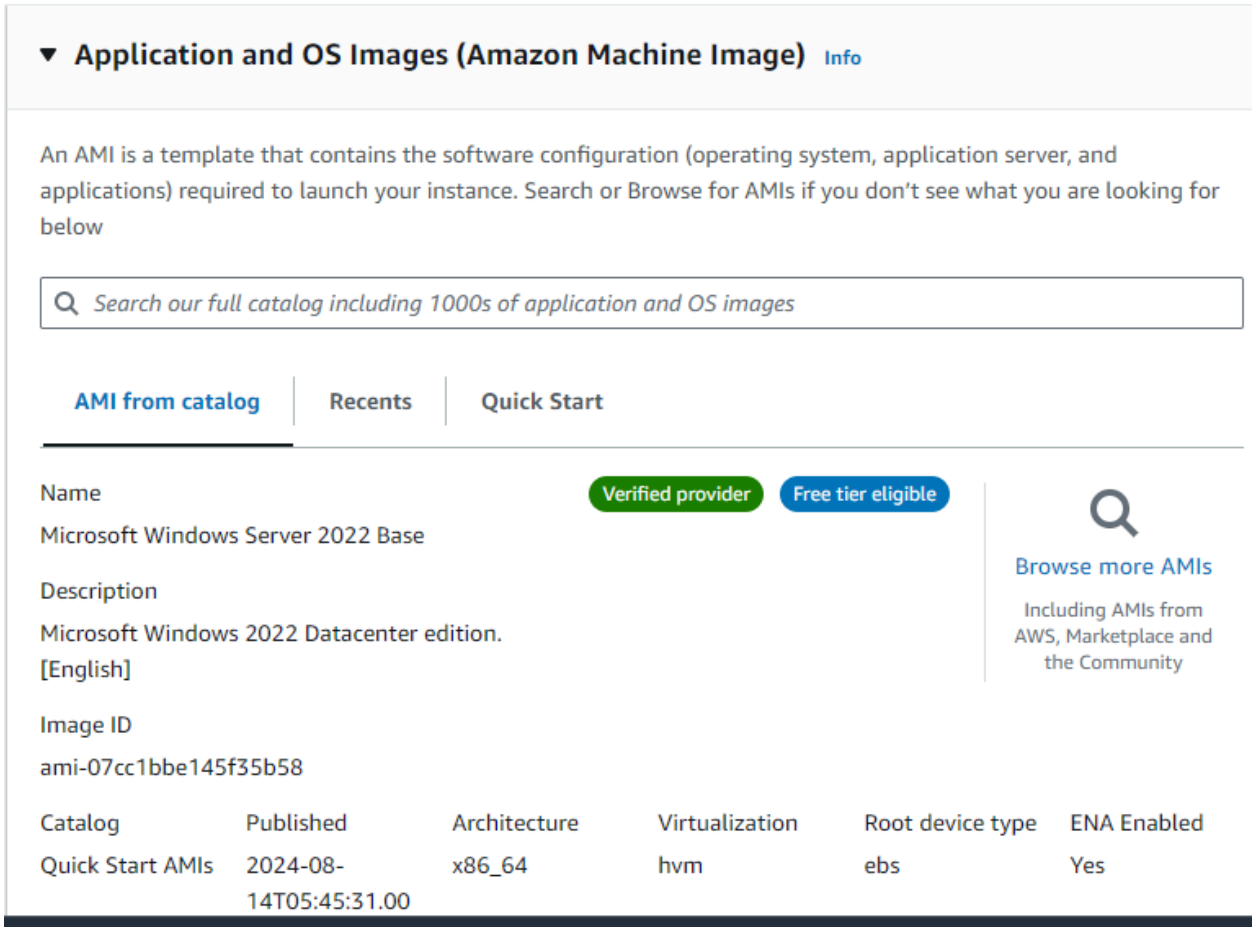
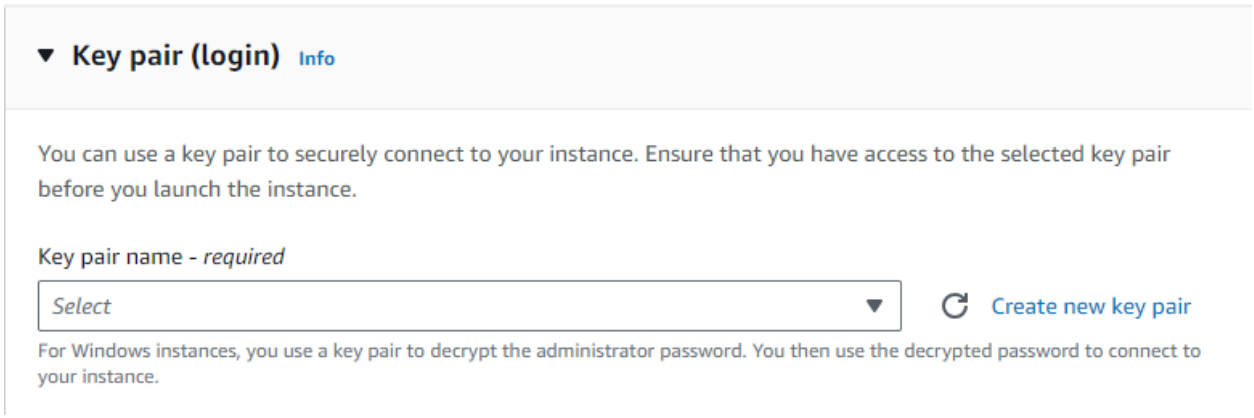
EC2 Instances

