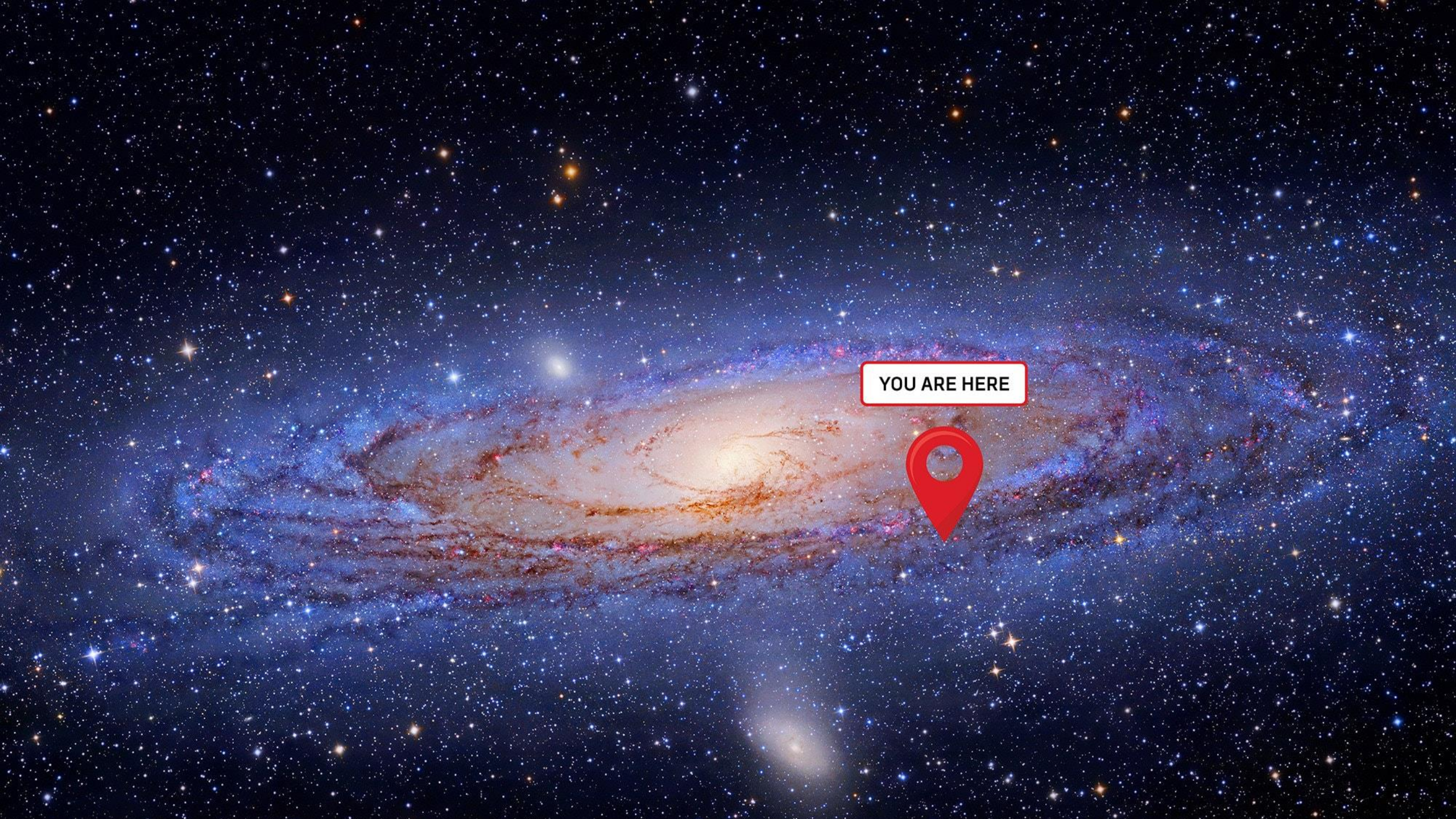
NIC Cloud Connect

Oslo Spektrum
November 7 - 9

Bastiaan Wassenaar

Hub-spoke virtual networks in Azure


YOU ARE HERE

NIC Cloud Connect

Before we start…

- Basic network knowledge
  - CIDR-range
  - Subnets
  - Seen an Azure vnet

nic Cloud Connect

Before we start…

What we cover

- Service Endpoints
- Private Endpoints
- Private DNS Zones
- Peering
- Hub Spoke (IP)
- Hub Spoke (DNS)

