TD SYNNEX

Veeam Backup & Replication Click to Run™ Solution for AWS

The information below includes detailed pre-deployment requirements, an in-depth step by step guide for the AWS Veeam Backup and Replication v11 Click to Run deployment, and post deployment steps that will need to be considered. This guide will outline the overall design, and scope, and technical build requirements

AWS Veeam B&R V11 Pre-Requisites

✓ Infrastructure Requirements

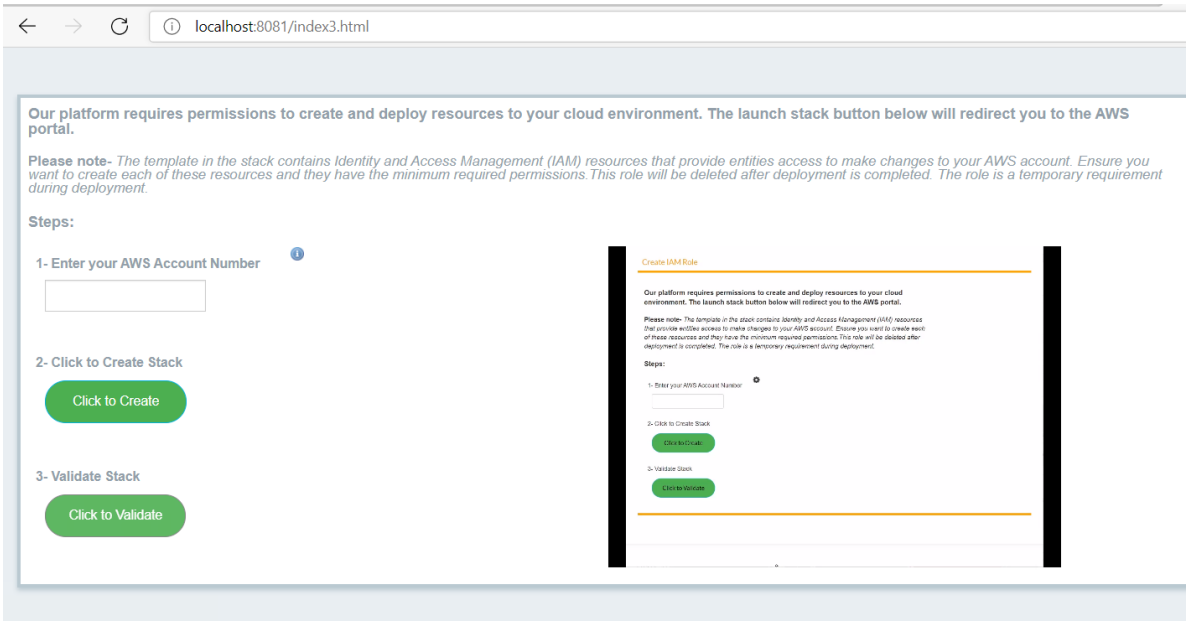
• Existing VPC and Subnet - This is a requirement because EC2 instances are deployed inside Subnets and VPC's. A VPC with associated subnets must already exist in the region, with corresponding route tables, gateways etc. Those resources will be retrieved from the AWS Account and drop downs will allow the user the selection of those resources.

• Existing Key Pair – This is a requirement because at some point the user will have to connect to the newly created VM and to do so a key in a pem format is usually required to decrypt the password for the administration user. A list of existing keys will be shown in a drop down and the user must confirm he can use the one he has selected.

AWS Veeam B&R V11 Pre-Deployment Steps

1. In case the user decides to deploy to an existing VPC (future releases will offer VPC creation) he needs to make sure the VPC is created and has at least one subnet. The user will need to record the ID's or names of those resources.

2. When the user starts the purchasing process, he will be sent to the Role creation page. This creates a temporal permission set that allows resource creation inside his AWS account. The least-privilege concept is applied here, and this role will be deleted automatically after a successful deployment. The user must have his AWS credentials and the MFA device at hand (if two-factor authentication is used). This step is always required.



Once the role is created and validated the deployment can start.

Solution Overview:

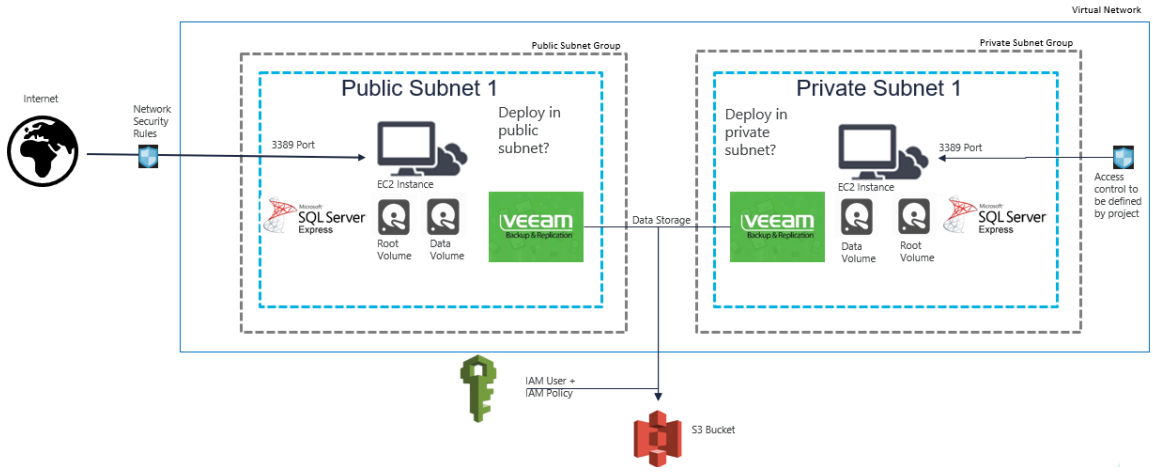
Veeam Backup & Replication is a proprietary backup app developed by Veeam for virtual environments built on VMware vSphere, Nutanix AHV, and Microsoft Hyper-V hypervisors.[3] The software provides backup, restore and replication functionality for virtual machines, fisical servers and workstations, as well as cloud-based workload.[4]

Parameters & Inputs (a more detailed overview is shown on the next pages):

- Select a Region to deploy to.
- Input a name for your EC2 instance.
- Select your Operating System.
- Create a password for the local user in the EC2 instance.
- Create an S3 bucket for Veeam Data storage.
- Select a Key Pair for connecting to the VM.
- Use an existing IAM user or create a new one for connectivity between EC2 and S3.
- Select the size of your instance.
- Select your root volume and data volume sizes.
- Enable/disable and configure Remote Access to the VM.
- Select the VPC in which the VM will be placed.
- Select the Subnet in which the VM will be placed.

