Day 2 - Create an Azure VM

Overview

The Nautilus DevOps team is planning to migrate a portion of their infrastructure to the Azure cloud incrementally. As part of this migration, you are tasked with creating an Azure Virtual Machine (VM).

The requirements are:

1. Use the existing resource group.
2. The VM name must be `devops-vm`, it should be in `West US` region.
3. Use the `Ubuntu 22.04 LTS` image for the VM.
4. The VM size must be `Standard_B1s`.
5. Attach a default Network Security Group (NSG) that allows inbound SSH (port 22).
6. Attach a 30 GB storage disk of type `Standard HDD`.
7. The rest of the configurations should remain as default.

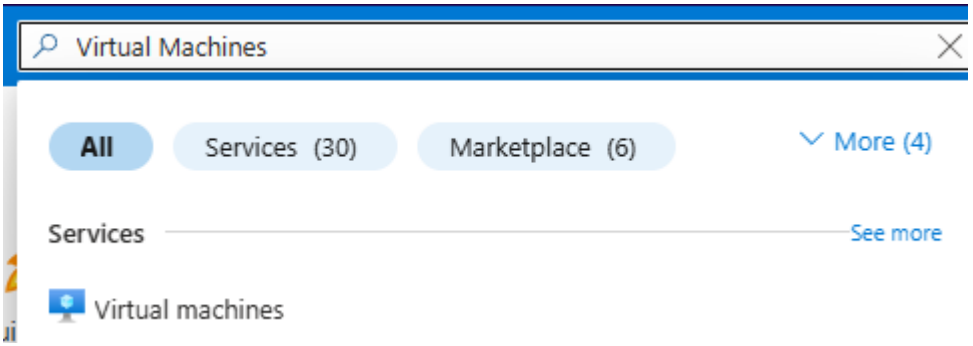
After completing these steps, make sure you can SSH into the virtual machine.

What is an Azure VM

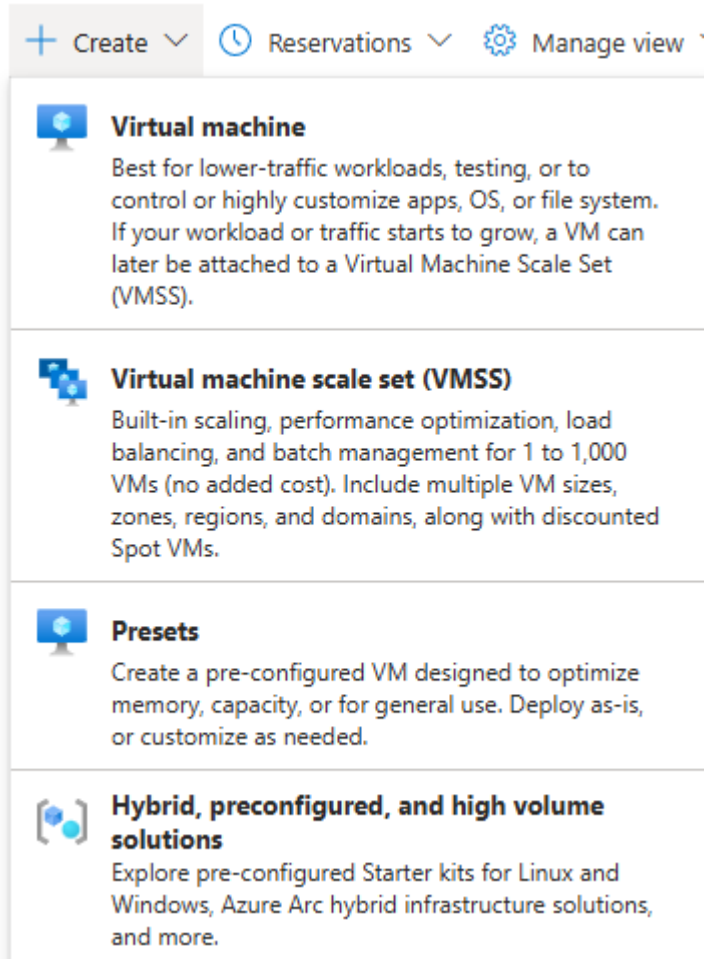
An Azure Virtual Machine (VM) is a computer running in Microsoft's cloud service that you can access and control remotely over the internet, without needing to own or maintain the physical hardware.

