail prices that include applicable third-party software costs. Prices do not reflect applicable taxes and may include currency conversions.

| DS1 Standard | | DS2 Standard | |
|--------------------------------|-------|-------------------------------|-------|
| 1 | Core | 2 | Cores |
| 3.5 | GB | 7 | GB |
| 2 Data disks | | 4 Data disks | |
| 3200 Max IOPS | | 6400 Max IOPS | |
| 7 GB Local SSD | | 14 GB Local SSD | |
| Load balancing | | Load balancing | |
| Auto scale | | Auto scale | |
| Premium disk supp... | | Premium disk supp... | |
| 33.18 GBP/MONTH (ESTIMATED) | | 66.3 GBP/MONTH (ESTIMATED) | |
| DS4 Standard | | DS11 Standard | |
| 8 | Cores | 2 | Cores |

Select

Now we fill in a few advanced settings but the only important one here is the Storage account so give it something meaningful. All VM's that get created must be in the same storage group so we must select this group later when we configure each VM we want to configure for recovery.

1 Basics
Done

2 Size
Done

3 Settings
Configure optional features

4 Summary
Windows Server 2012 R2 Datac...

Storage

Disk type ⓘ
Standard Premium (SSD)

* Storage account ⓘ
(new) maxbackupstoragegroup

Network

* Virtual network ⓘ
(new) MaxBackupNetwork

* Subnet ⓘ
default (10.0.0.0/24)

* Public IP address ⓘ
(new) MaxBackupPublicIP

* Network security group ⓘ
(new) MaxBackupSecurityGroup

Monitoring

OK

Everything looks good so OK to finish.

| | | |
|---|--------------------------------------------|---|
| 1 | Basics Done | ✓ |
| 2 | Size Done | ✓ |
| 3 | Settings Done | ✓ |
| 4 | Summary Windows Server 2012 R2 Datac... | > |

| Basics | |
|----------------|---------------------------|
| Subscription | Development and Testing C |
| Resource group | (new) MaxBackupResource |
| Location | North Europe |

| Settings | |
|-----------------------------|-----------------------------|
| Computer name | MaxBackupMgmtVM |
| User name | southernit |
| Size | Standard DS1 |
| Disk type | Standard |
| Storage account | (new) maxbackupstoragegr |
| Virtual network | (new) MaxBackupNetwork |
| Subnet | (new) default (10.0.0.0/24) |
| Public IP address | (new) MaxBackupPublicIP |
| Network security group | (new) MaxBackupSecurityG |
| Availability set | None |
| Diagnostics | Enabled |
| Diagnostics storage account | (new) maxbackupstoragegr |

OK

Wait a few minutes for the deployment to complete.



Once the deployment has completed login to your new management VM and browse to: <http://downloads.maxfocus.com> and select 'Additional Tools'.



CLOUD MANAGEMENT CONSOLE

Download the latest version of MAX Backup [Cloud Management Console](#). Simply click the button below to receive the most recent edition for your operating system.

[DOWNLOAD](#)



RELEASE NOTES

Review the latest features, functions and upgrades for the MAX Backup cloud software.

[READ MORE](#)

Download the Recovery console, here I used the 64bit version.



ADDITIONAL TOOLS



RECOVERY CONSOLE

WINDOWS X86

WINDOWS X64

[Manual](#)