As a Cloud Architect and Consultant for Advanced Accounting LLC., I have been discussing steps for migrating to the cloud with owner Jessica Smith. We have decided on a measured, methodical migration process. While the company is eager to begin using and learning about their cloud infrastructure, we have chosen to start with spinning up Compute instances for each employee to use. Although it is a simple start to establishing a cloud infrastructure, it allows us to set proper inbound and outbound rules for security groups, and set network access controls for a solid security framework.

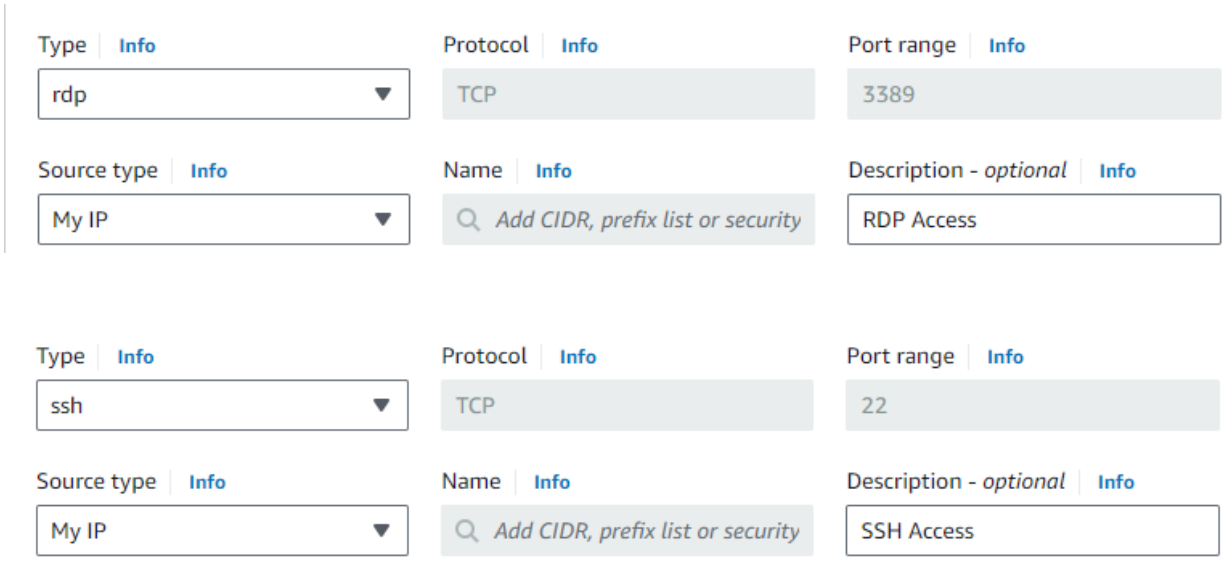
Although this is a project with real world scenarios and use cases, I still need to use the free tier to demonstrate the project. Because the employees are familiar with Microsoft Windows, we chose Windows Server 2022, as our machine image which is the underlying operating system used on the Compute instance to run any programs.



When adding new instances a key pair must be created or an existing key pair may be used. While I did create a key pair, for security reasons the actual key pair is not displayed in the screenshot.

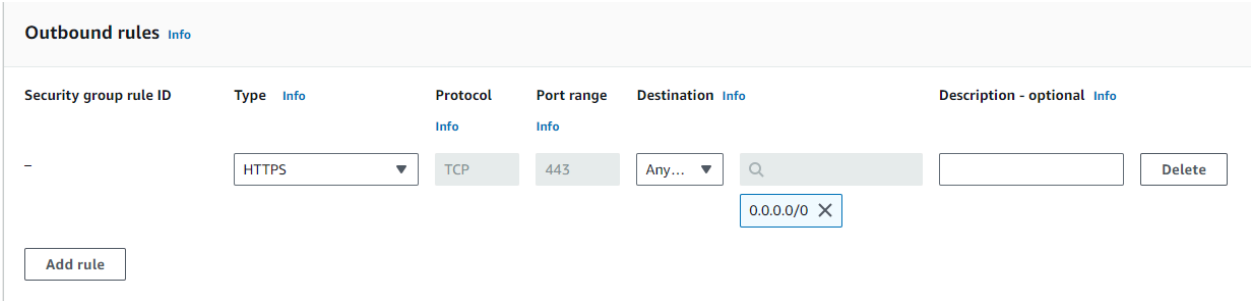


In order to minimize the attack surface of our EC2 instances and help protect against threats like ransomware, we have established inbound rules using AWS security groups to restrict traffic only to RDP and SSH traffic from the local IP addresses. Because the security groups are stateful all other inbound traffic is denied by default. It is also possible to disable SSH and RDP completely and use the Session Manager for instance management.

