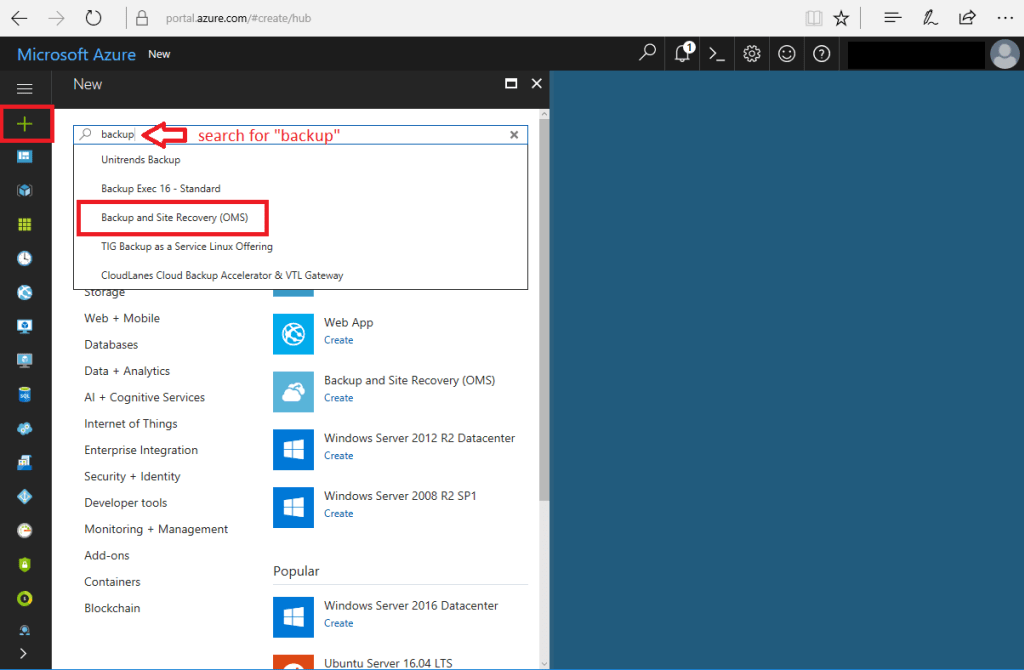
Azure Backup agent only supported file and folder backup from an on-premises server to the cloud. We now have support for System State protection added to this list, so we will cover how to configure that today. Azure Backup also offers other ways to protect your on-premises application workloads, as well as virtual machines, but we will cover those topics in future posts.

The steps in this tutorial are:

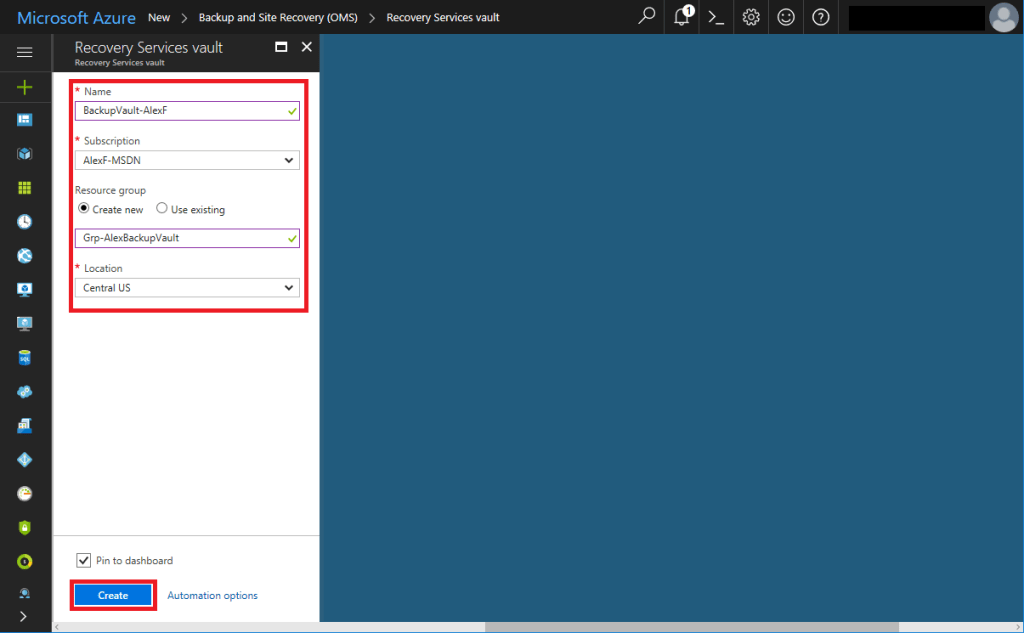
1. Create an Azure Recovery Services vault
2. Download the MARS Agent and your vault credentials
3. Install the agent and provide your credentials
4. a. Enable System State Backup  
   b. Configure the MARS Agent Backup Schedule
5. Setup Notifications

1. Create an Azure Recovery Services vault

Before you install the MARS agent, you will need to sign into your Azure portal and create a Recovery Services Vault (which they have apparently renamed again). Click **New (+)** then start typing “Backup” to find **Backup and Site Recovery (OMS)** in the list–or some other name by the time you read this, perhaps.

