



main

EngITFrame / FileShare / Security.md



shekhawatajit Documents updated

3e00ae3 · 3 minutes ago



42 lines (21 loc) · 1.72 KB

Preview

Code

Blame

Raw



# Security Considerations

## 1. Private Network Communication using Private Endpoint only

- VNet Peering ensures that all communication between the two offices remains within Azure's private network, reducing exposure to the public internet. Additionally, we are using Private EndPoint Services which ensures Storage Accounts accessed only internally through endpoint DNS.

## 2. Identity and Access Management

- We use Azure Active Directory (AAD) to manage access to resources.
- Multi-factor authentication (MFA) is used for additional security.

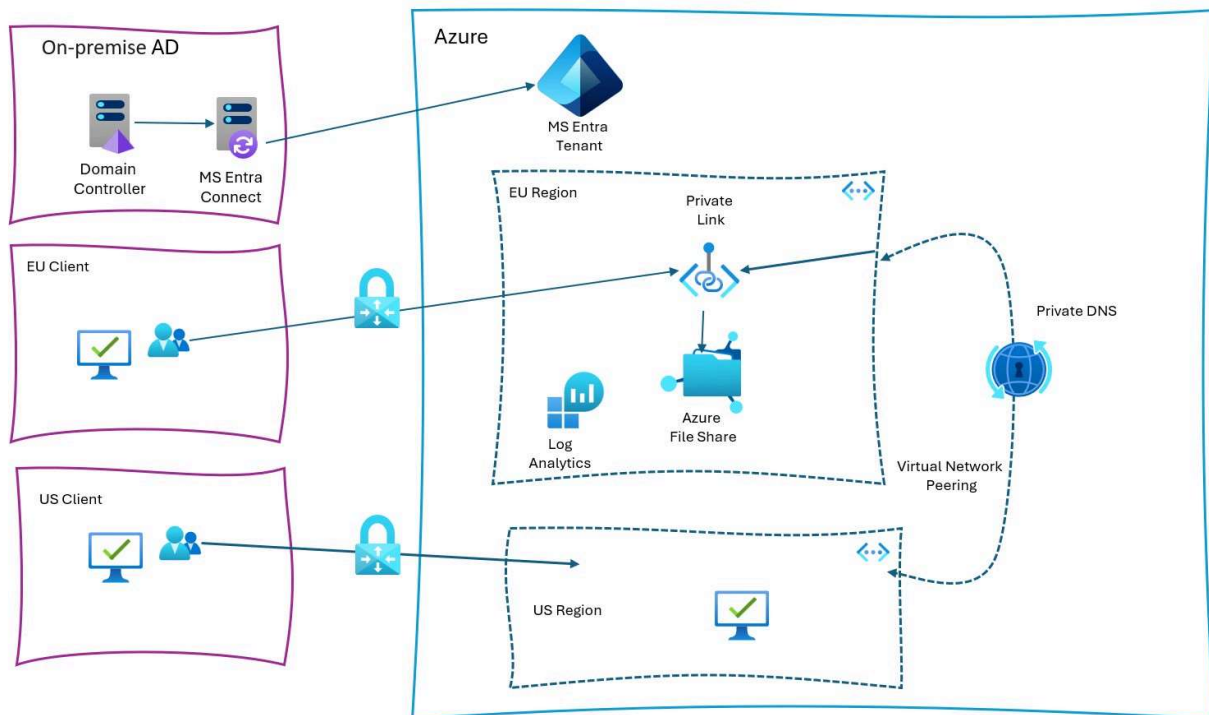
## 3. Network Security Groups (NSGs)

- NSGs control inbound and outbound traffic. Our configured rules only permit necessary traffic between the US and EU subnets, and block any other connections by default.

## 4. Monitoring and Logging

- Used **Log Analytics** for real-time monitoring and logging of network traffic, authentication attempts, and encryption statuses.

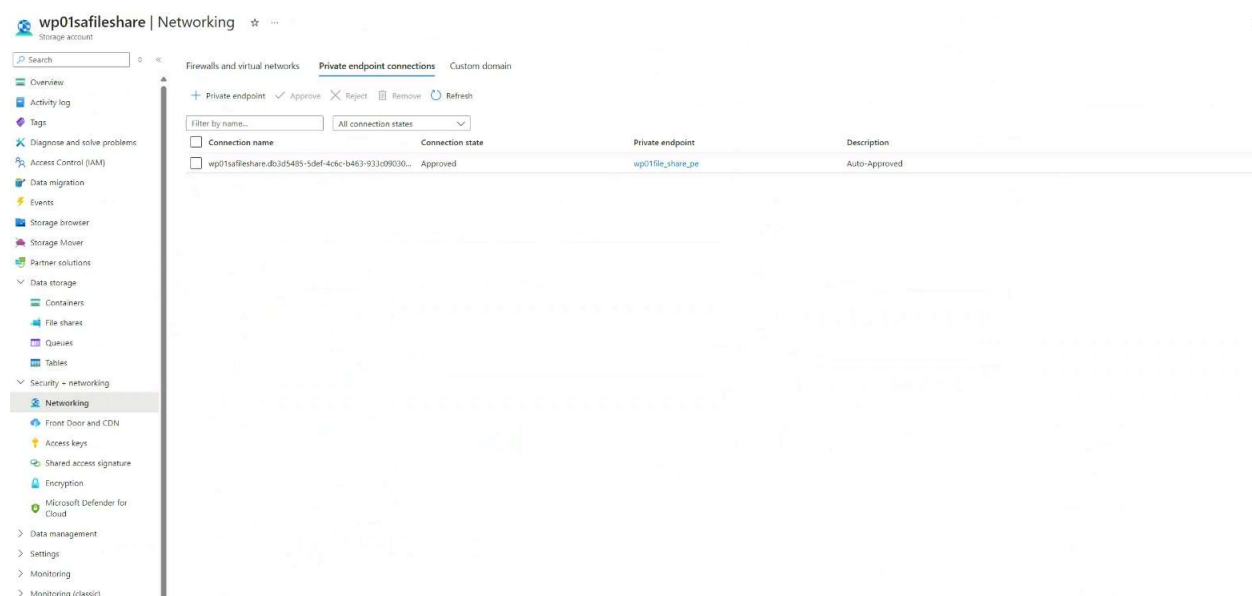
As an example, File Share performance from US region user is monitored and shown on performance dashboard. Other metrics can be added as needed.



## 5. FileShare Access using Private EndPoint and DNS Records

The secure connection between File share goes through Private Endpoint which is resolved through private DNS records for US region internal file access.

### Private Endpoint



### DNS Record Entry

privatelink.file.core.windows.net | Recordsets

Private DNS zone

Search

+ Add Refresh Delete

A record set is a collection of records in a zone that have the same name and are the same type. Record Sets will be automatically fetched in batches of 100 as you scroll through the existing record sets. [Learn more](#)

Search

Fetches 2 record set(s).  
0 record sets selected

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
wp01safileshare	A	300	10.1.1.4	False

## Network Access disabled

Direct Access of Storage is disabled. It can only be accessed using Private Endpoint by resources in the same VNET or peered VNET.

wp01safileshare | Networking

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh Give feedback

Public network access to this storage account has been disabled. Please create a private endpoint connection to grant access.

Public network access

- ☐ Enabled for all networks
- ☐ Enabled from selected virtual networks and IP addresses
- ☒ Disabled

Configure network security for your storage accounts. [Learn more](#)

**Network Routing**

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference \*

- ☒ Microsoft network routing
- ☐ Internet routing

Publish route-specific endpoints

- ☐ Microsoft network routing
- ☐ Internet routing