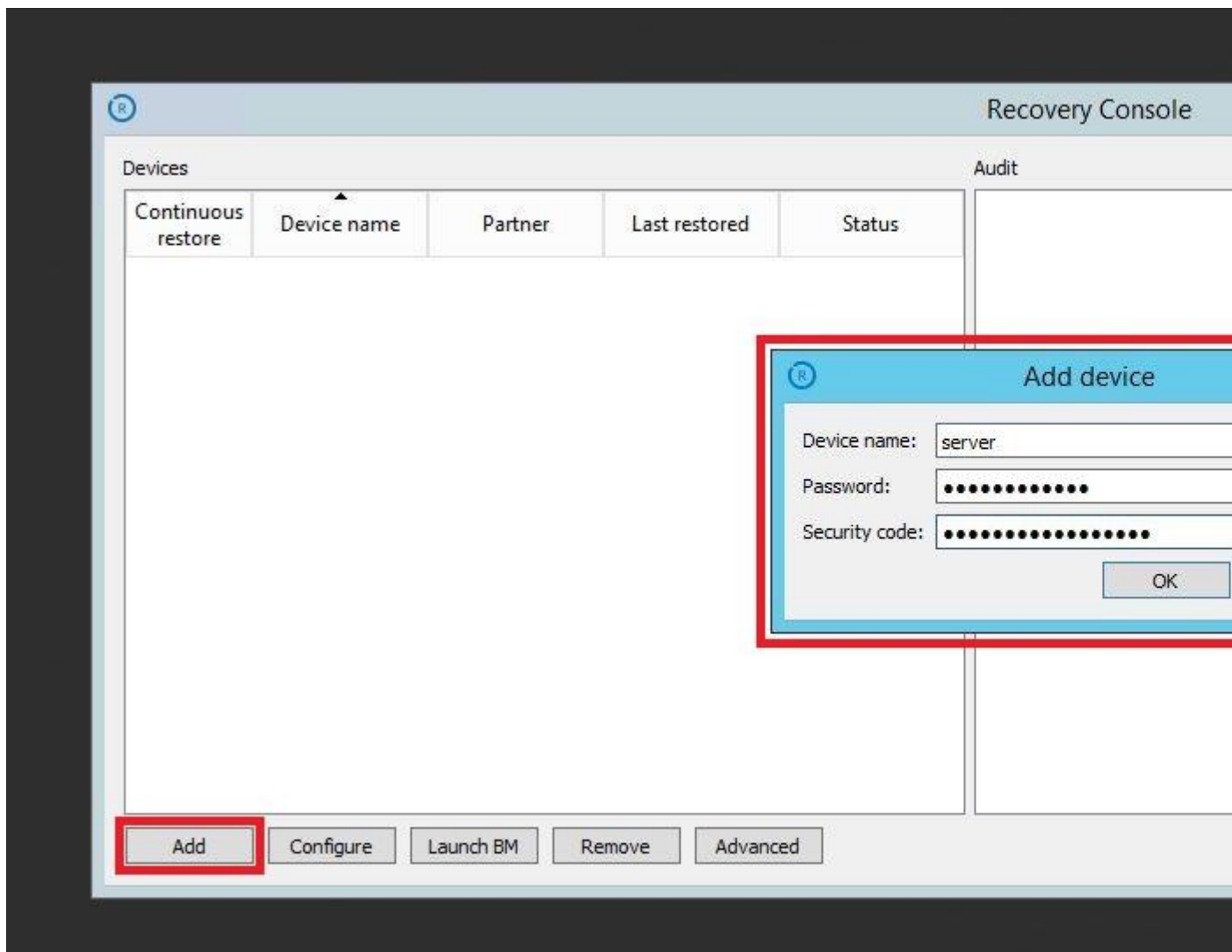


SERVER TOOL

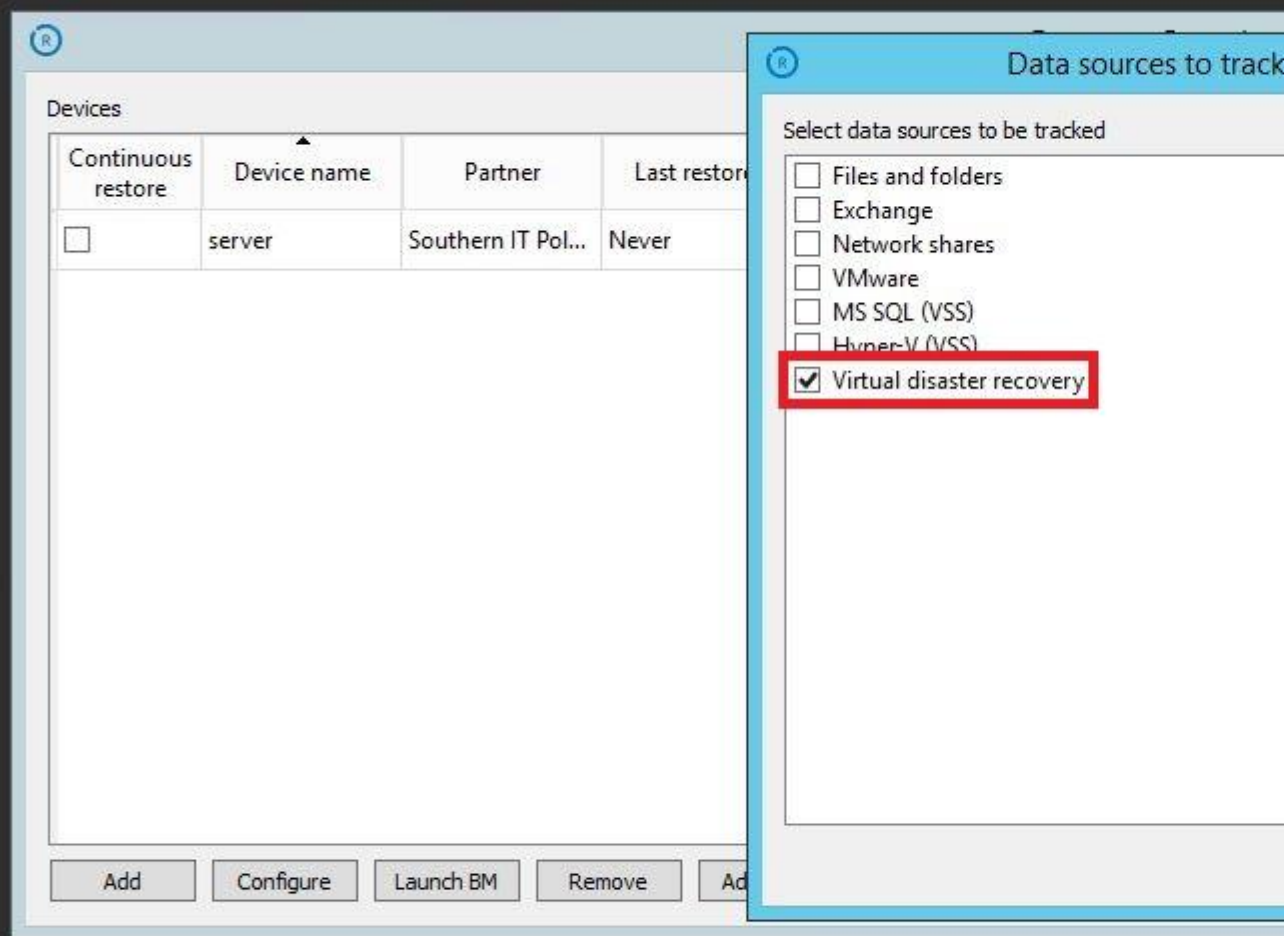
Download and run the installer.