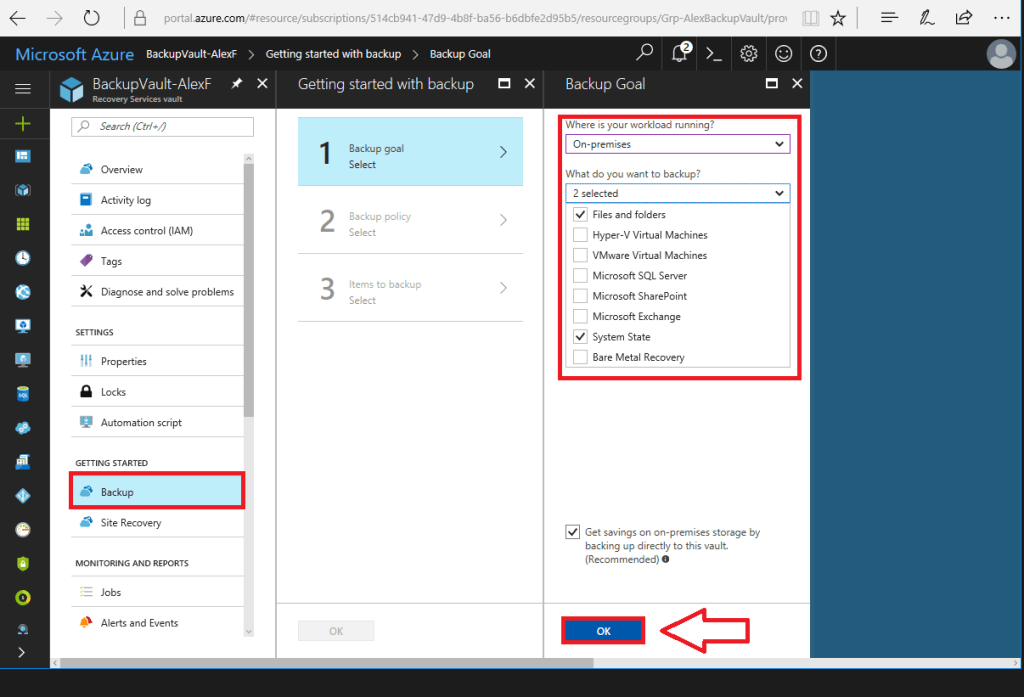


Next, click on **Create.** Then you need to fill out some options, like naming the vault, choosing a region and so on. Click **Create** again when you’re done.

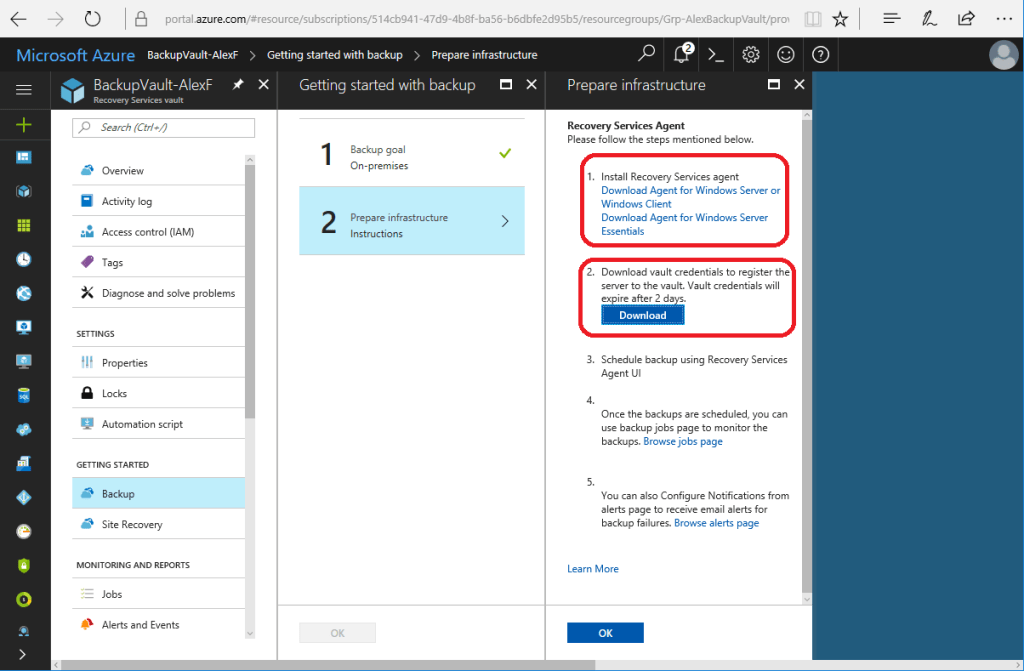


2. Download the MARS agent and your vault credentials

Once Azure is finished provisioning your resources, you can click through to your vault, and go to **Backup** under **Getting Started**. Based on the selections you make here, it will recommend one of the various Azure Backup solutions. Choose **On-premises**, and then **Files and folders** and/or **System State**. Click **OK**.