Deployment Architecture:

Architecture Design Veeam B&R V11

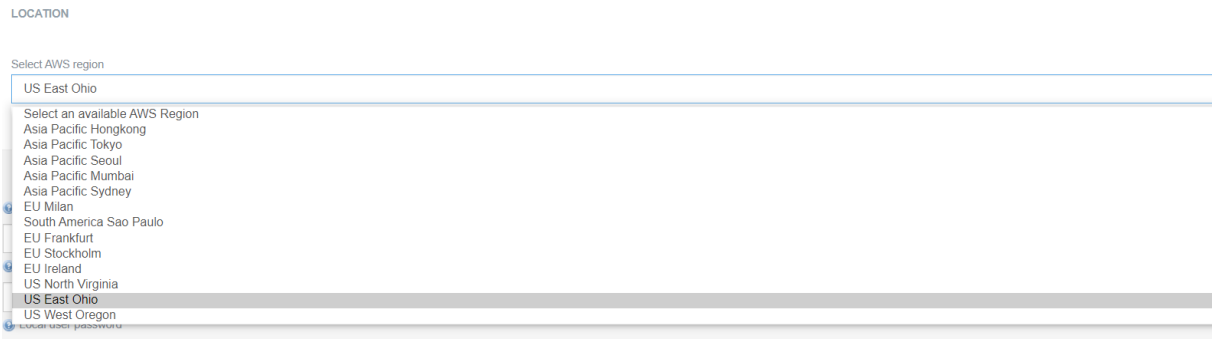


AWS Veeam B&R V11 Click to Run Deployment

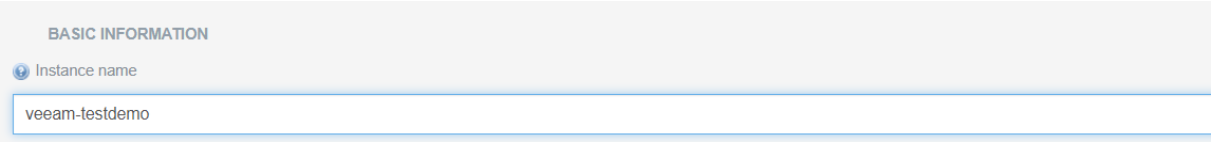
AWS RDS v2 Deployment and Considerations

Purchase the AWS Veeam Backup and Replication V11 Click to Run Solution through StreamOne Marketplace and proceed to the Digital Locker to configure and deploy the solution.

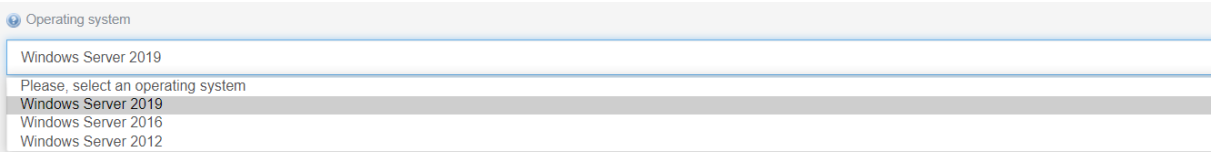
1. Select an available AWS Region: This is the region where the solution will be deployed. Some regions need to be enabled first on the target account before deploying to them, a warning message will appear in such case.



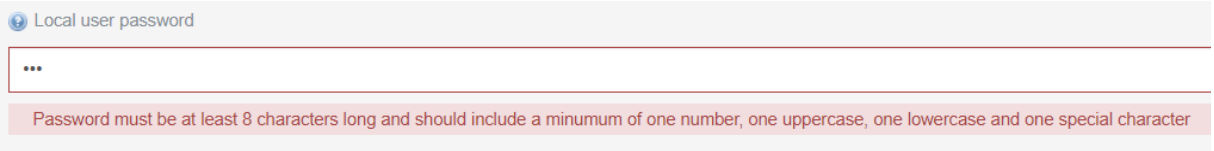
2. Select the name for the created VM: This is the name that will be shown in your AWS Console, it does not alter the host name of the VM.



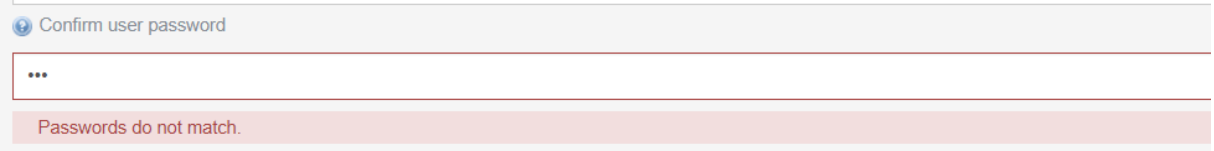
3. Select the Operating System: Currently only Windows VM's are supported.



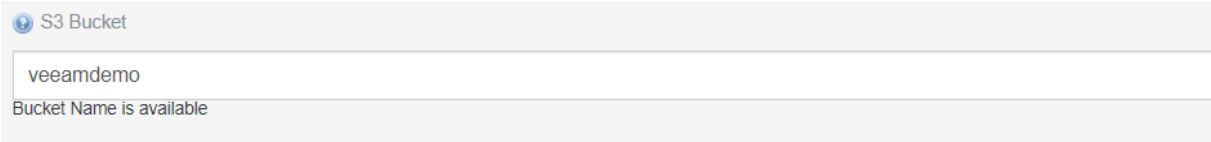
4. Select a Password for the local user: In order for the installation process to succeed a local user with admin privileges is required. The "Administrator" user cannot be used in this case because it is not possible to obtain the password generated by AWS in a programmatic matter therefore a new "veeam" user will be created inside the new Virtual Machine with the password provided in the interface. Please note that standard Windows OS password restrictions apply here.