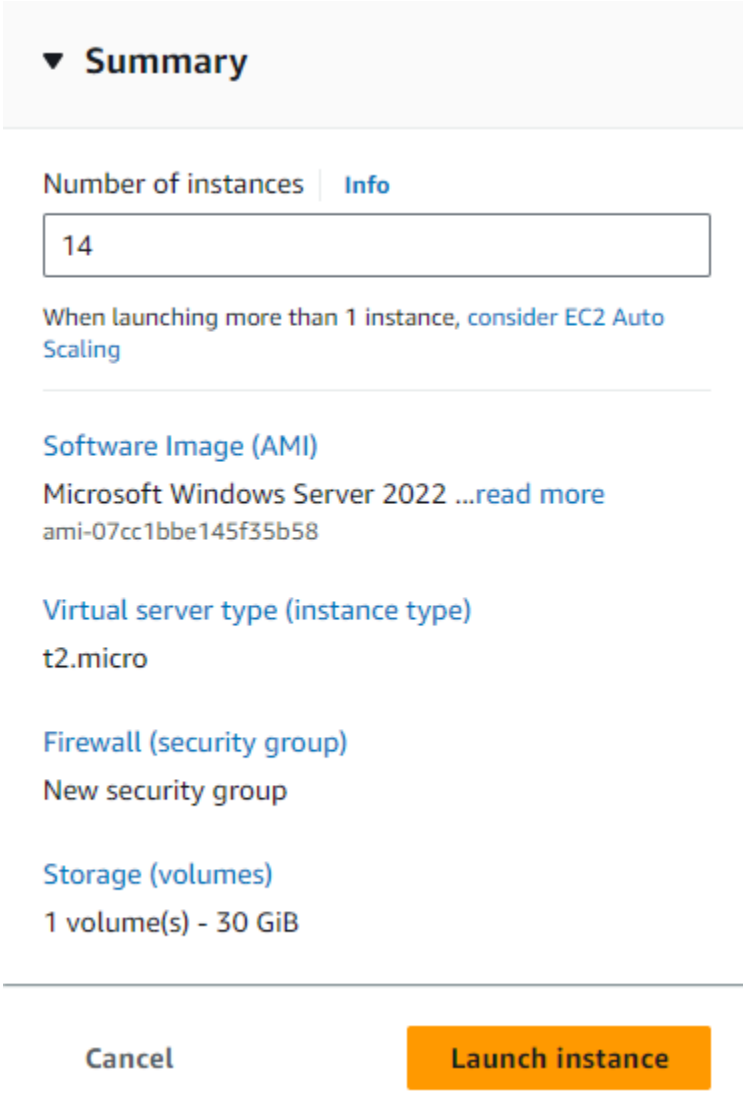


In order to further protect against attacks like ransomware, we will restrict our outbound traffic to necessary traffic on port 443 and disable the default outbound rule that allows all traffic. We will also employ Endpoint Protection to detect and prevent ransomware and will employ data loss protection to prevent data exfiltration. Finally,

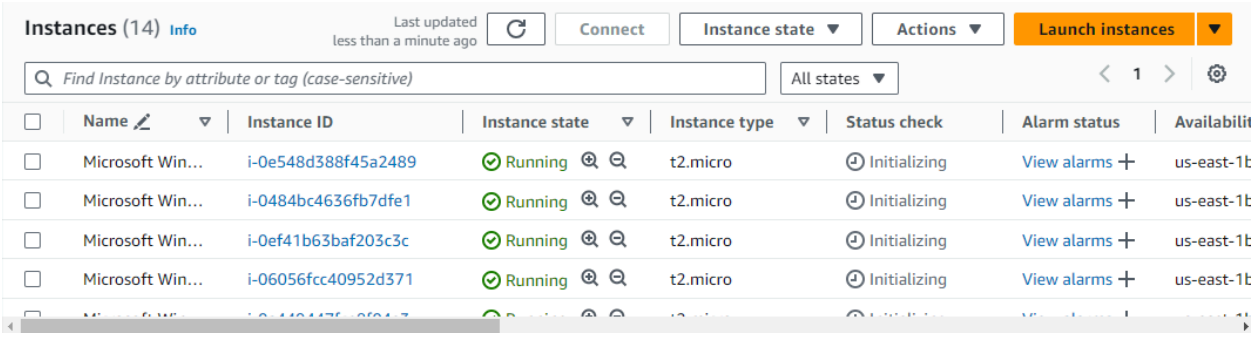
we will use an AWS Web Application Firewall to protect against web exploits that could be used to inject ransomware.



Now that our rules are set we can launch our instances!



Our instances are now up and running!



In my future projects I will create storage including a database and web server for hosting documents and files for use by the company. I will also delve deeper into security policies and frameworks like Identity and Access Management. Stay Tuned!