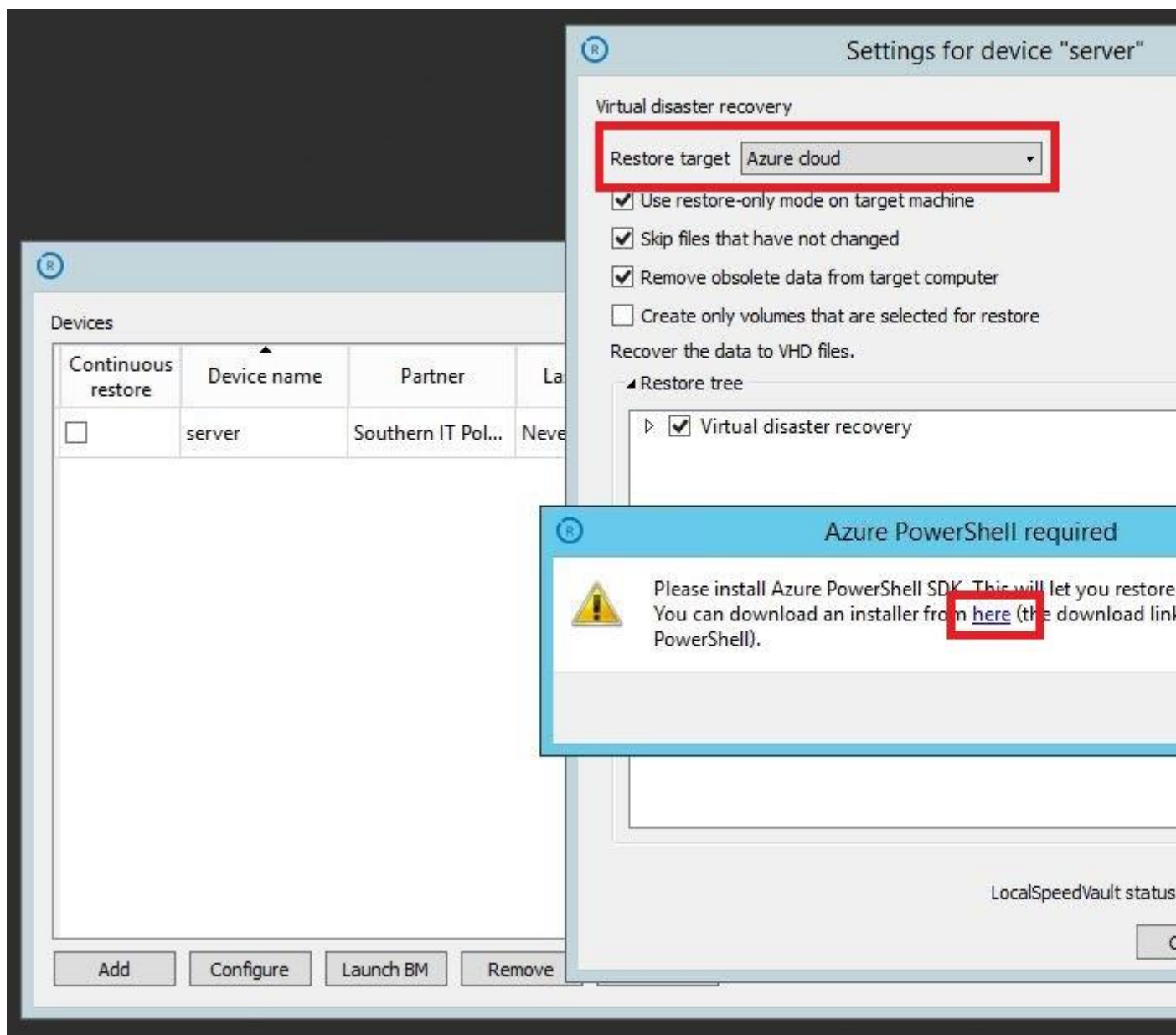
Ok so we have the Recovery console running on our VM lets add a server we wish to configure for constant recovery. Enter a meaning full name for the server but I would suggest using the hostname of the VM you are setting up. Enter the Password and encryption key for the VM. If you are not sure what the password is you can get them from the Cloud Management Console.



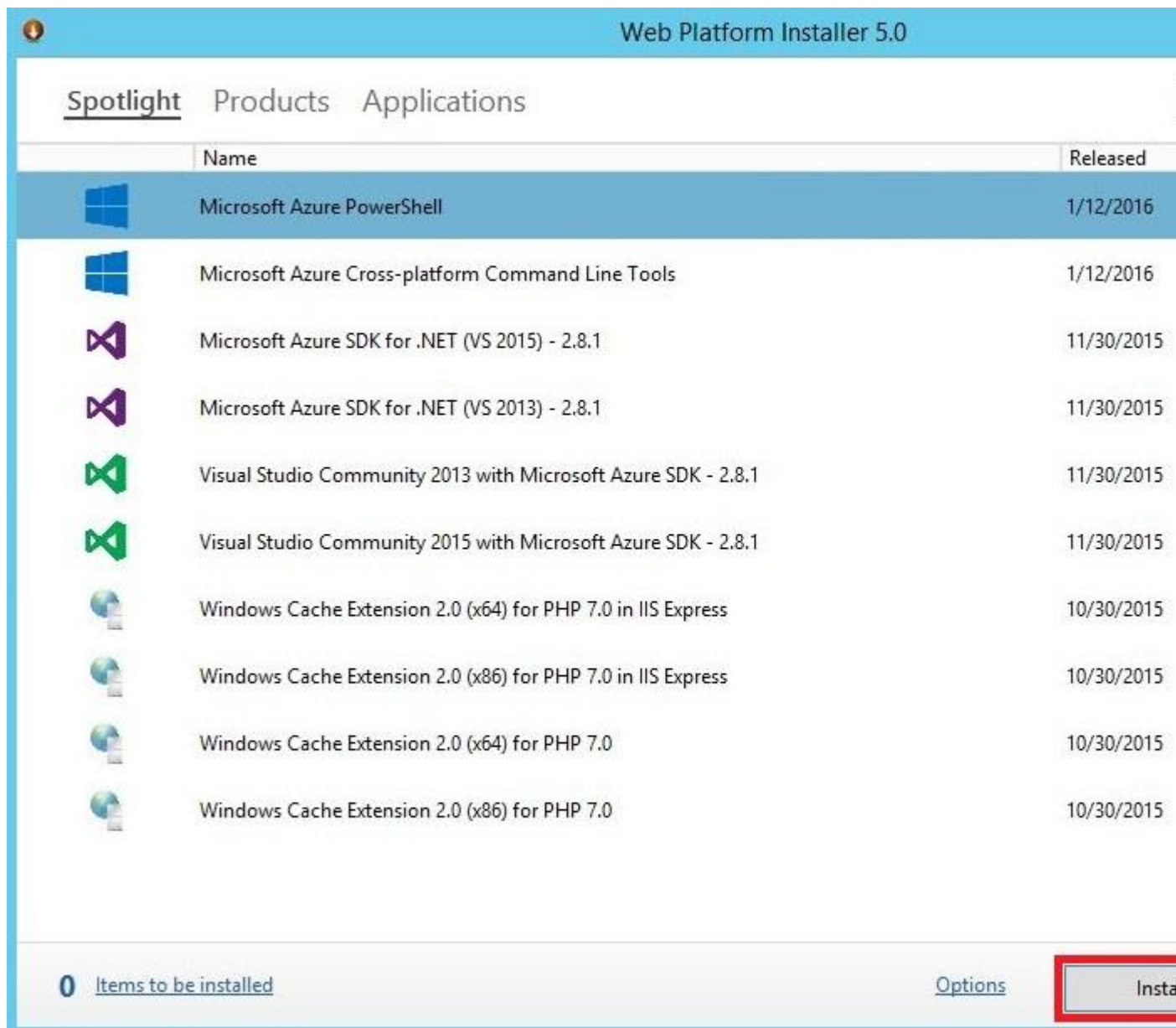
Next select 'Virtual disaster recovery.