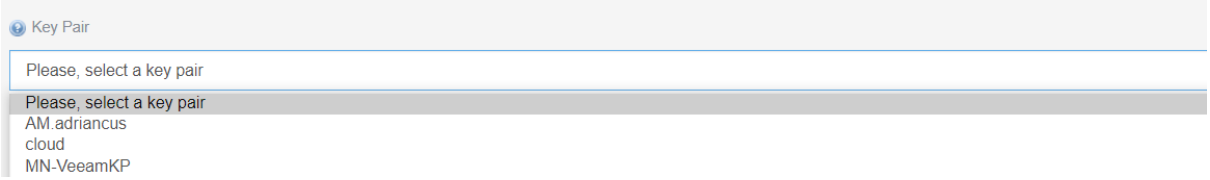
5. Confirm the Password.

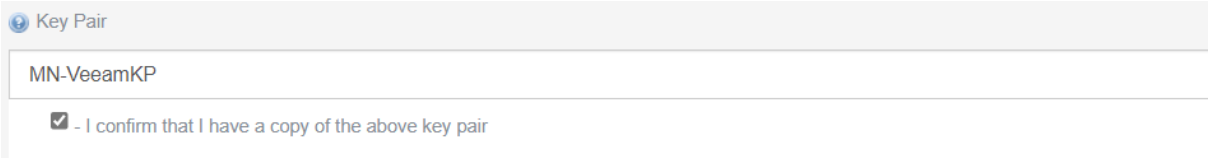


6. Select a name for the S3 Bucket: Live validations will check if the bucket already exists.

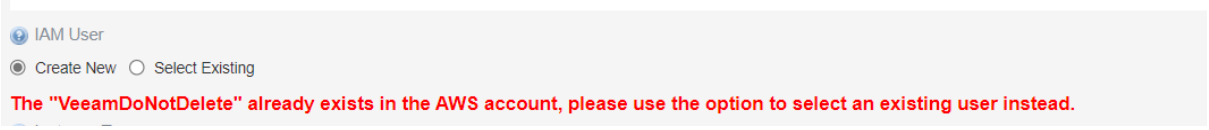


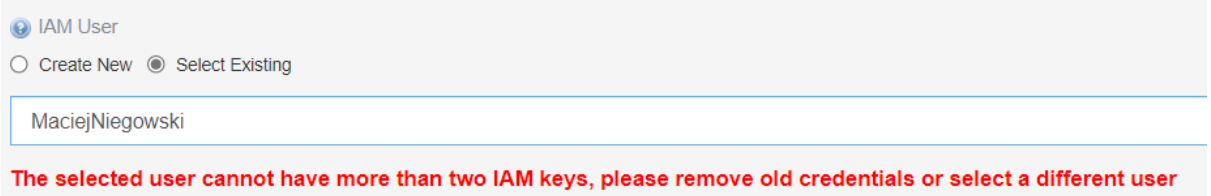
7. Select Key pair for Remote Desktop Connection: You will need to confirm you can use this key to connect.



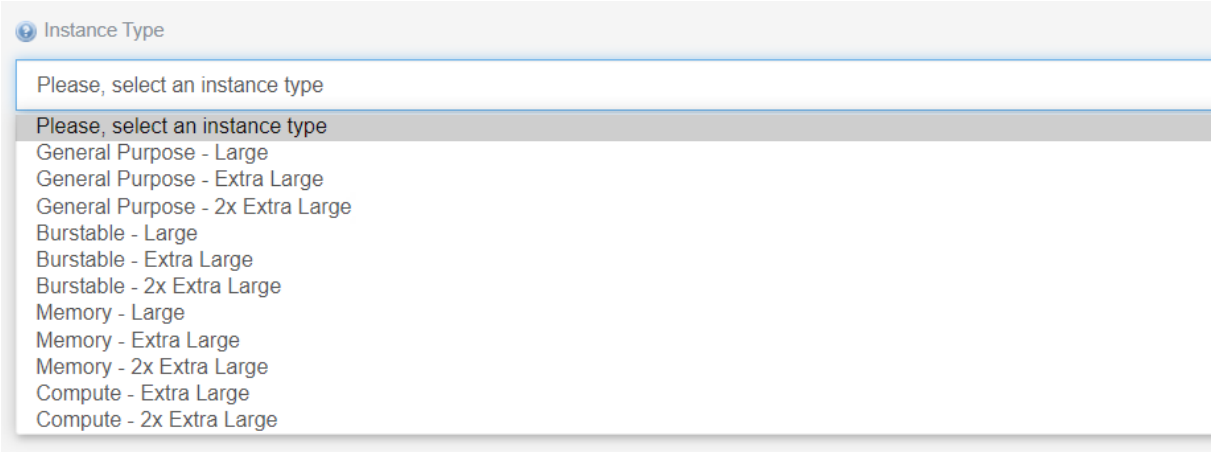


8. Select the IAM user: The user that will be used for programmatic access of the communication between EC2 and S3. There is an option to create a new user but if the username “VeeamDoNot Delete” already exists in the account it must be selected as an existing user. An existing user cannot have two or more security credential sets already created.

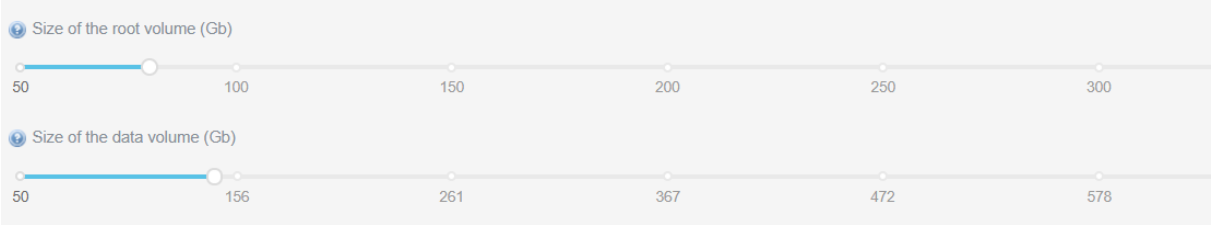




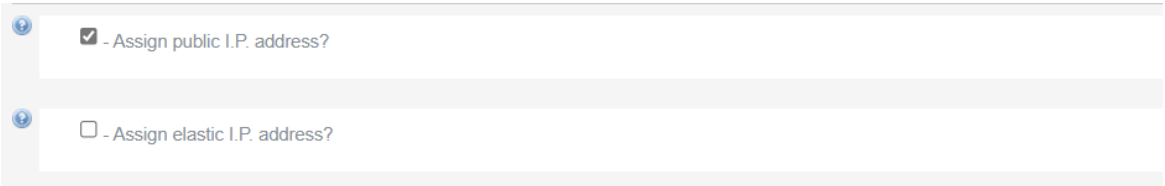
9. Select Instance Size Please choose the best price to performance ratio that interests you