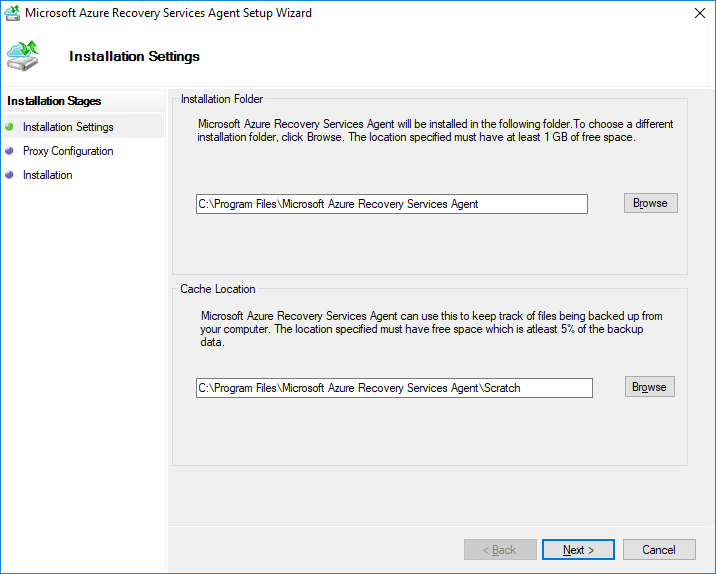


The big downside to this process is, there isn’t really an “automatic way” to deploy this solution. It’s a manual install per machine, and you’ll need both of these downloads to complete the setup. Use the links for **Download Agent for Windows Server or Windows Client**, as well as the **Download**button for vault credentials.

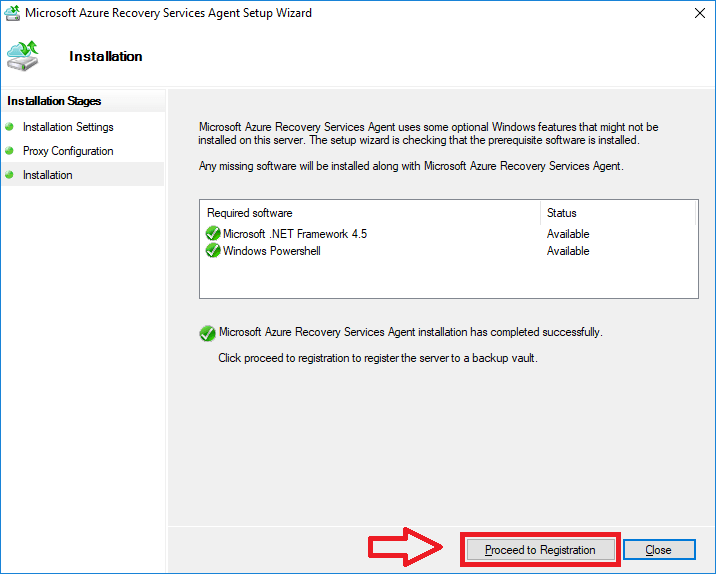


3. Install the agent and provide credentials

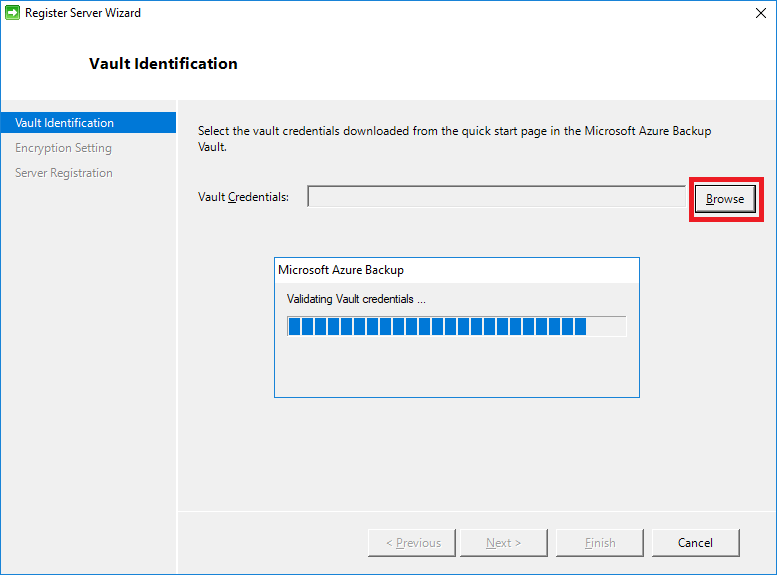
Step through the setup wizard one screen at a time. **Next**, **Next**click **Install**.



When it has finished the agent installation, click **Proceed to Registration**.