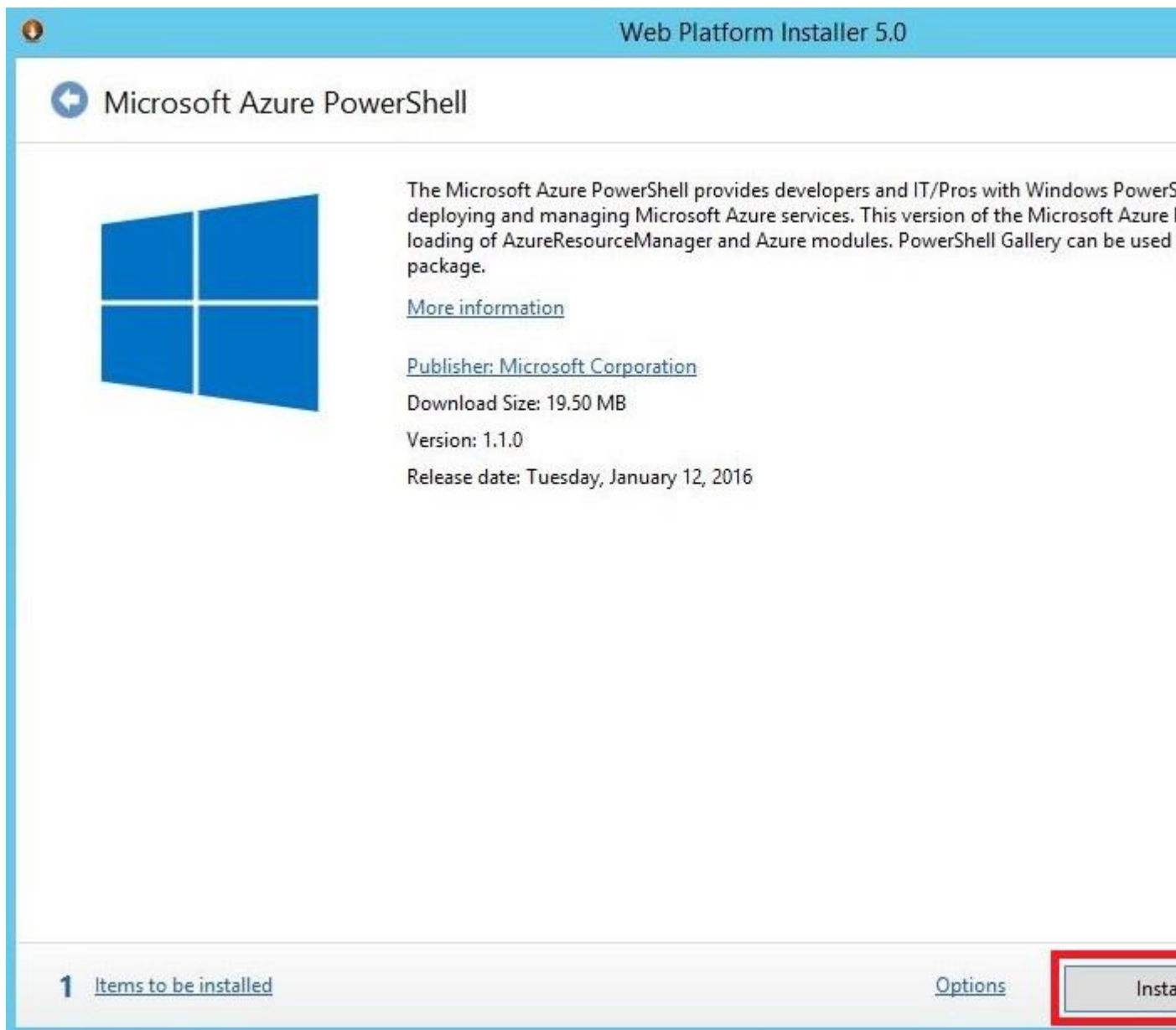
Select the Restore target to be 'Azure cloud' and you will then be prompted to install the Azure PowerShell SDK. Take a slight tangent and go download it by clicking the link.



The installer runs so let's select 'Microsoft Azure PowerShell' and press 'Add' then 'Next'.



Press 'Install'



Once the install finishes exit the installer and go back to configuring the VM in the recovery console.

Now we change the Restore target back to 'Azure cloud' which gives us lots of options to play with.