NIC Cloud Connect

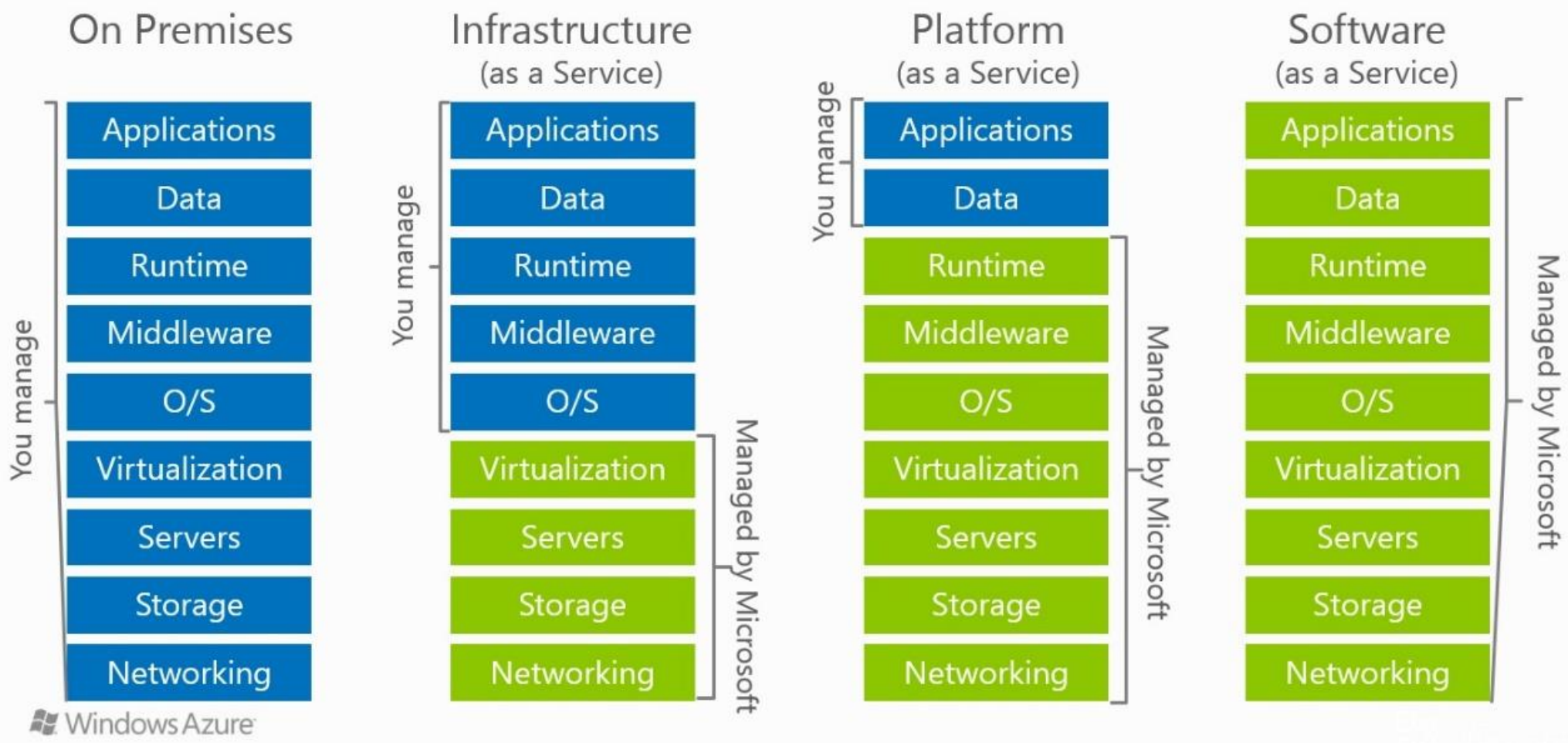
Before we start…

- Things we do NOT touch upon this session
  - Azure Virtual Network manager
  - Azure DNS Private Resolver
  - Azure Virtual WAN
  - Azure Firewall
  - Cross region / subscription / tenant
  - On-prem to cloud connectivity

The history of VNETs


In the beginning. . .

