**CREATE A VIRTUAL MACHINE AND DEPLOY A WEB SERVER**

## SUMMARY

In this project a Nextcloud web server is deployed in a screened subnet using Azure cloud. Project started by creating a virtual network followed by a subnet. Subnet is protected by inbound and outbound rules by using Network Security Groups. An ubuntu server is deployed in a VM within the subnet. For remote administration of the server, Bastion service is used. Bastion allows connection to the VM using SSH without exposing an external port to the internet. Lastly, created a public IP and a DNS Label to access the web server through the public internet. This report also lists top five risks present in the network and remediations for each risk.

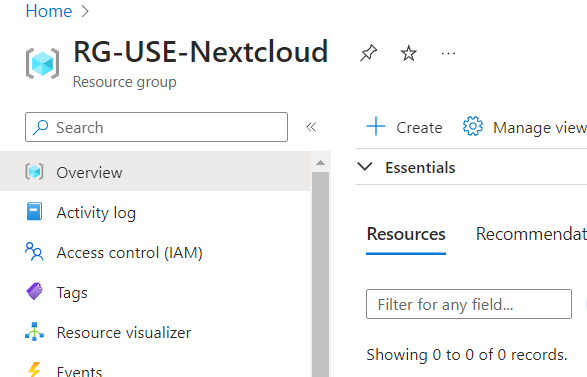
NETWORK DIAGRAM



## NETWORK DESIGN

### RESOURCE GROUP

A resource group is created specifically for this project. This resource group is in the US East data center with High Availability Zone 1. A standard naming convention is used throughout the project i.e. resource name followed by region and the project name. In this case, the resource group is identified as RG-USE-Nextcloud.

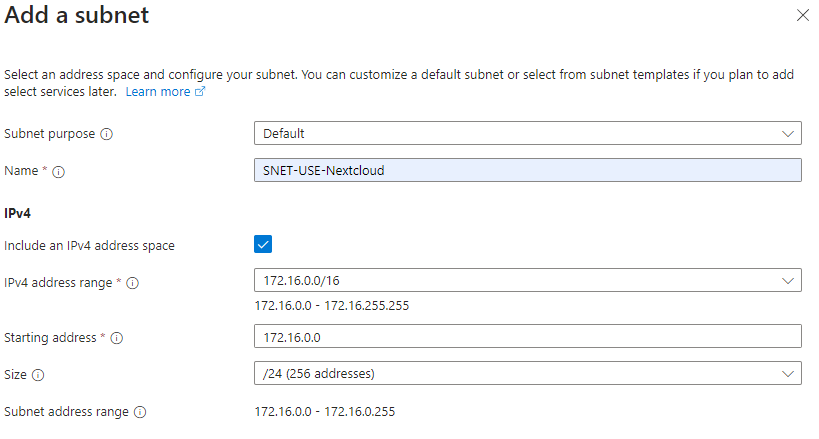


### VIRTUAL NETWORK

Under this resource group a virtual network VNET-USE-Nextcloud is created.

### 

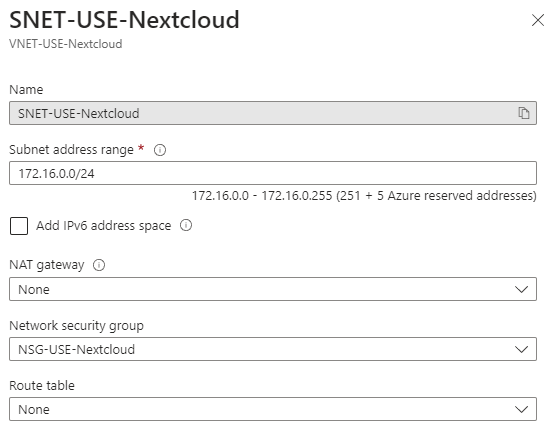
VNET-USE-Nextcloud is configured with 172.16.0.0/16 address space according to RFC 1918. After that, a screened subnet was created where the Nextcloud web server will be deployed. This subnet, SNET-USE-Nextcloud, is configured with an IP address range of 172.16.0.0/24.