Solution

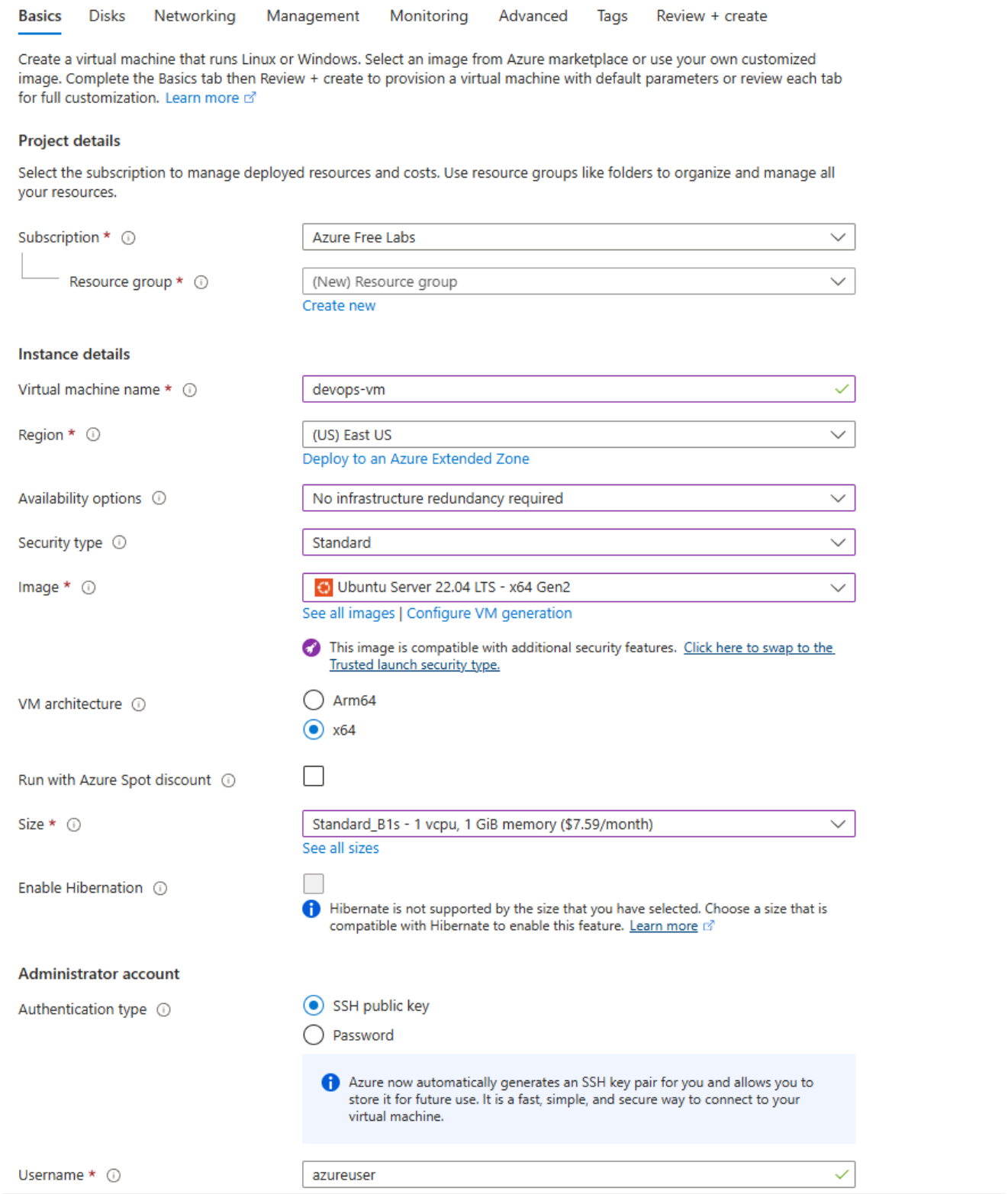
First we search for Virtual Machines at the top