10. Select the size of your Root and Data volumes.

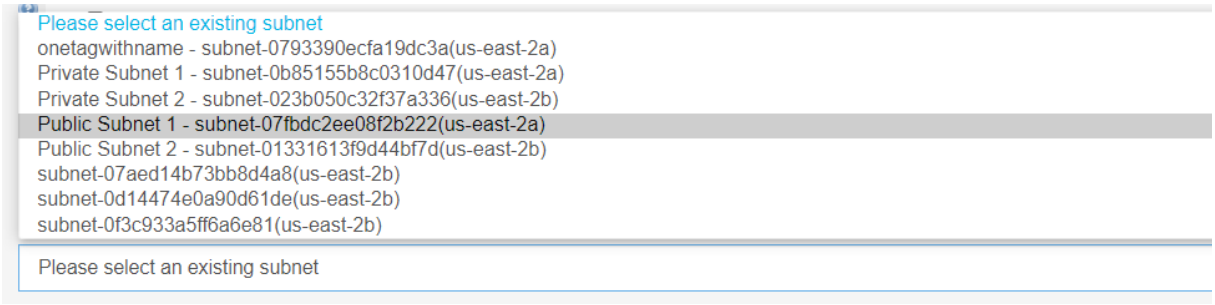


11. Select if a public IP is required When selecting an elastic IP, a quota check will be performed.

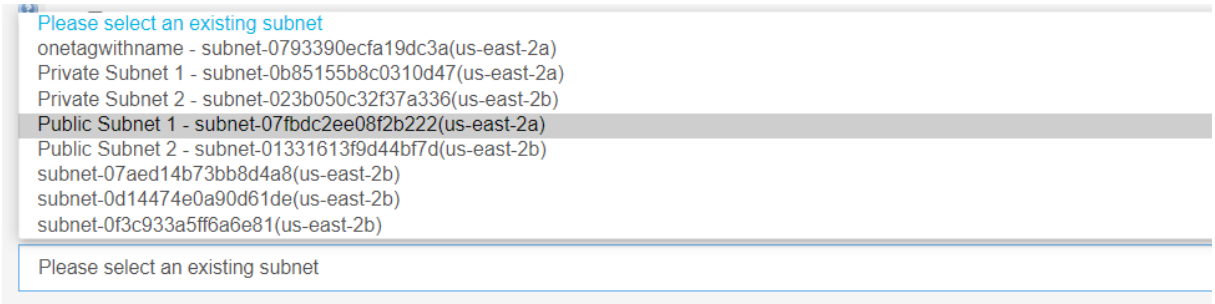


---------- Continue to next page ----------

12. Select the VPC Every EC2 requires a VPC to be placed in, if no custom VPC's are in the selected region you can select the default one



13. Choose a Subnet from the Selected VPC.



---------- Proceed to the next page to for post-deployment steps ----------

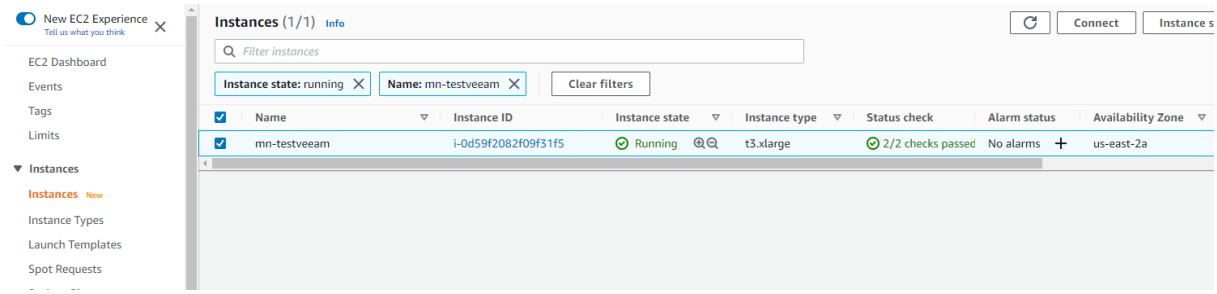
Post-Deployment activities for AWS Veeam B&R V11:

- Verifying the state of your instance.
- Connecting to your VM.
- Verifying the state of the installation.
- License installation screen.

Post Deployment Activities

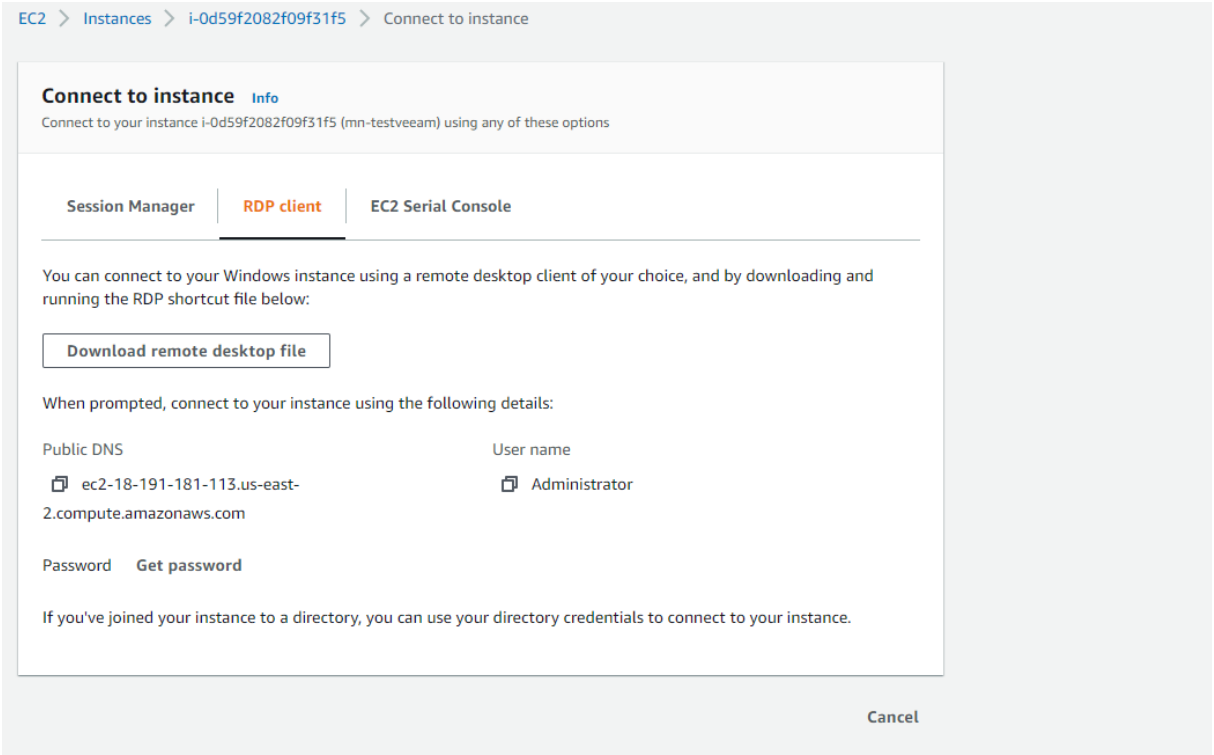
- Verifying the state of your instance.