### NETWORK SECURITY GROUP

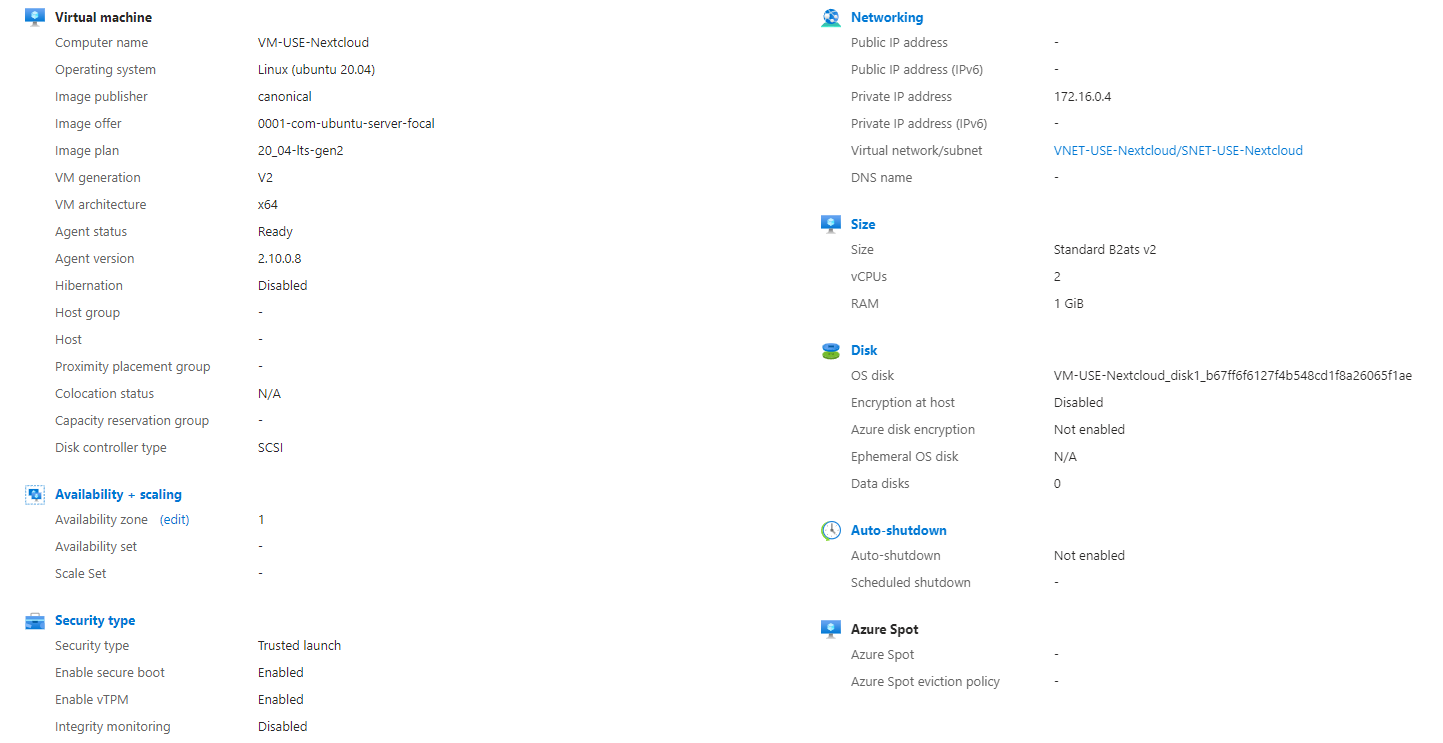
Azure network security group NSG-USE-Nextcloud is created to filter network traffic between Azure resources in an Azure virtual network. This network security group contains security rules that allow or deny traffic inbound or outbound from several resources according to source and destination, port and protocol used by the traffic.

Now that NSG is created, it is added to the subnet SNET-USE-Nextcloud to apply NSG rules.

