CREATE A VIRTUAL MACHINE AND DEPLOY A WEB SERVER

SUMMARY

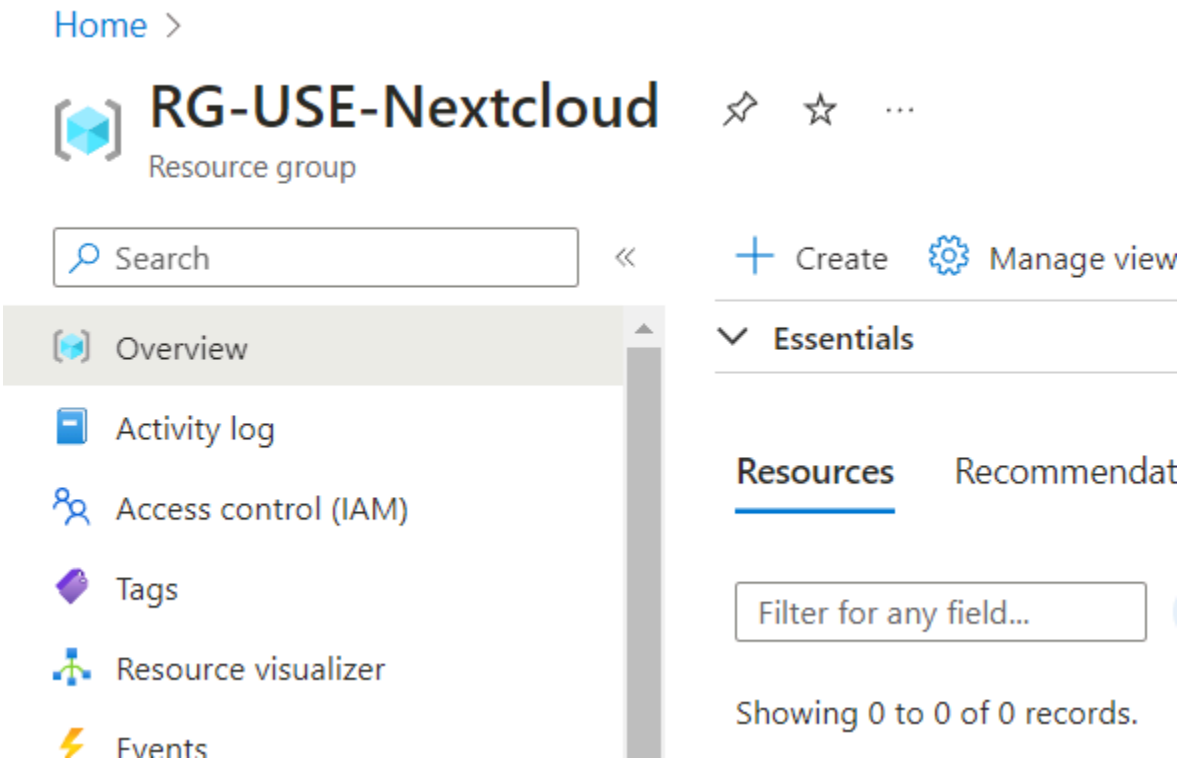
Deployed a Nextcloud web server within an Azure cloud environment, hosted in a screened subnet for enhanced security. The project commenced with the creation of a virtual network and a subnet, both protected by inbound and outbound rules using Network Security Groups. An Ubuntu server was then deployed within the subnet, with remote administration facilitated through the implementation of a Bastion service. Utilizing Bastion allowed secure SSH connections to the VM without exposing external ports to the internet. Furthermore, a public IP and DNS label were configured to enable access to the web server from the public internet. Additionally, the project included a risk assessment, identifying the top five risks in the network along with corresponding remediation strategies.