When the instance is first deployed, its state will change to “running” after some minutes. If the instance doesn’t start there might have been a problem during startup, so either check the deployment logs or contact our support. To verify the state, go to your AWS console. Once logged in, select the service “EC2”. Go to “Instances”. Your instance should appear there, with the name you selected as “Instance Name”. The state will be displayed in the “status” column.



Connecting to your VM.

You will need to connect to your VM to finish the installation. To do so you need to decrypt the password using the keypair selected in the UI. To do so select the “Connect” button in the EC2 panel, and select the “RDP Client” option.

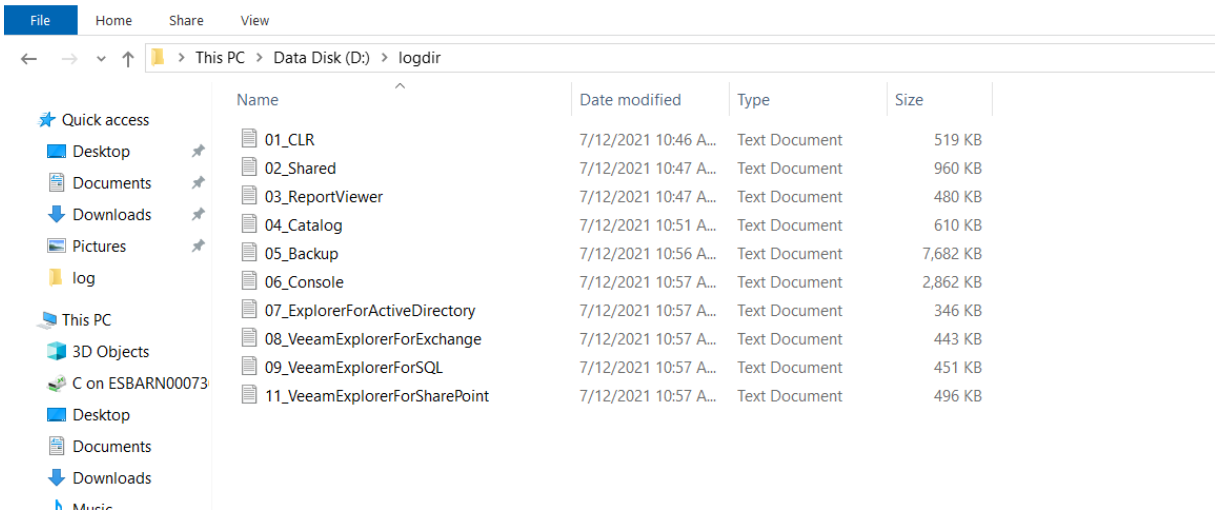


In the “Get password” field you need to provide your key to decrypt the password, once this is done paste the DNS, “Administrator” user and the password into your Remote Desktop client.

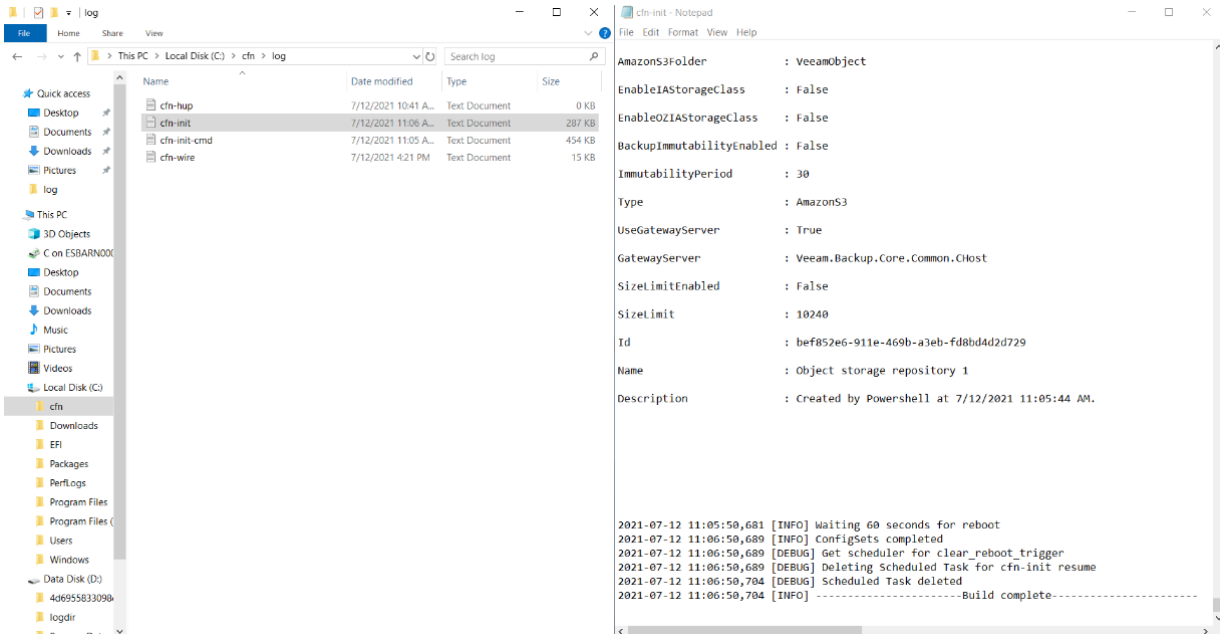
Verifying the state of the installation

Once you can establish a Remote Desktop session to your VM you may want to check if the installation was successful. Those steps are optional. There are several places where you can look:

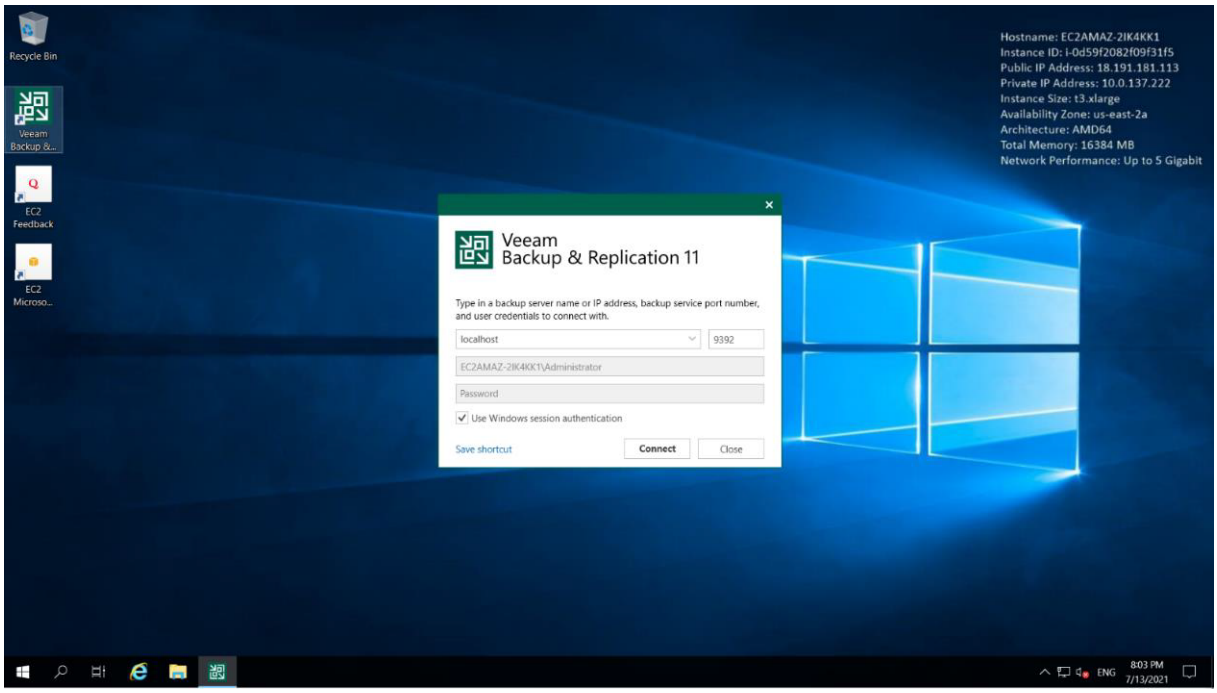
- On the data disk in the log directory D:\logdir there should be 11 files



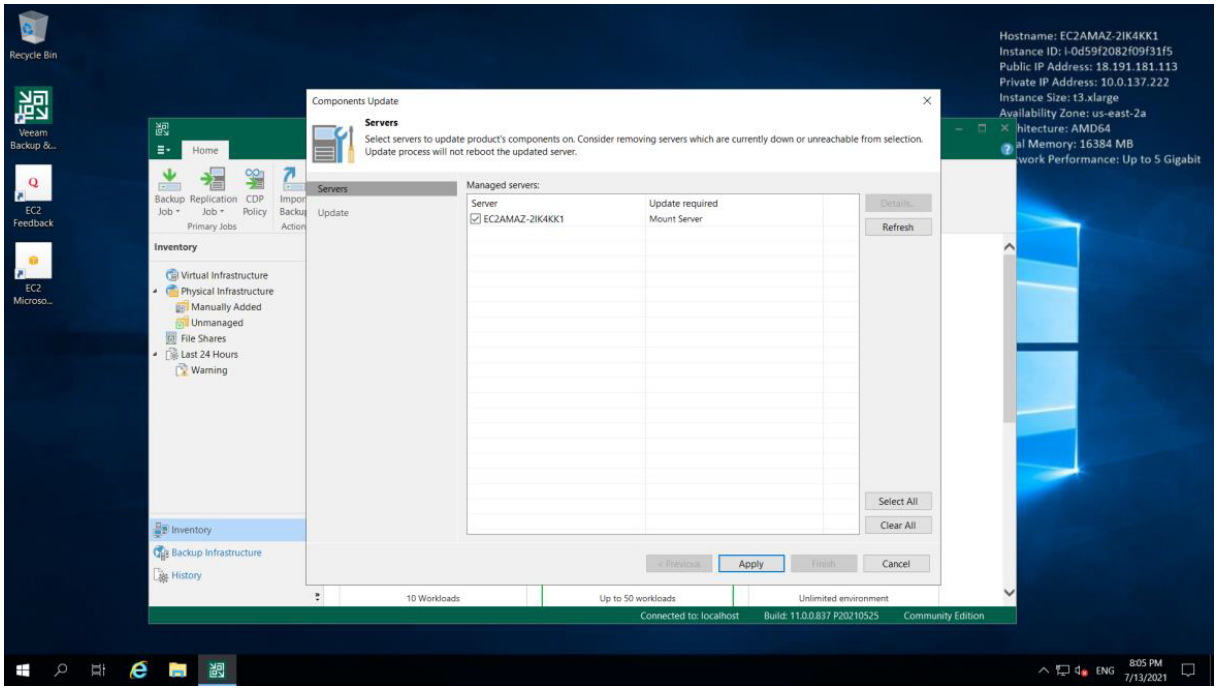
The bootstrap log should have all steps confirmed, and the last one should indicate the S3 bucket has been configured in C:\cfn\log\cfn-init.txt