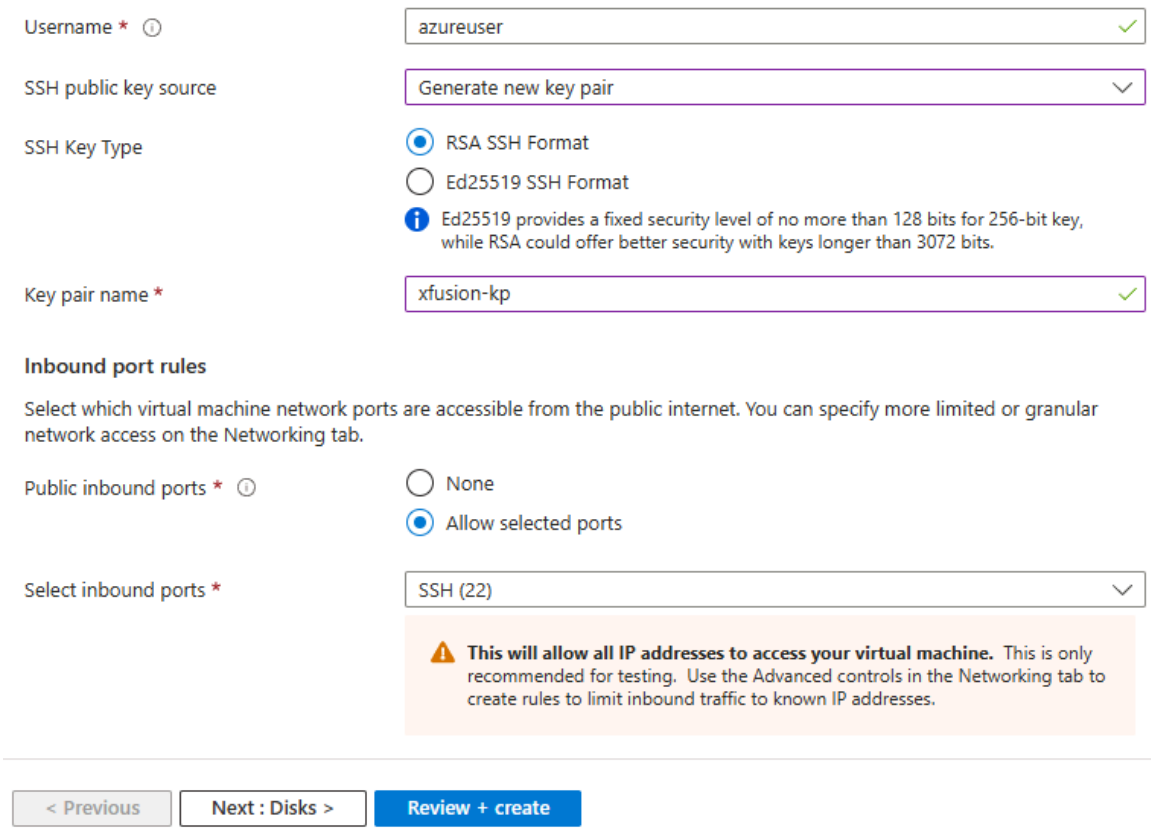


Now we create a new Virtual machine from the drop down

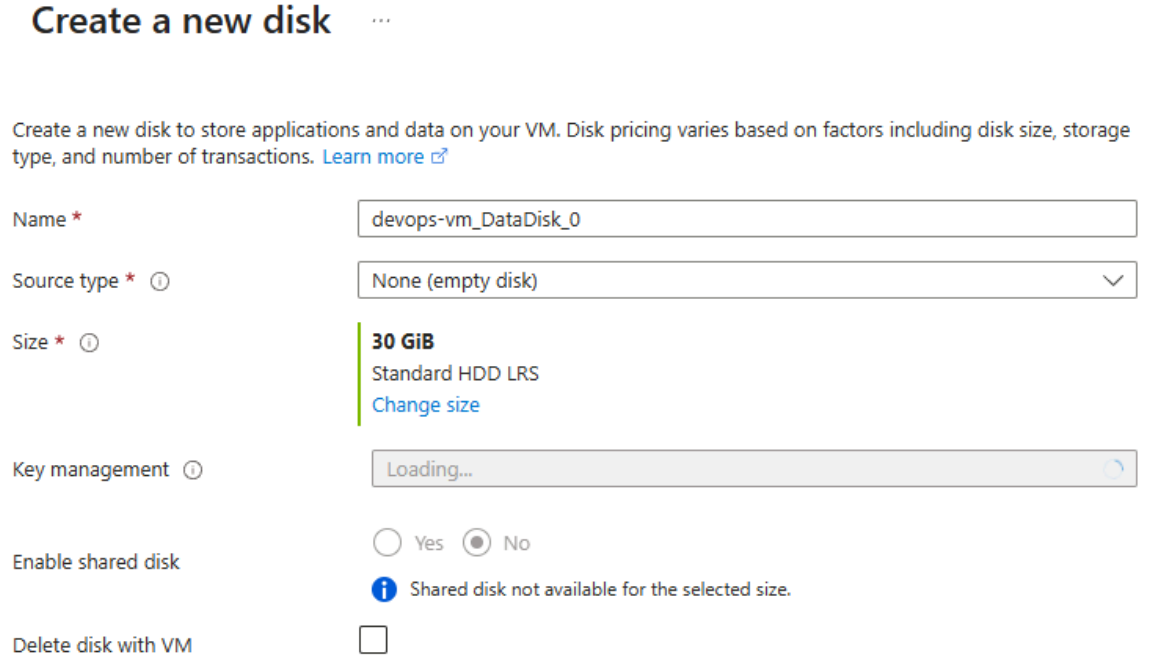


After we fill out all the relevant