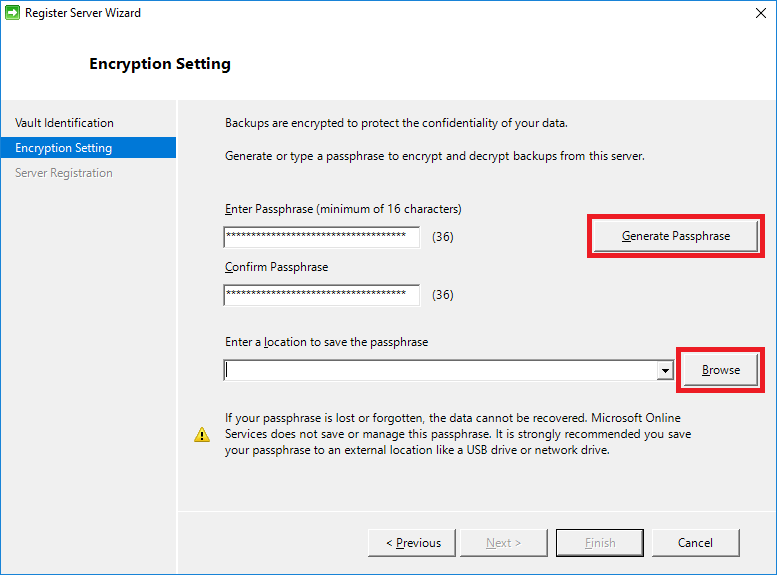


And here you will **Browse** to find and select the credentials you downloaded earlier from Azure.



Note: if you just downloaded your credentials but the wizard rejects them, suggesting that you should download them again and use within two days, check your system clock–and be sure you are syncing to a proper time authority.

After your credentials are validated, you will choose or generate an encryption passphrase, and save it to a file (store this somewhere safe for your customers, not on the local machine).

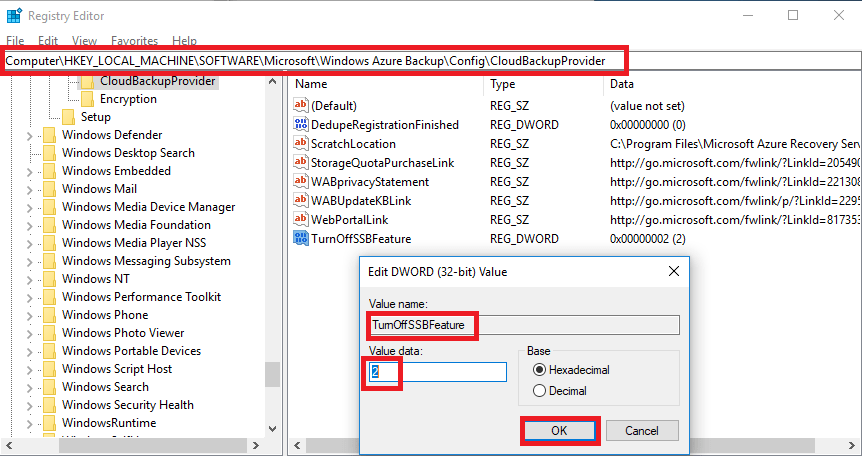


After you complete this wizard, you will be given the option to launch the Azure Recovery Services Agent. Click **Close** to proceed.

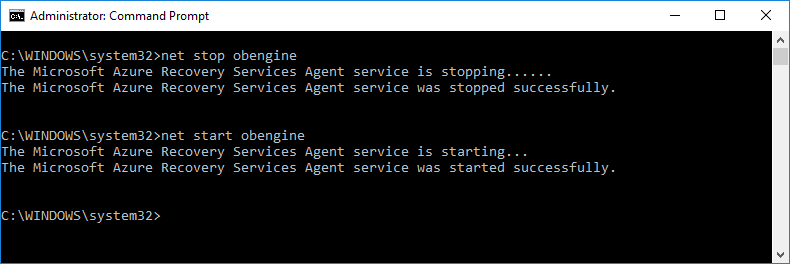
4a. Enable System State Backup (recommended)

NOTE: If you want to include the System State (critical for Domain Controllers), then at the time of this writing you will need to create a new registry key as follows:

Create a new **REG\_DWORD**value called **TurnOffSSBFeature** in **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Config\CloudBackupProvider** and set the value to **2**.