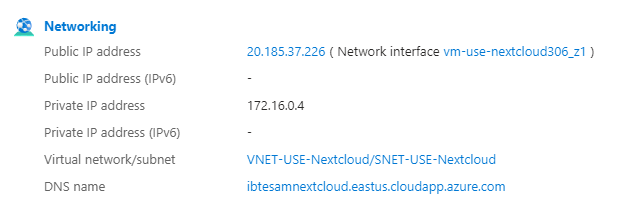


### VM CREATION

Virtual machine VM-USE-Nextcloud is created with Ubuntu Server 20.04 LTS image. Authentication type for this VM is configured to SSH public key. A trusted launch is also configured with secure boot enabled, and also uses a vTPM. This VM is deployed in the virtual network VNET-USE-Nextcloud and within the screened subnet of SNET-USE-Nextcloud. Here is an overview of the VM:

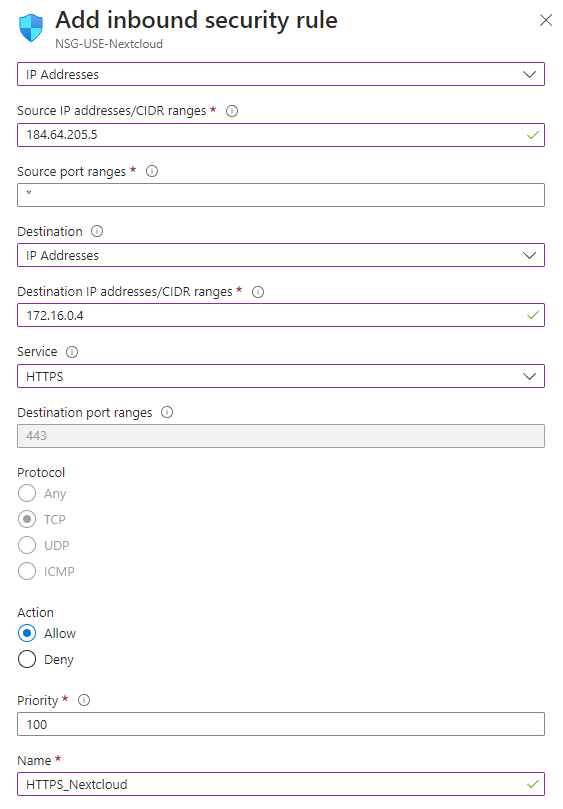


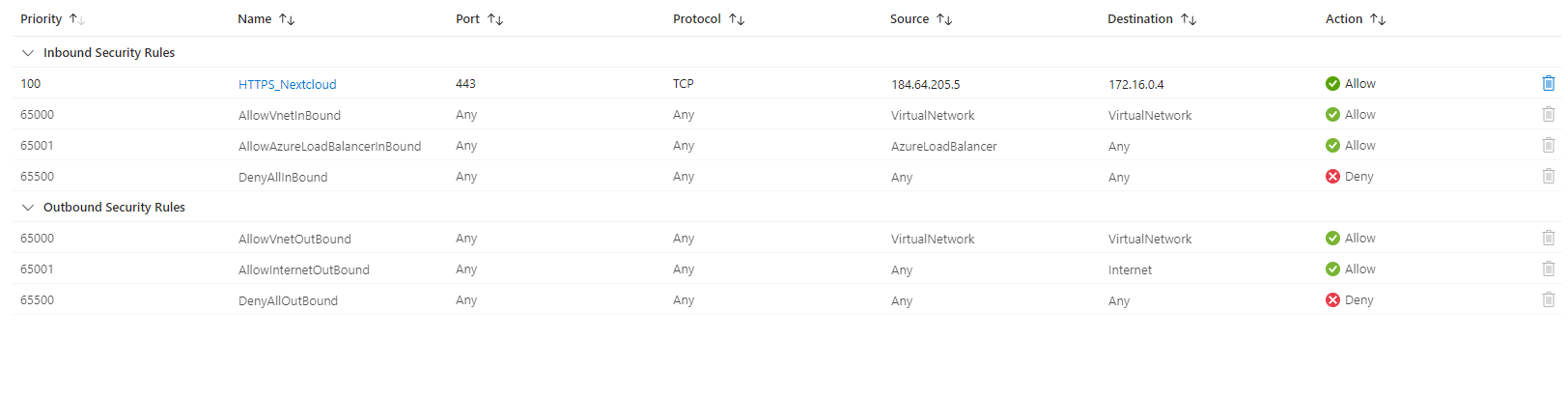
This VM is not able to route through the public internet yet as the public IP is not configured. The NIC is configured to add a public IP address 20.185.37.226 for the web server VM. Also, a DNS label, ibtesamnextcloud.eastus.cloudapp.azure.com, is created within Azure.