information in the fields



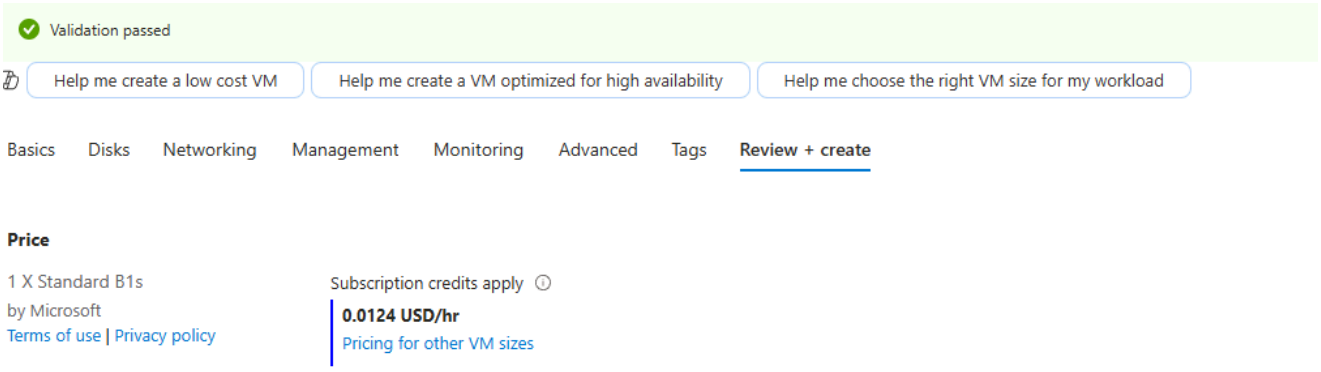


Now we head to disks and change the OS disk type to `Standard HDD`. Then create and attach a new disk