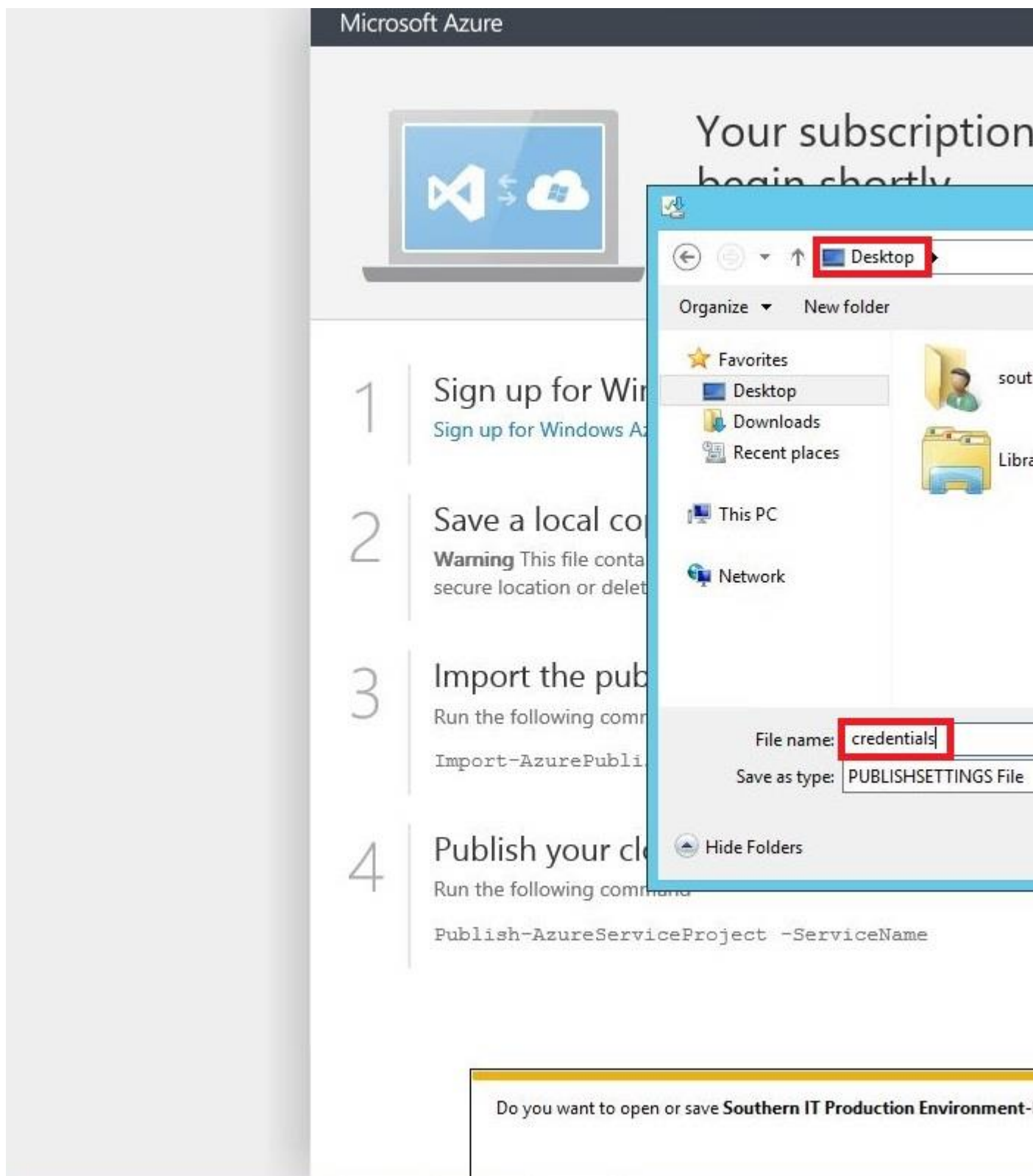
Click the 'Download credentials file' now because we need a special file from Azure which the Recovery console will use to connect.

▲ Access to virtual machine

Credentials file

[Download credentials file](#)

Clicking the download link will open up your web browser and prompt you to log into the Azure account you are using to host the DR network. Once you log in save the credentials file and put it somewhere safe where it won't get moved or deleted.



Now we have the file we can click Browse and select the credentials file we just downloaded.

After that you need to specify a name for the new virtual machine and service it will use. These two options need to be unique but relate to the same virtual machine. Just for info the service is a name we use to connect to the virtual machine remotely later.

Ensure the tick boxes are ticked as shown then press 'Create network' to setup the network used in Azure.

Settings for device "server"

Virtual disaster recovery

Restore target: Azure cloud

☐ Clean temporary data after restore

☒ Use restore-only mode on target machine

☒ Skip files that have not changed

☒ Remove obsolete data from target computer

☐ Create only volumes that are selected for restore

Recover the data to a new virtual machine created in the Azure Cloud (a Microsoft Azure account is required).

▶ Restore tree

▲ Access to virtual machine

Credentials file: C:\Users\southernit\Desktop\credentials.publishsettings ?

[Download credentials file](#) Browse

Subscription: Development and Testing Credits (748c6808-77af-47c ?

Machine name: SITServerVM ?

Service name: SITDRServiceServerVM ?

▲ Virtual machine properties (optional)

☐ Boot disk size (GB) ?

Machine location: North Europe ?

Machine size: Standard_D1 (1 cores, 3584 MB) ?

Storage type: Standard_LRS ?

DNS server:

☒ Enable Remote Desktop

☒ My new VM should be part of virtual network

▲ Virtual network settings

Create network

Network name: ?

Subnet name: ?

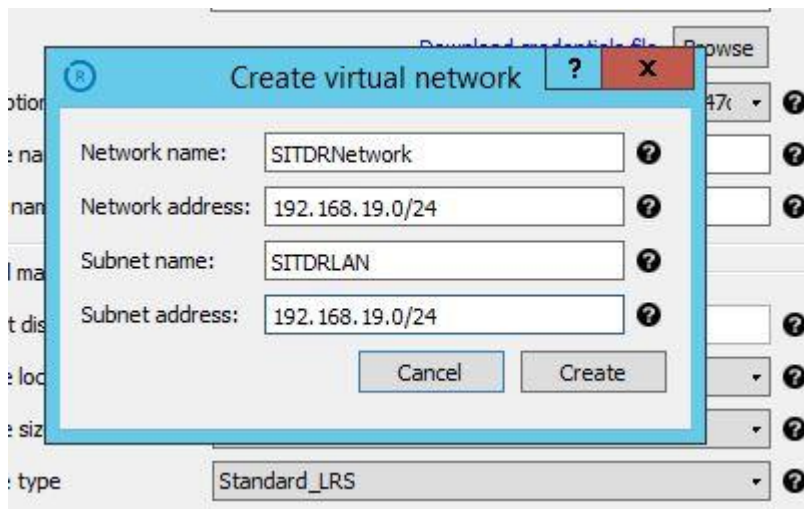
Static IP-address: ?