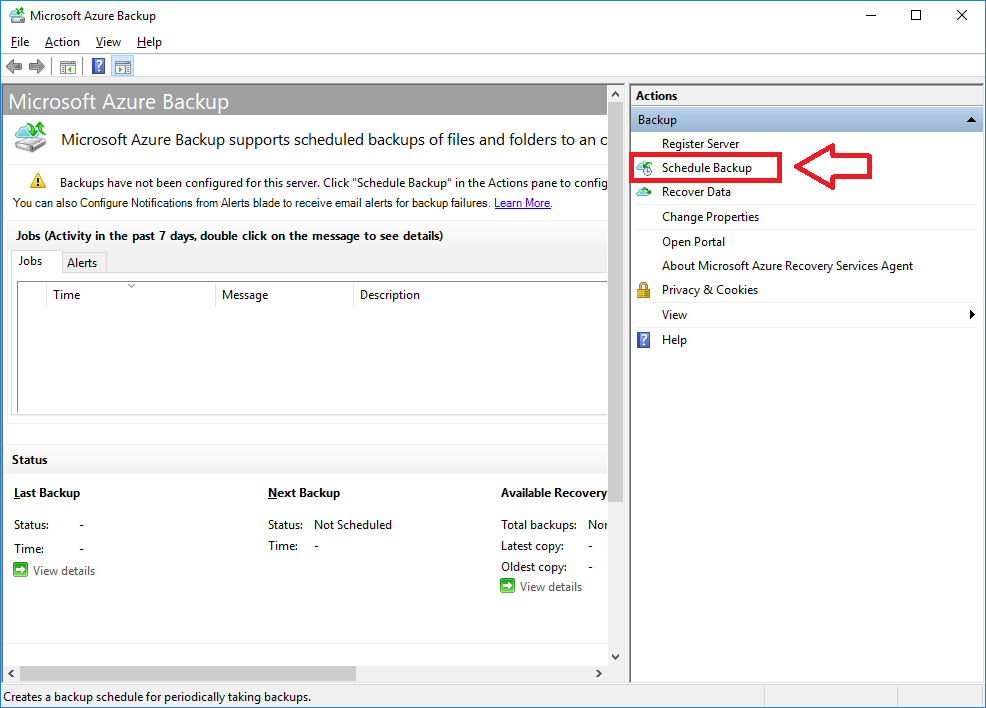


Be sure to restart the Microsoft Azure Recovery Services Agent (obengine) service before configuring your backup.

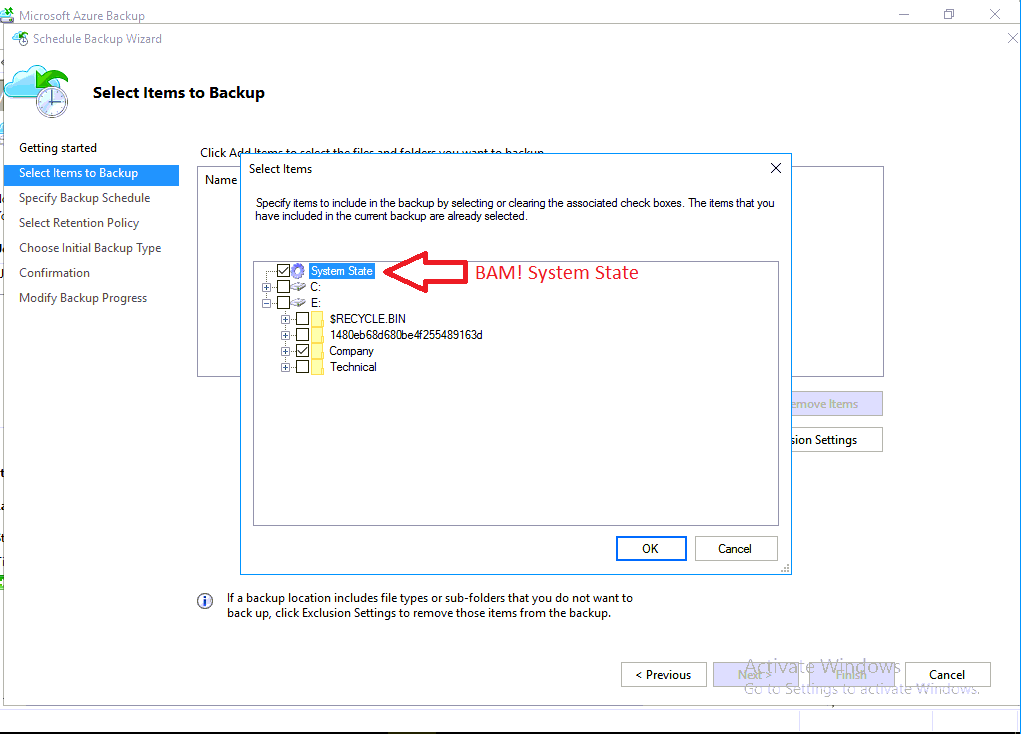


4b. Configure the MARS Agent Backup Schedule

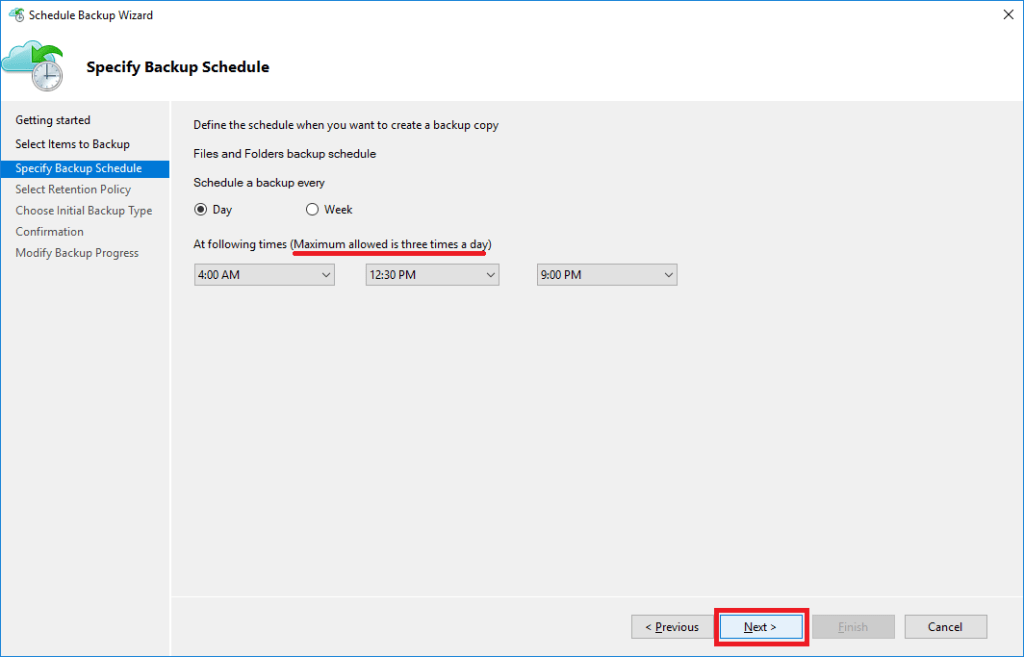
The Microsoft Azure Backup console will look very familiar to most Windows Admins (it has an uncanny resemblance to Windows Server Backup. Click **Schedule Backup**to begin.