NETWORK DIAGRAM

NETWORK DESIGN

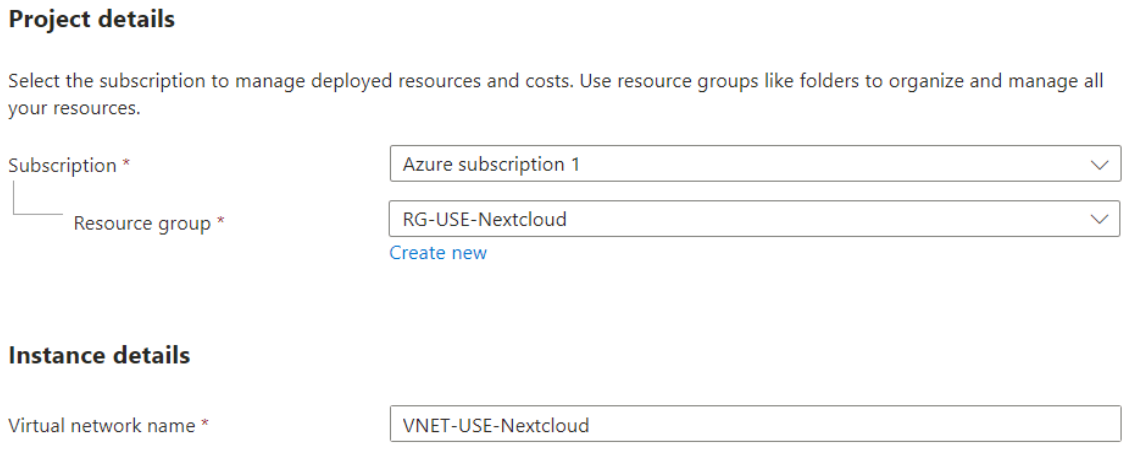
RESOURCE GROUP

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.