### ADD NSG FIREWALL RULES

An inbound TCP connection over port 443 is added only from the admin IP address for this project only. This rule will allow web browsers to connect to the web server over SSL/TLS.





### BASTION SUBNET

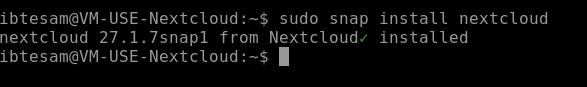
Azure Bastion is a fully managed PaaS that is used to securely connect to virtual machines via private IP address. It will provide secure and seamless SSH connectivity to the VM in the subnet SNET-USE-Nextcloud directly over TLS without exposing the VM to the public internet. Bastion subnet does not require NSG to be



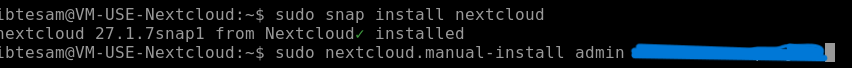
Added as it connects to the VM through a private IP address. And the NSG rules on the SNET-USE-Nextcloud only allows inbound traffic within the virtual network VNET-USE-Nextcloud.

### NEXTCLOUD INSTALLATION AND CONFIGURATION

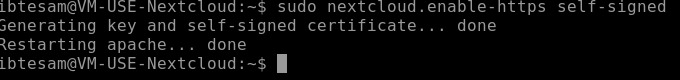
Nextcloud web server is installed with the following command:



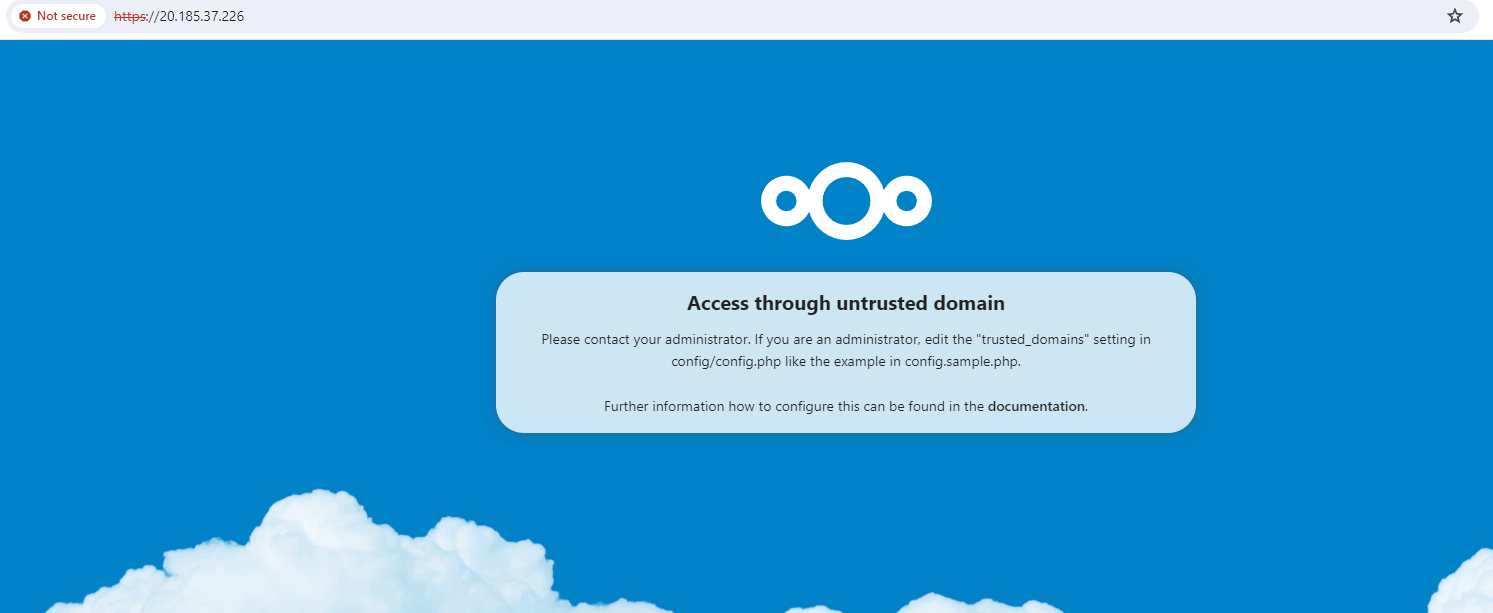
After a successful installation, web server admin is added.