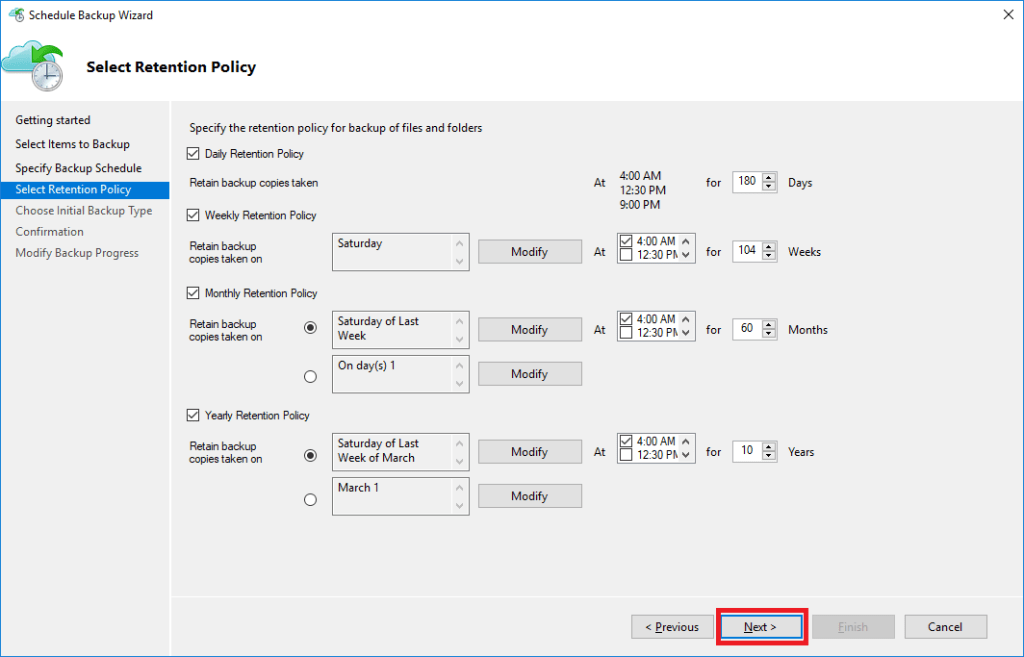
Step through the wizard adding the items you need to protect. You will notice that there is an option for System State now!



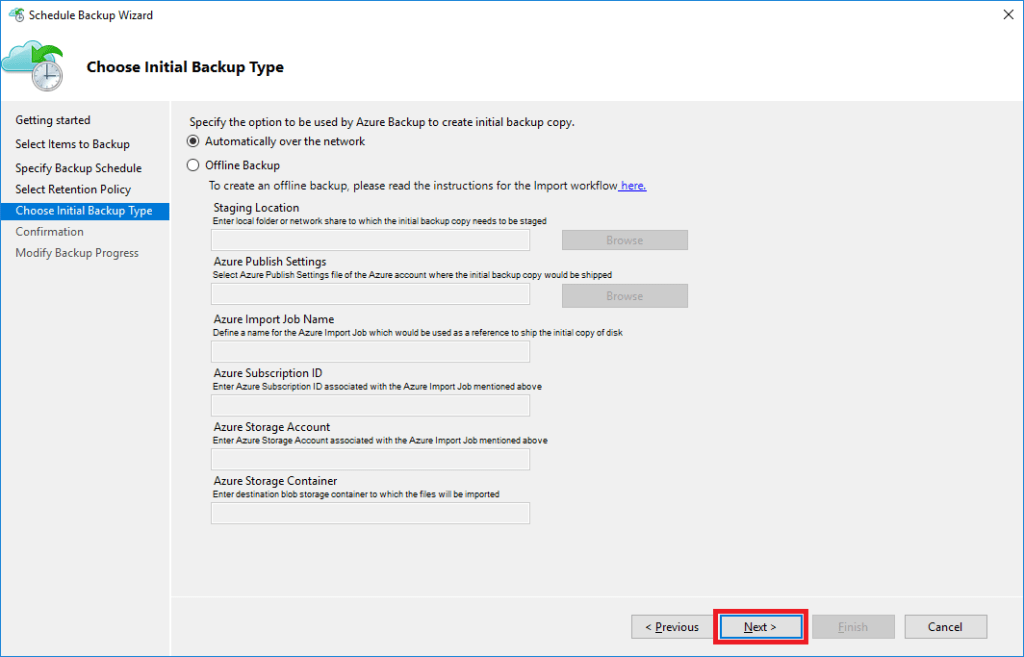
Although many small businesses will be okay with one backup per day, it is always a good idea to go through a downtime tolerance exercise with your clients, to ensure that you are on the same page about RPO and RTO when designing a backup & disaster recovery solution. We can configure a maximum of three backups per day here. Click **Next**.