LocalSpeedVault status: disabled [Configure](#)

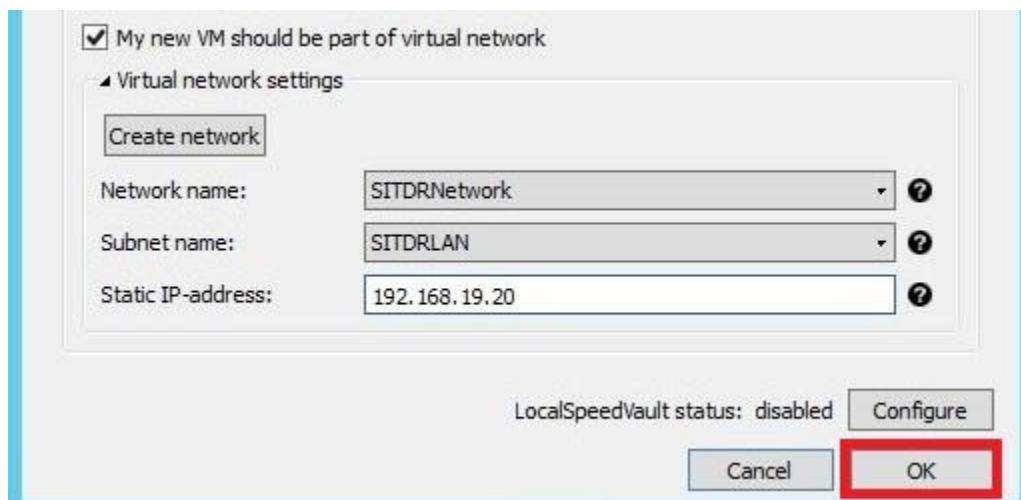
Cancel OK

In this lab we only have one subnet 192.168.19.0/24 so we configure it as shown. These network settings must match your on-premises network

exactly. So if your internal LAN is setup with 192.168.0.0/24 or 192.168.1.1/24 then enter your details as required. Remember the virtual machines hosted in Azure will mirror your on-premises setup which includes the network address and individual server IP addresses.

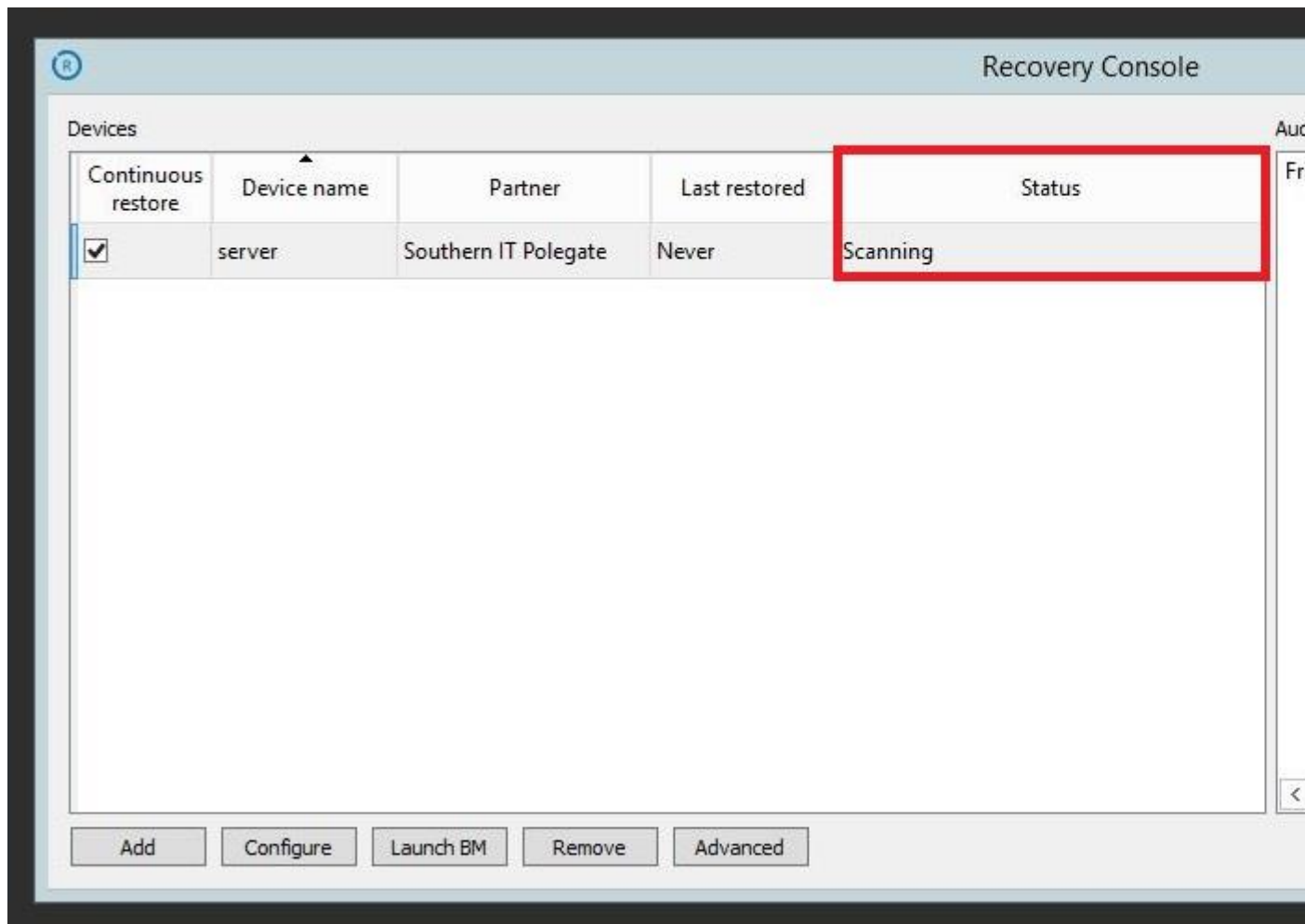


Now we've created the network we set this server to have a static IP address. Again this is the same IP address that the on-premises server is using. Here we set the static IP address for our server as 192.168.19.20 and press OK.