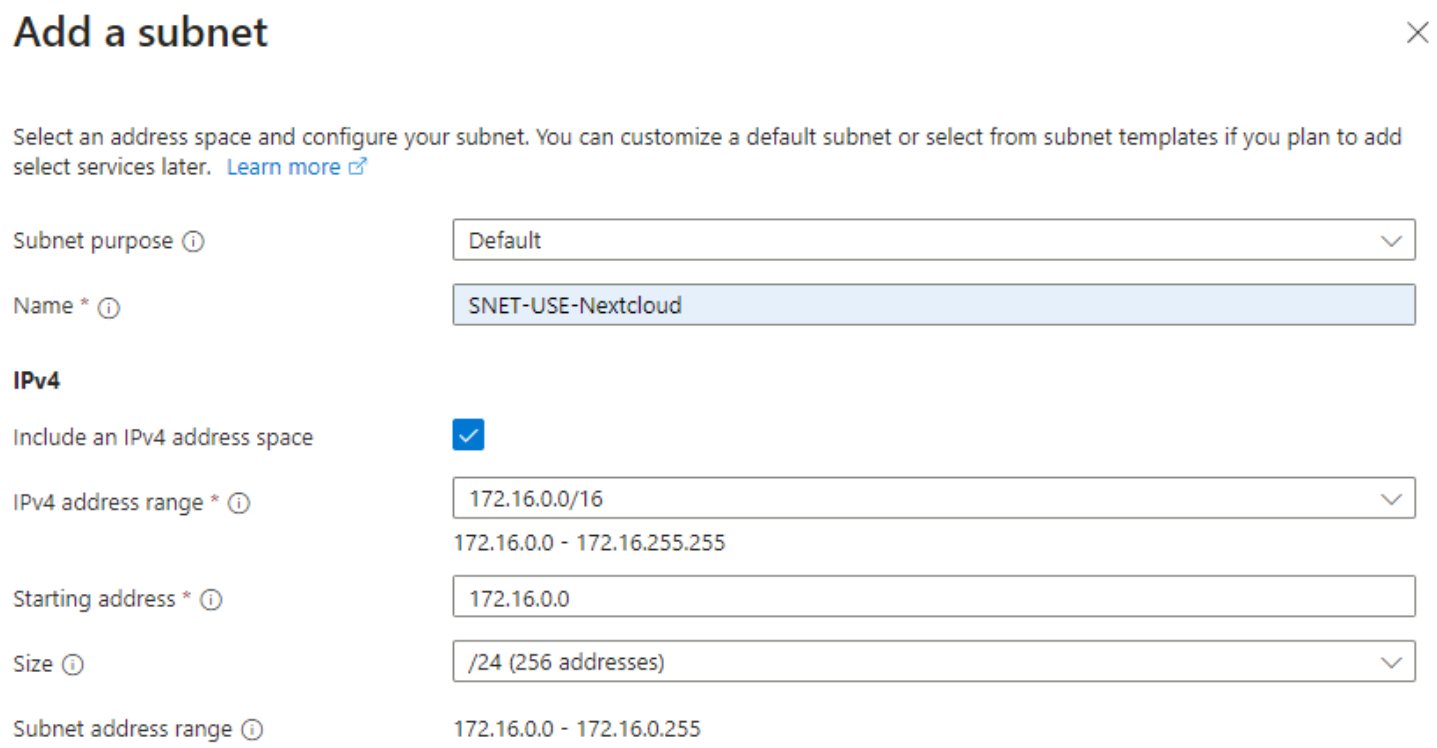


VIRTUAL NETWORK

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



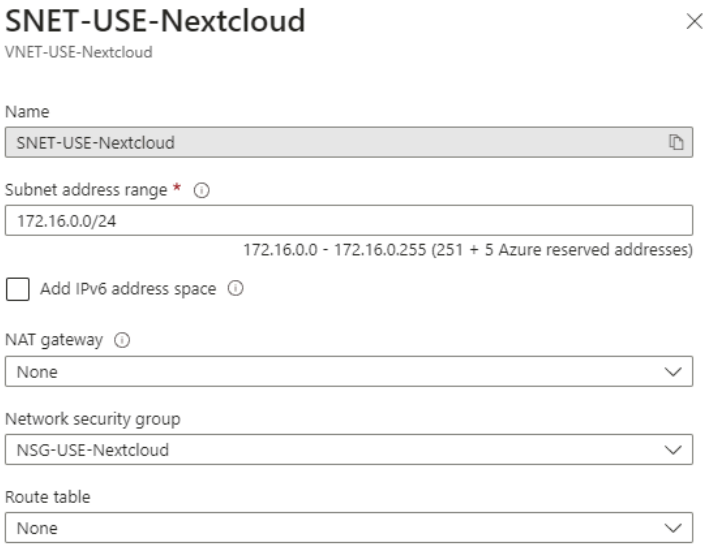
VNET-USE-Nextcloud is configured with 172.16.0.0/16 address space according to RFC 1918. After that, a screened subnet was created where the Nextcloud web server will be deployed. This subnet, SNET-USE-Nextcloud, is configured with an IP address range of 172.16.0.0/24.



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:

Virtual machine

Computer name	VM-USE-Nextcloud
Operating system	Linux (ubuntu 20.04)
Image publisher	canonical
Image offer	0001-com-ubuntu-server-focal
Image plan	20_04-lts-gen2
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.10.0.8
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Availability + scaling

Availability zone (edit)	1
Availability set	-
Scale Set	-

Security type

Security type	Trusted launch
Enable secure boot	Enabled
Enable vTPM	Enabled
Integrity monitoring	Disabled

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	172.16.0.4
Private IP address (IPv6)	-
Virtual network/subnet	VNET-USE-Nextcloud/SNET-USE-Nextcloud
DNS name	-

Size

Size	Standard B2ats v2
vCPUs	2
RAM	1 GiB

Disk

OS disk	VM-USE-Nextcloud_disk1_b67ff6f6127f4b548cd1f8a26065f1ae
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