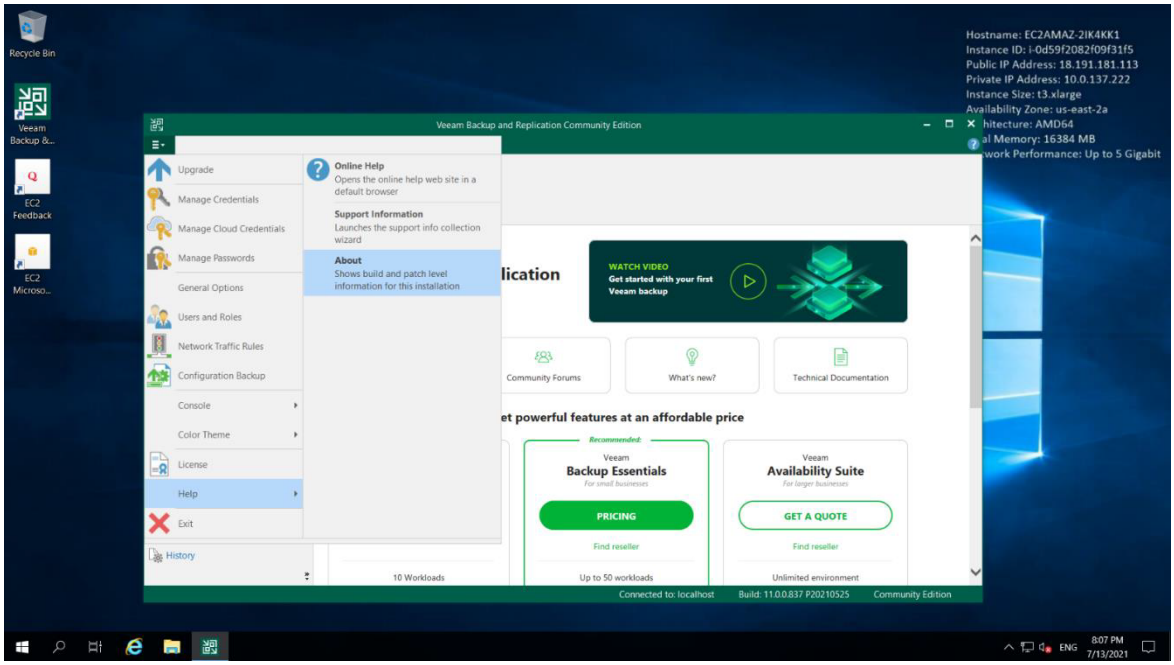
Launch the Veeam Console and connect to localhost