Now the magic starts to happen, you will notice the status change after a few minutes and will eventually turn to 'Monitoring'. This means its waiting for changes to occur in the backup set. When it detects changes it will

automatically start downloading the data and create the virtual machines, network and VHD files.



Now you run through the same process for each server you want to setup. Here I configure with the same options as before except I change the machine and service name and set the static IP to match the real server on site in our office.

Settings for device "pbx"

Virtual disaster recovery

Restore target: Azure cloud

☐ Clean temporary data after restore

☒ Use restore-only mode on target machine

☒ Skip files that have not changed

☒ Remove obsolete data from target computer

☐ Create only volumes that are selected for restore

Recover the data to a new virtual machine created in the Azure Cloud (a Microsoft Azure account is required).

▶ Restore tree

▲ Access to virtual machine

Credentials file: C:\Users\southernit\Desktop\credentials.publishsettings ?

[Download credentials file](#) Browse

Subscription: Development and Testing Credits (748c6808-77af-47cf-889d-2bf073d12eb4) ?

Machine name: SITPBXVM ?

Service name: SITDRServicePBX ?

▲ Virtual machine properties (optional)

☐ Boot disk size (GB) ?

Machine location: North Europe ?

Machine size: ExtraSmall (1 cores, 768 MB) ?

Storage type: Standard_LRS ?

DNS server:

☒ Enable Remote Desktop

☒ My new VM should be part of virtual network

▲ Virtual network settings

Create network

Network name: SITDRNetwork ?

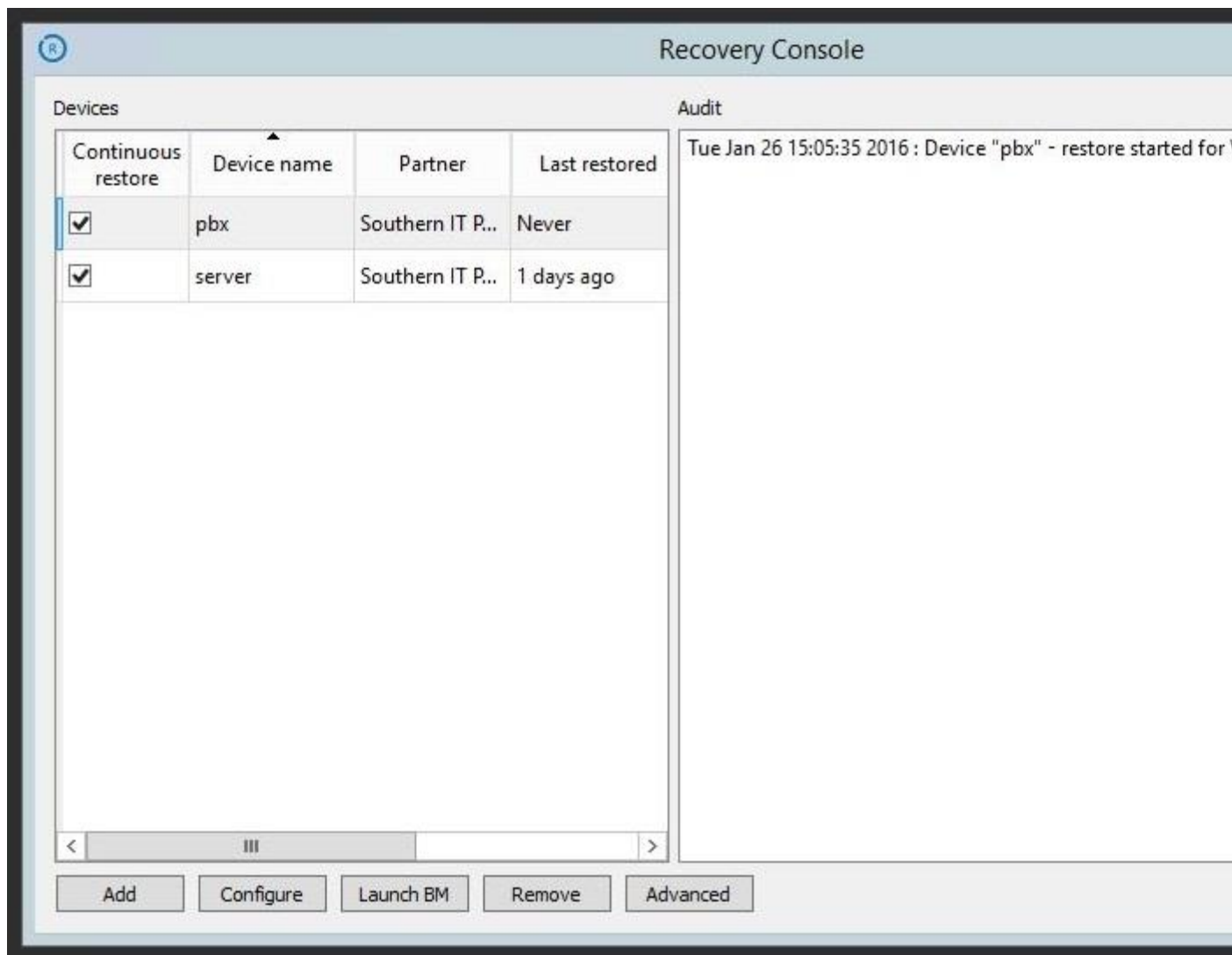
Subnet name: SITDRLAN ?

Static IP-address: 192.168.19.39 ?