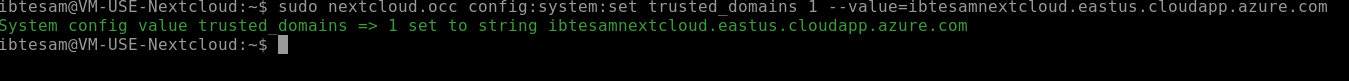
Adding a self-signed SSL/TLS certificate.



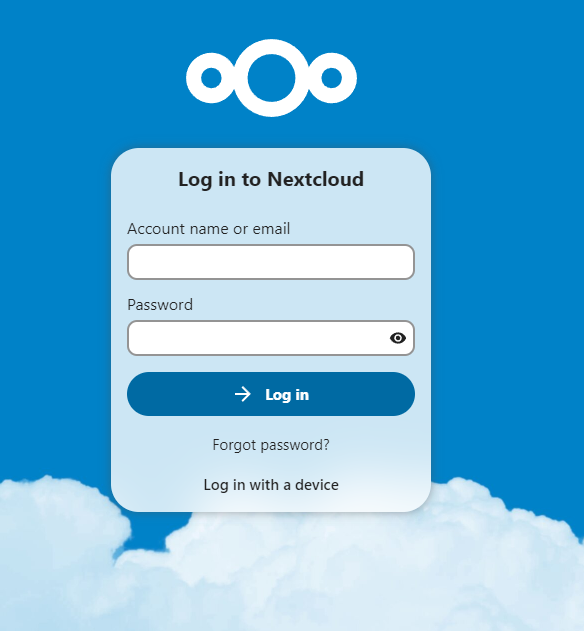
If the web server is accessed without configuring a trusted domain then it will show a nextcloud error: access through an untrusted domain as shown below.



Adding **ibtesamnextcloud.eastus.cloudapp.azure.com** as trusted domain



And after the trusted domain configuration: successful response from the server.



## RISKS AND REMEDIATIONS

1. Web servers in a screened subnet possesses high risk. Vulnerabilities can allow a threat actor to compromise the server and move into the internal network. After installation of the server, a vulnerability scan must be performed to find any existing vulnerabilities and implement controls accordingly.
2. A self signed certificate is used here for a public facing web frontend. This will cause browser certificate error as the user's browser will not recognize our certificates. This will disrupt business operations and can cause significant financial and reputational damage. A commercially available certificate by trusted CA should be implemented.
3. No endpoint security service is installed other than the secure boot and TPM. This makes the web server vulnerable to malware infection. An anti-malware solution needs to be installed.
4. No intrusion detection and prevention capabilities present in the network to identify and block intrusion. A network based IDS/IPS will solve this issue.
5. There is no visibility to the network to understand and analyze network traffic. A Security Information and Event Management (SIEM) tool can provide a clear picture to the network while alerting on any network event.

While it is not possible to identify every risk present in the network, it is important to constantly monitor the network and implement layered controls (defense in depth) to safeguard our infrastructure.

## CONCLUSION

This project successfully deployed an internet facing web server in a screened subnet within a private network. This mimics the real-world enterprise network infrastructure. Administration to the web server is securely done through the company intranet, in this case the AzureBastionSubnet over SSH. Also, the internal network is protected from the screened subnet with Network Security Group. TCP traffic from the public internet is allowed only over encrypted channels into the web server and data at rest is encrypted in the storage of the server.

This project followed best practices to design and creation of virtual networks, subnets, firewall configurations and secure protocols. After the project is done, unused resources are deprovisioned safely. This secure deprovisioning includes removal of Network Interfaces and SSH keys along with any user credentials, firewall rules and DNS label created.