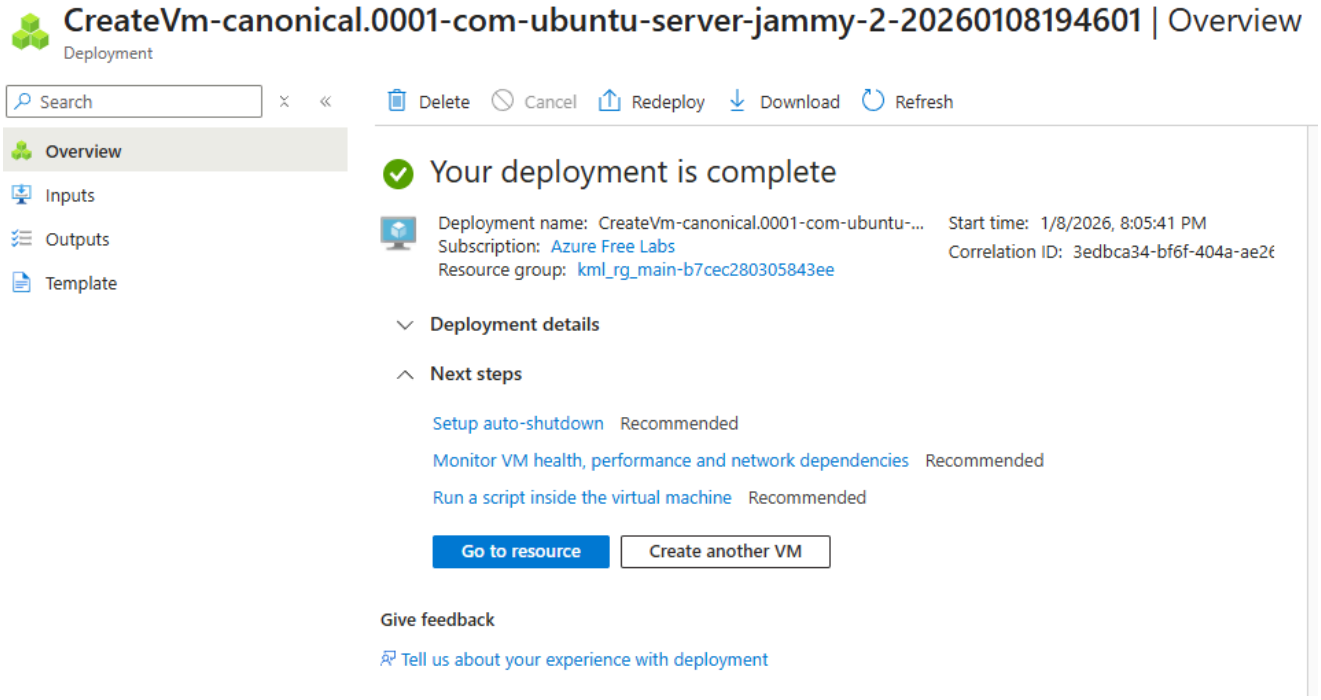


Now we can review and create once the disk has been attached, which we get a validation passed message which shows everything is setup correctly and now we fully

create the VM



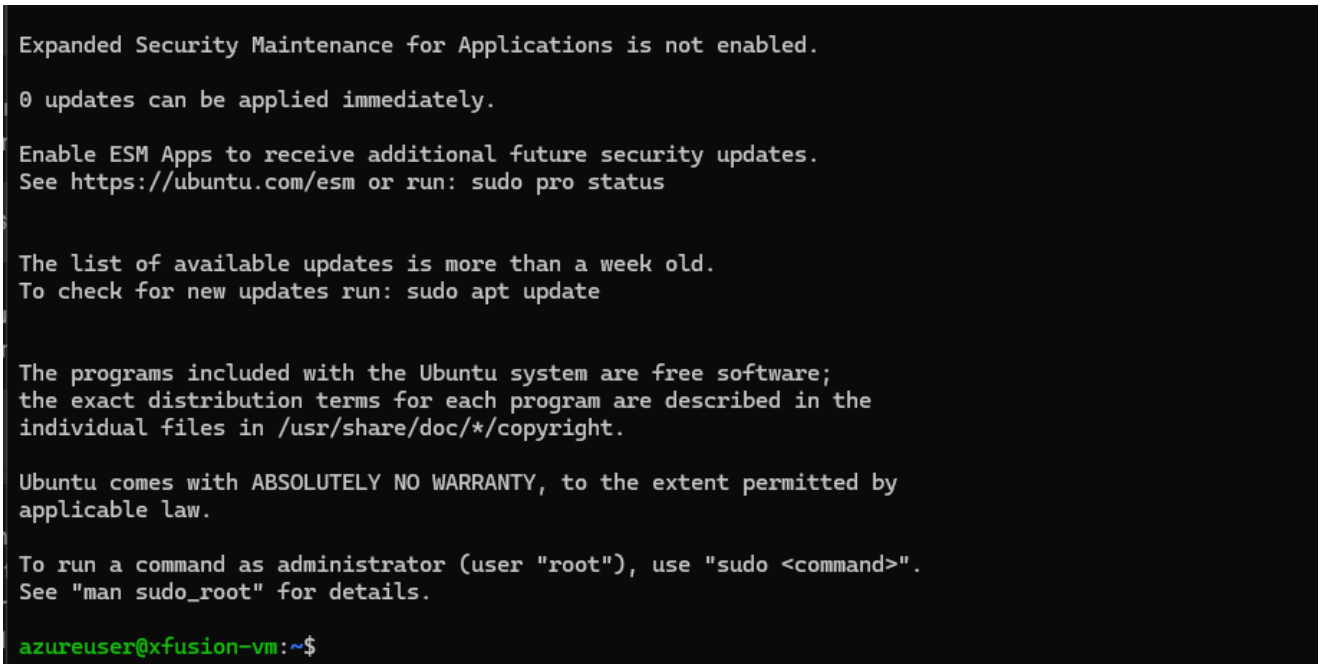
It can take a 1-2 minutes for the VM to be deployed whilst it goes through checks. Once it has gone through all the checks the VM will fully be deployed and running.



Now we can try SSH into the account using the key we downloaded when creating the VM:

```
ssh -i <keyname> azureuser@IP
```

It seems we are able to SSH into the machine with our key (my VM name is different here as I had to recreate another one due to an issue with the lab)



Security Best Practices

- **Restrict SSH access to specific IP addresses only**: Limit SSH (port 22) to your organization's IP range instead of allowing access from anywhere
- **Use SSH keys instead of passwords**: SSH key authentication is significantly more secure and resistant to brute-force attacks
- **Disable password authentication** in SSH configuration after confirming key-based access works
- **Implement role-based access control (RBAC)**: Grant users only the minimum permissions needed to perform their tasks
- **Enable Azure Disk Encryption**: Encrypt both OS and data disks to protect data at rest
- **Configure Azure Backup**: Set up automated backups for disaster recovery