LocalSpeedVault status: enabled Configure

Cancel OK

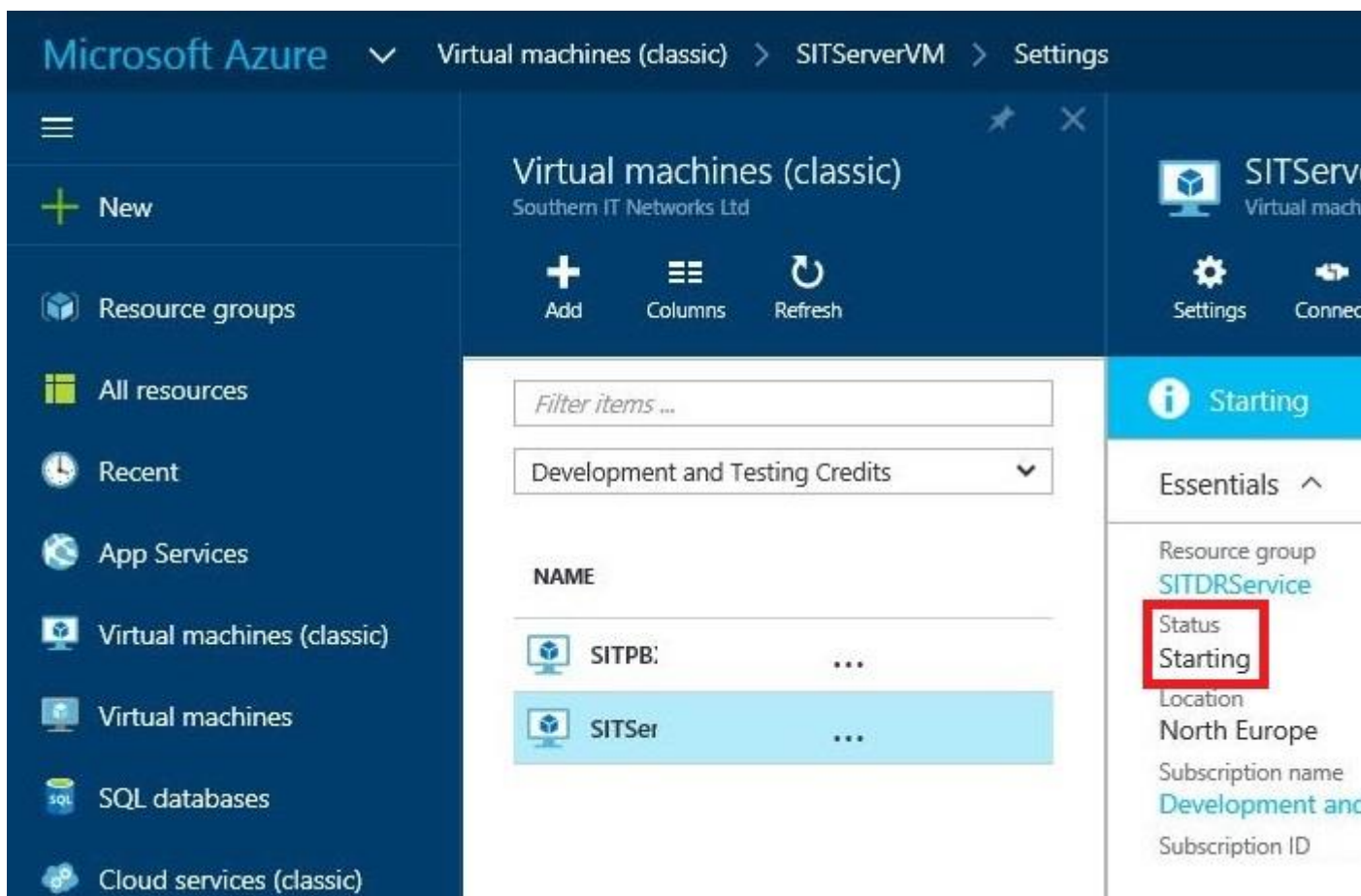
Once done we can see both devices in the list and when your ready tick all servers to enable 'Continuous restore'.



Once the Recovery console has finished downloading the data and had time to configure Azure you will find the virtual machines sitting there ready to be turned on!

| Virtual machines (classic) | | |
|-----------------------------------------------------------------------------------------------------------------------|-----------------------|-----------|
| Southern IT Networks Ltd | | |
| <div> <div>+</div> <div>≡</div> <div>↺</div> </div> <div> <div>Add</div> <div>Columns</div> <div>Refresh</div> </div> | | |
| <div>Filter items ...</div> <div>Development and Testing Credits</div> | | |
| NAME | STATUS | LOCATION |
|  SITPBXVM | Stopped (deallocated) | North Eur |
|  SITServerVM | Stopped (deallocated) | North Eur |

If you need to test them simply select one of the servers and start it up.



The screenshot shows the Microsoft Azure portal interface. On the left is a navigation pane with options like 'New', 'Resource groups', 'All resources', 'Recent', 'App Services', 'Virtual machines (classic)', 'Virtual machines', 'SQL databases', and 'Cloud services (classic)'. The main area displays 'Virtual machines (classic)' for 'Southern IT Networks Ltd'. It includes a table with columns 'NAME', 'STATUS', and 'LOCATION'. Two VMs are listed: 'SITPBXVM' and 'SITServerVM', both with a status of 'Stopped (deallocated)'. The 'SITServerVM' row is highlighted. On the right, a 'Starting' status panel is visible, showing 'Status Starting' (highlighted with a red box), 'Location North Europe', 'Subscription name Development and Testing Credits', and 'Subscription ID'.

Once its started you can then press connect and login to verify everything is working as expected. Just remember to stop the machine so its becomes de-

allocated in Azure. If you don't you could still be charged for the VM because its technically still alive. Just ensure all machines say 'Stopped (deallocated)' and if they do you will only be charged for the storage space. Should you ever need to activate this network you then get charged for the storage space and for the running of the virtual machines.

So we have configured an offsite hot standby DR network in Azure but we can also do something similar onsite too. This gives you the ability to have a hot standby virtual machine should anything happen to a single server. Within a few minutes you can activate the local copy but that's another blog post for another time.

The last thing to think about is how would users connect to this network if they ever needed it? Its actually pretty easy to configure a VPN but I may do a post on how to do it soon.