Auto-shutdown

Auto-shutdown	Not enabled
Scheduled shutdown	-

Azure Spot

Azure Spot	-
Azure Spot eviction policy	-

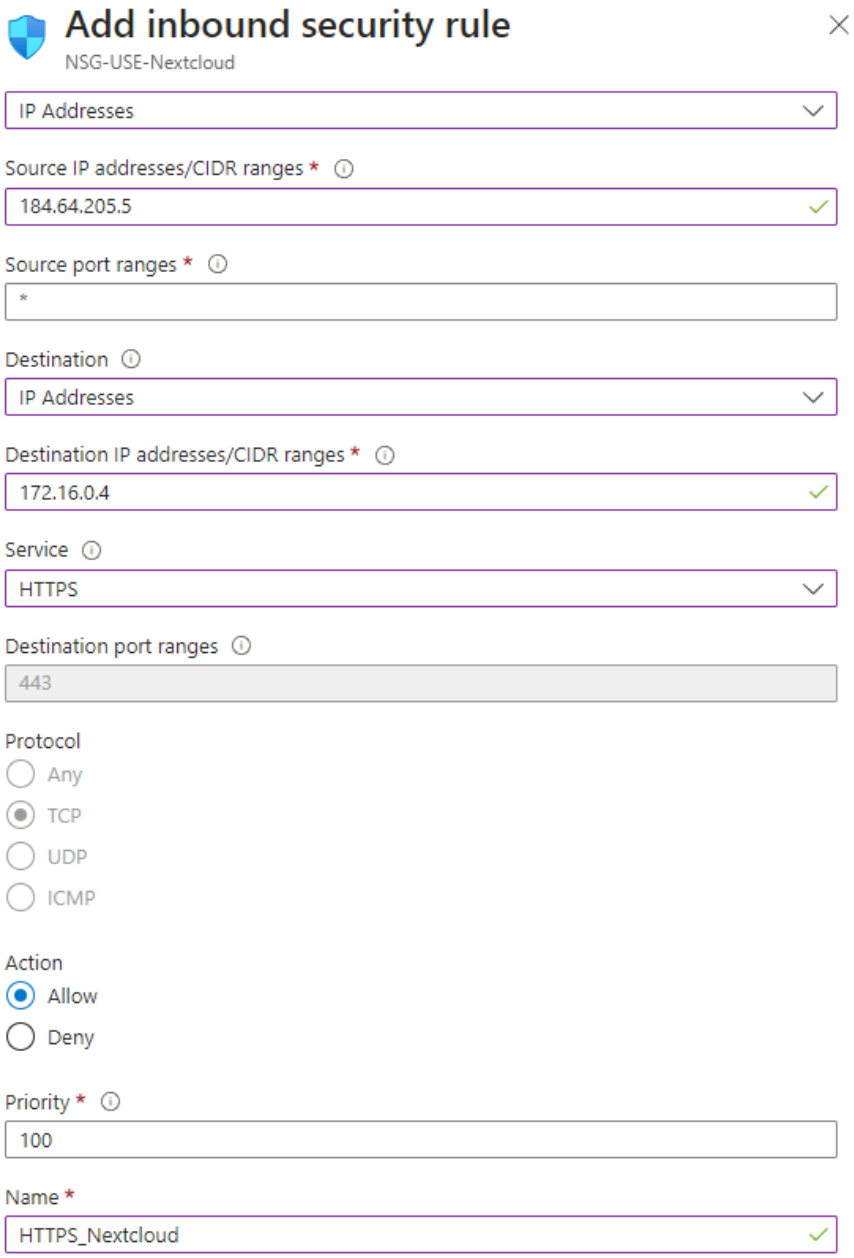
This VM is not able to route through the public internet yet as the public IP is not configured. The NIC is configured to add a public IP address 20.185.37.226 for the web server VM. Also, a DNS label, ibtesamnextcloud.eastus.cloudapp.azure.com, is created within Azure.

Networking

Public IP address	20.185.37.226 (Network interface vm-use-nextcloud306_z1)
Public IP address (IPv6)	-
Private IP address	172.16.0.4
Private IP address (IPv6)	-
Virtual network/subnet	VNET-USE-Nextcloud/SNET-USE-Nextcloud
DNS name	ibtesamnextcloud.eastus.cloudapp.azure.com

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.



Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	HTTPS_Nextcloud	443	TCP	184.64.205.5	172.16.0.4	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

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

Summary

Basics

Name	BASTION-USE-Nextcloud
Subscription	Azure subscription 1
Resource group	RG-USE-Nextcloud
Region	East US
Virtual network	VNET-USE-Nextcloud
Tier	Standard
Subnets	AzureBastionSubnet
Public IP address	BASTION-USE-Nextcloud
Instance count	2
Copy and paste	Enabled
IP-based connection	Disabled
Kerberos authentication	Disabled
Shareable Link	Disabled
Native client support	Disabled

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:

```
ibtesam@VM-USE-Nextcloud:~$ sudo snap install nextcloud
nextcloud 27.1.7snap1 from Nextcloud✓ installed
ibtesam@VM-USE-Nextcloud:~$
```

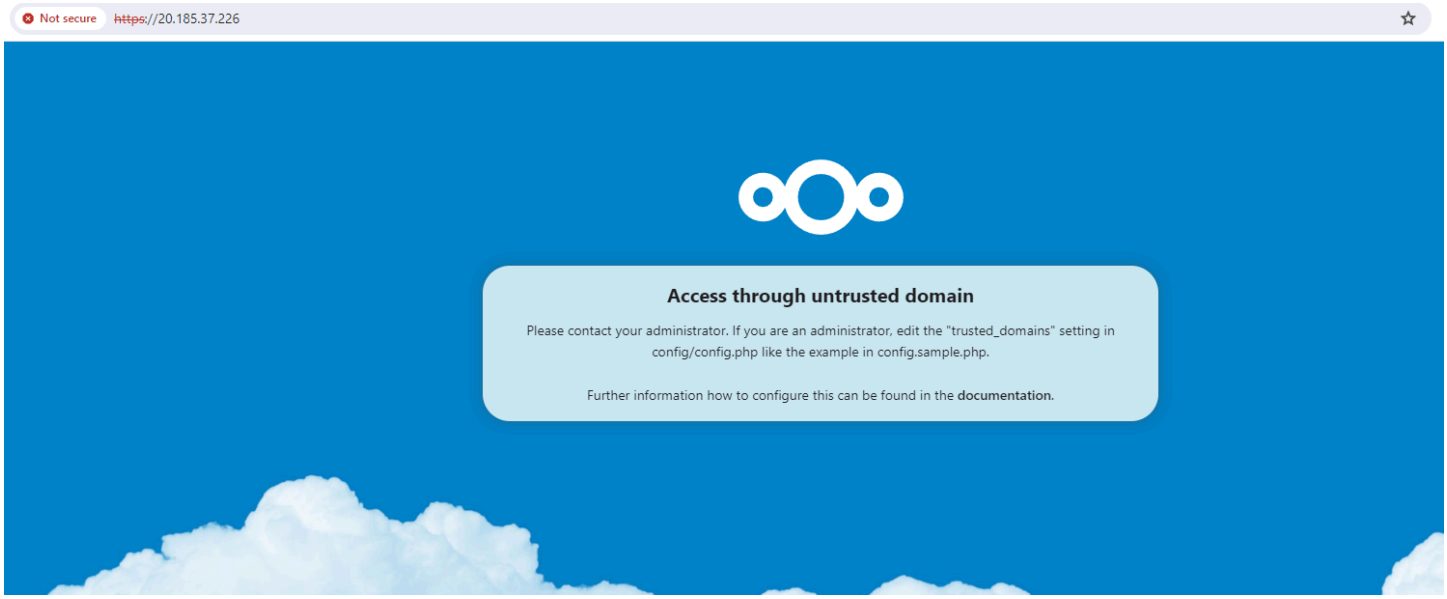
After a successful installation, web server admin is added.

```
ibtesam@VM-USE-Nextcloud:~$ sudo snap install nextcloud
nextcloud 27.1.7snap1 from Nextcloud✓ installed
ibtesam@VM-USE-Nextcloud:~$ sudo nextcloud.manual-install admin [redacted]
```