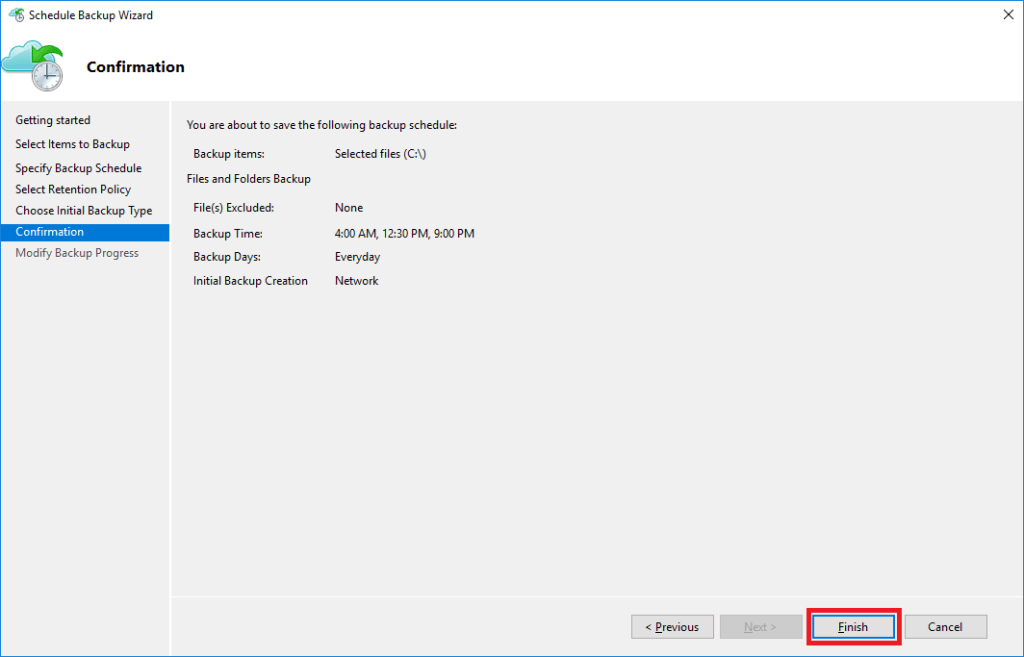
As I mentioned, retention options have grown substantially and is one of the reasons we are seeing more adoption of this service in the SMB / SME space. Modify the default values as needed, then click **Next**.



Most of us will just choose to upload the backup directly from the server into the Azure cloud, however, some folks may choose to pre-seed the data in Azure by sending physical media (so that you only have to upload incremental changes over the wire). There is an offline option here with a link to further instructions, but otherwise just accept the default: **Automatically over the network**. **Next**.