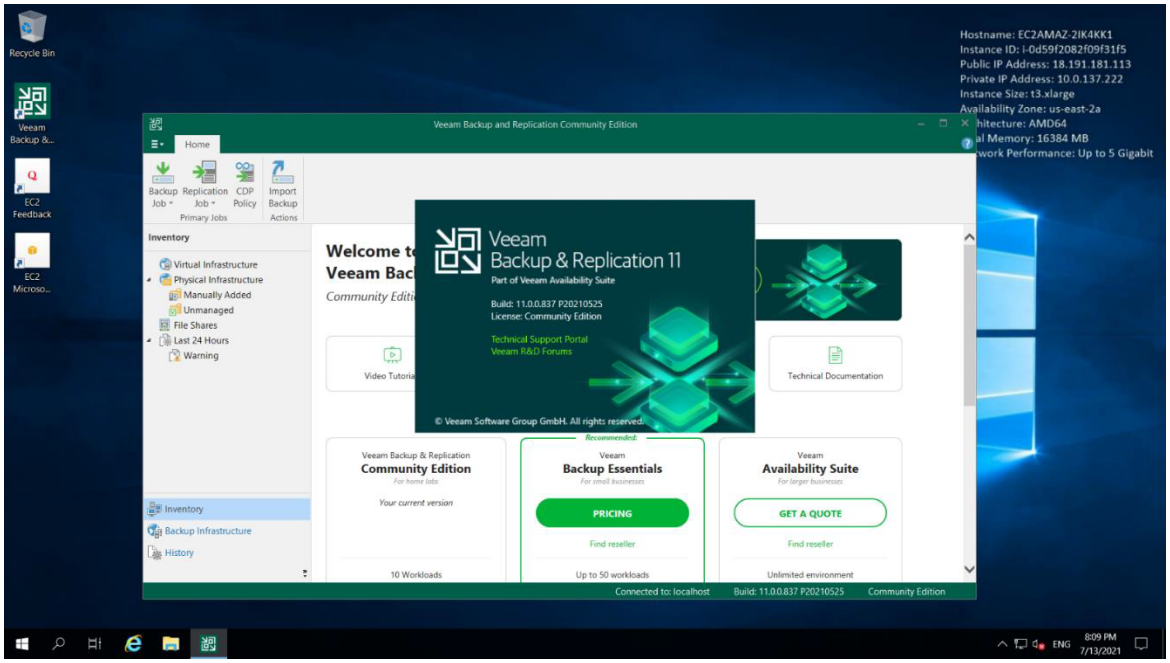


It should ask you to update some components

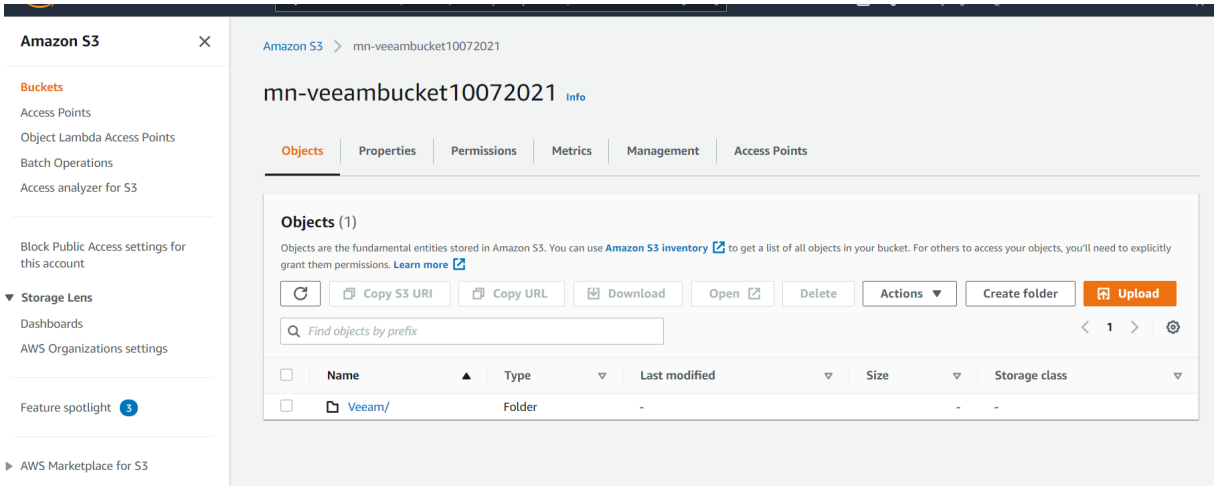


The “About” page should indicate version 11.0.0.837 P20210525





Review the S3 bucket has a “Veeam/” folder in the AWS Console



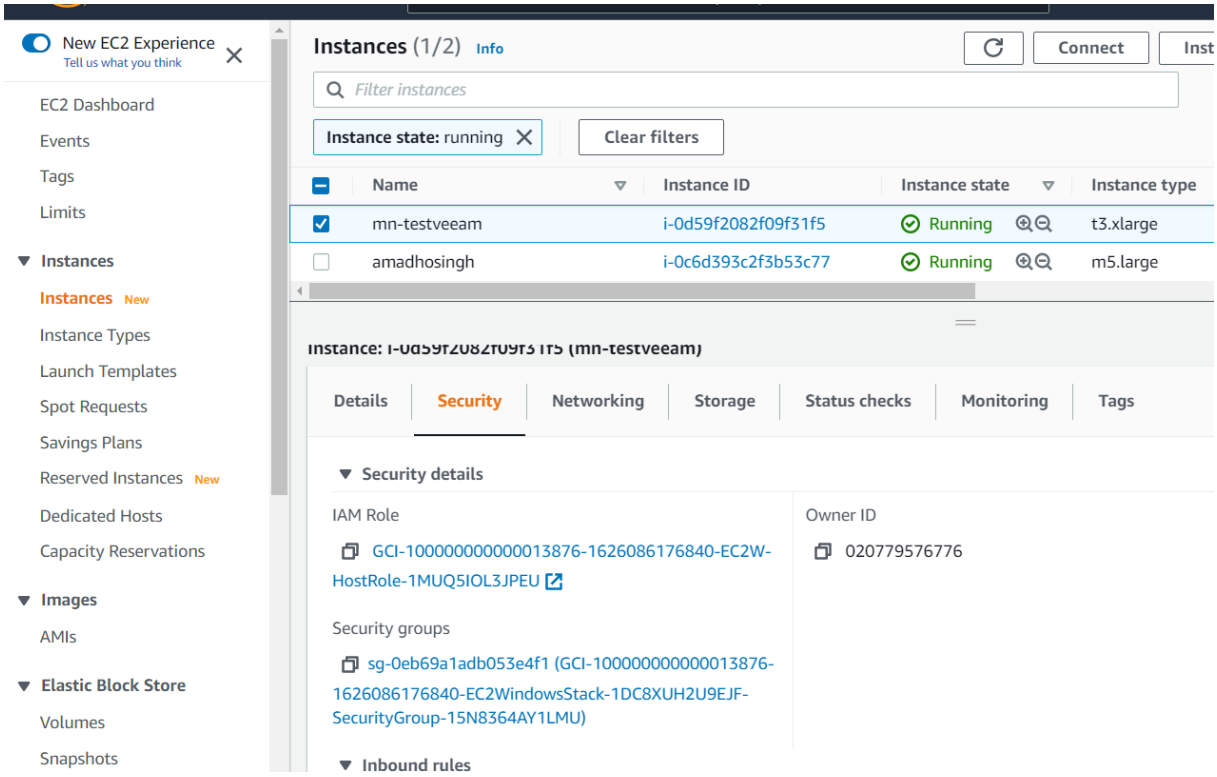
Modifying network access permissions

It is possible that the basic permissions issued at instance deployment will need to be modified later as demands change, source IP changes, or it could be that a mistake was made and the proper CIDR block was entered incorrectly. To modify the network access permissions, follow these steps:

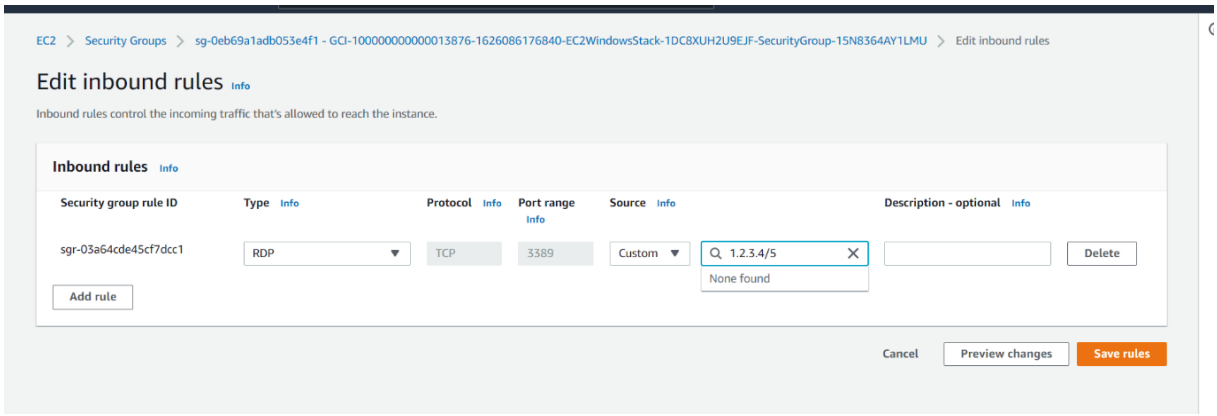
1. Connect to your AWS console. Select the service “EC2” and “Instances”.

2. Go to the “Security” tab of the selected VM.

3. Select the Security Group attached to your instance:



4. Edit the inbound rules:



License installation screen.

• Last step is to select the license and start using the solution.