Adding a self-signed SSL/TLS certificate.

```
ibtesam@VM-USE-Nextcloud:~$ sudo nextcloud.enable-https self-signed
Generating key and self-signed certificate... done
Restarting apache... done
ibtesam@VM-USE-Nextcloud:~$
```

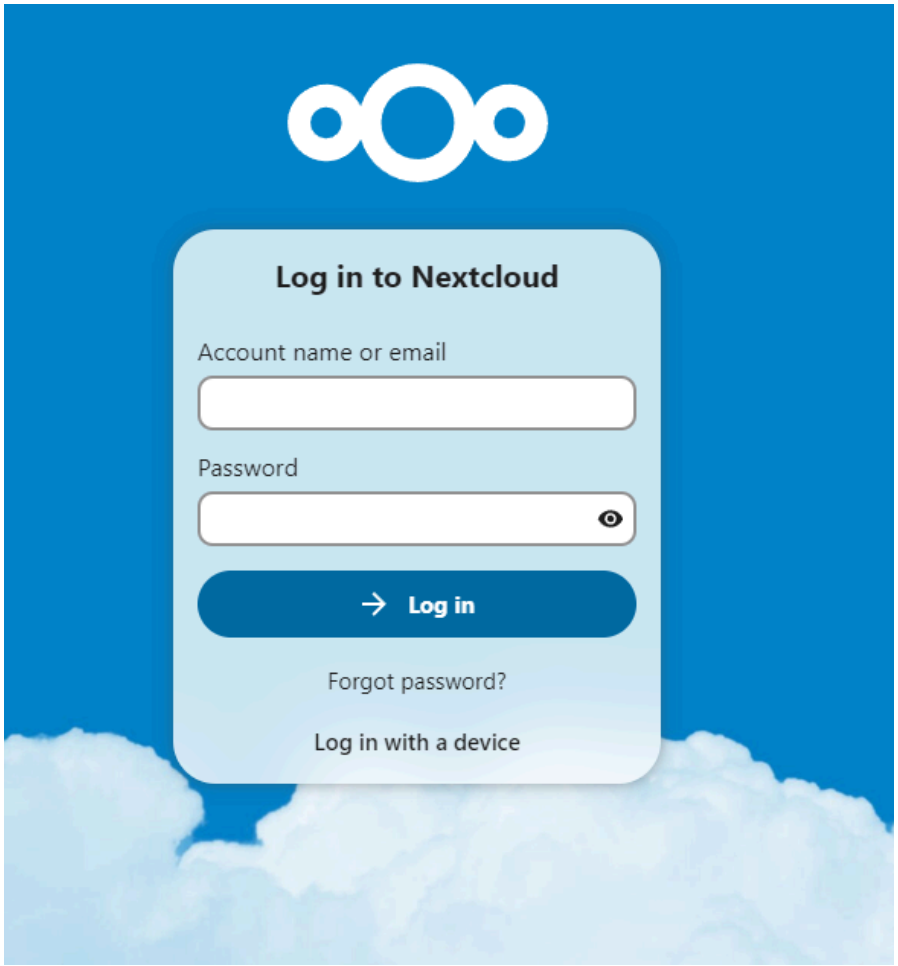
If the web server is accessed without configuring a trusted domain then it will show a nextcloud error: access through an untrusted domain as shown below.



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

```
ibtesam@VM-USE-Nextcloud:~$ sudo nextcloud.occ config:system:set trusted_domains 1 --value=ibtesamnextcloud.eastus.cloudapp.azure.com
System config value trusted_domains => 1 set to string ibtesamnextcloud.eastus.cloudapp.azure.com
ibtesam@VM-USE-Nextcloud:~$
```

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.