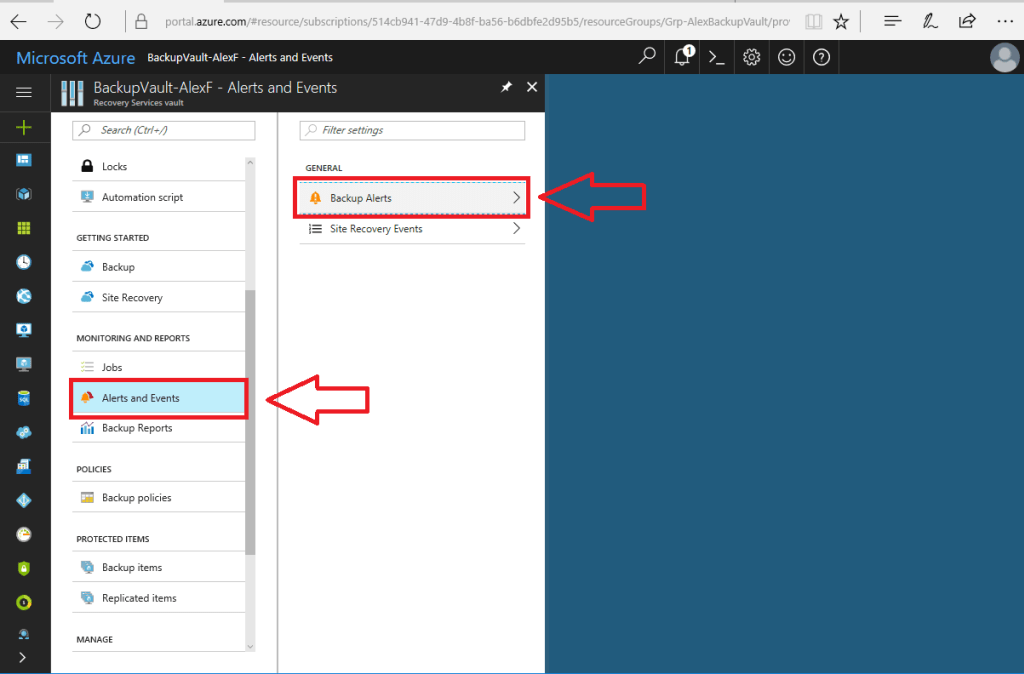


And just like that, you’re done. Review your selections and click **Finish.**

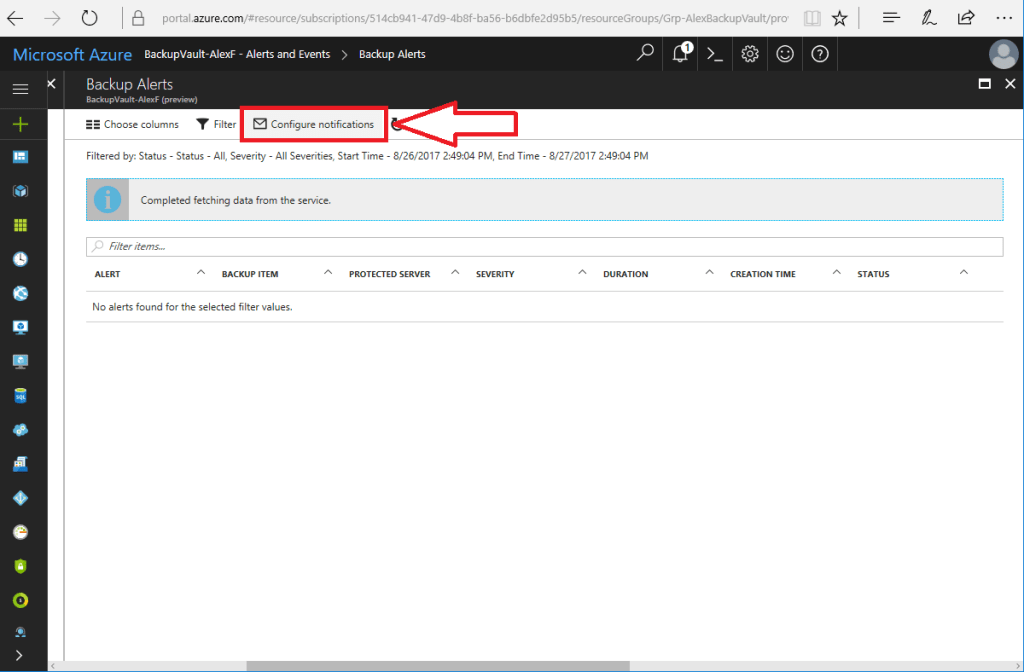


5. Setup Notifications

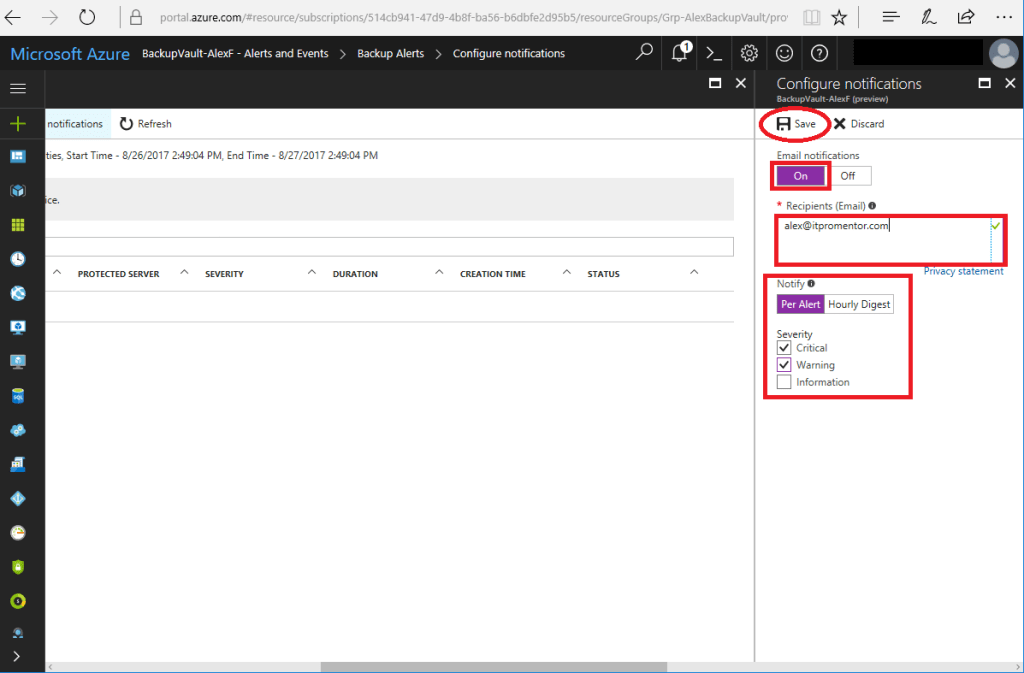
You might want to setup notifications on your backup jobs. Return to your Azure Recovery Vault in the Azure Portal. Scroll down to find **Alerts and Events**. Then click on **Backup Alerts**.



On this next page, just click **Configure Notifications**.



Now pick the settings appropriate to your need, and **Save** at the top.



All done. See below for an example of a notification alert which I have received on this backup agent.