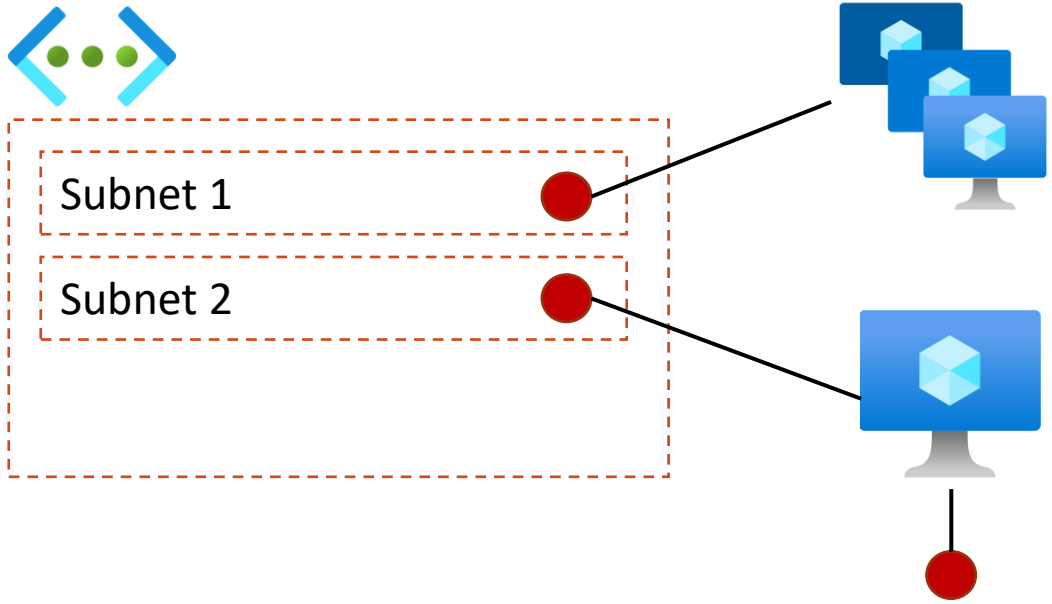
Cloud Models

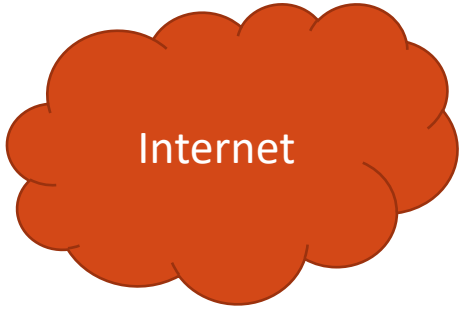


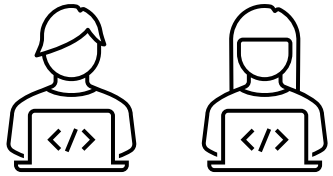
Cloud Connect

MyDatabaseServer

mydatabase.databases.windows.net







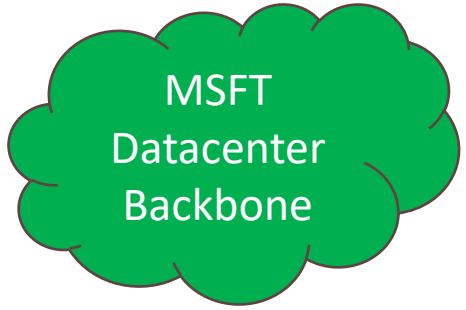
Cloud before *-endpoints

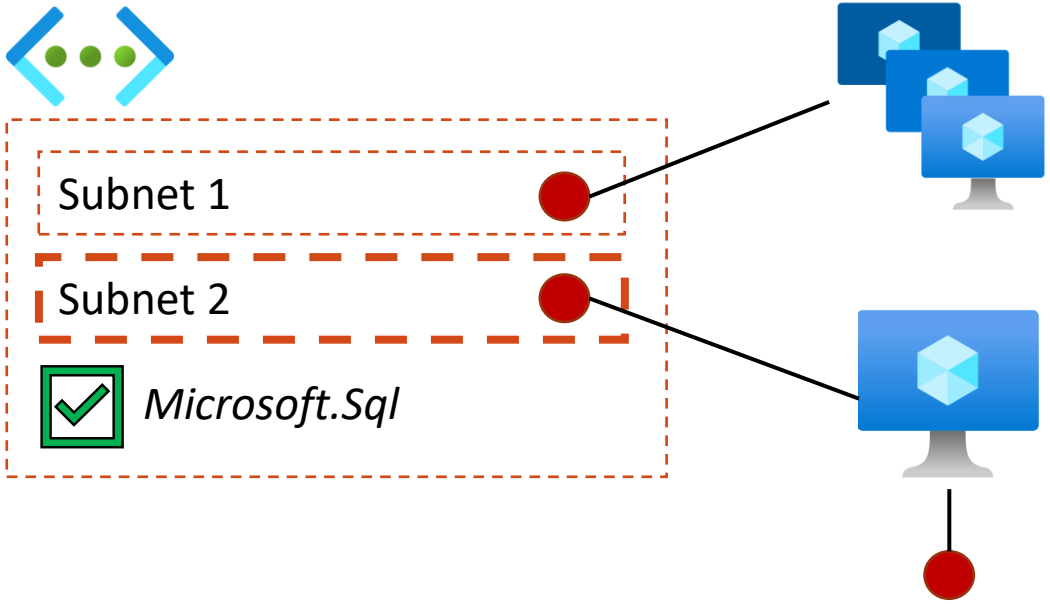

IT'S A CLOUD SERVICE!
YEAH BUT WE DON'T WANT OUR NETWORK TRAFFIC ON THE INTERNET!
CLIENTS
MICROSOFT

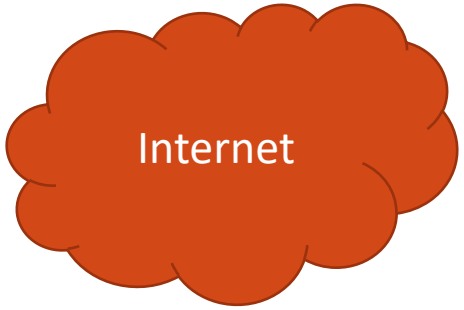
Cloud Connect

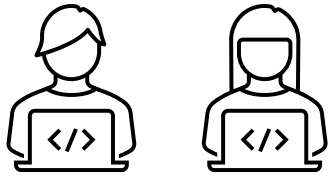
MyDatabaseServer

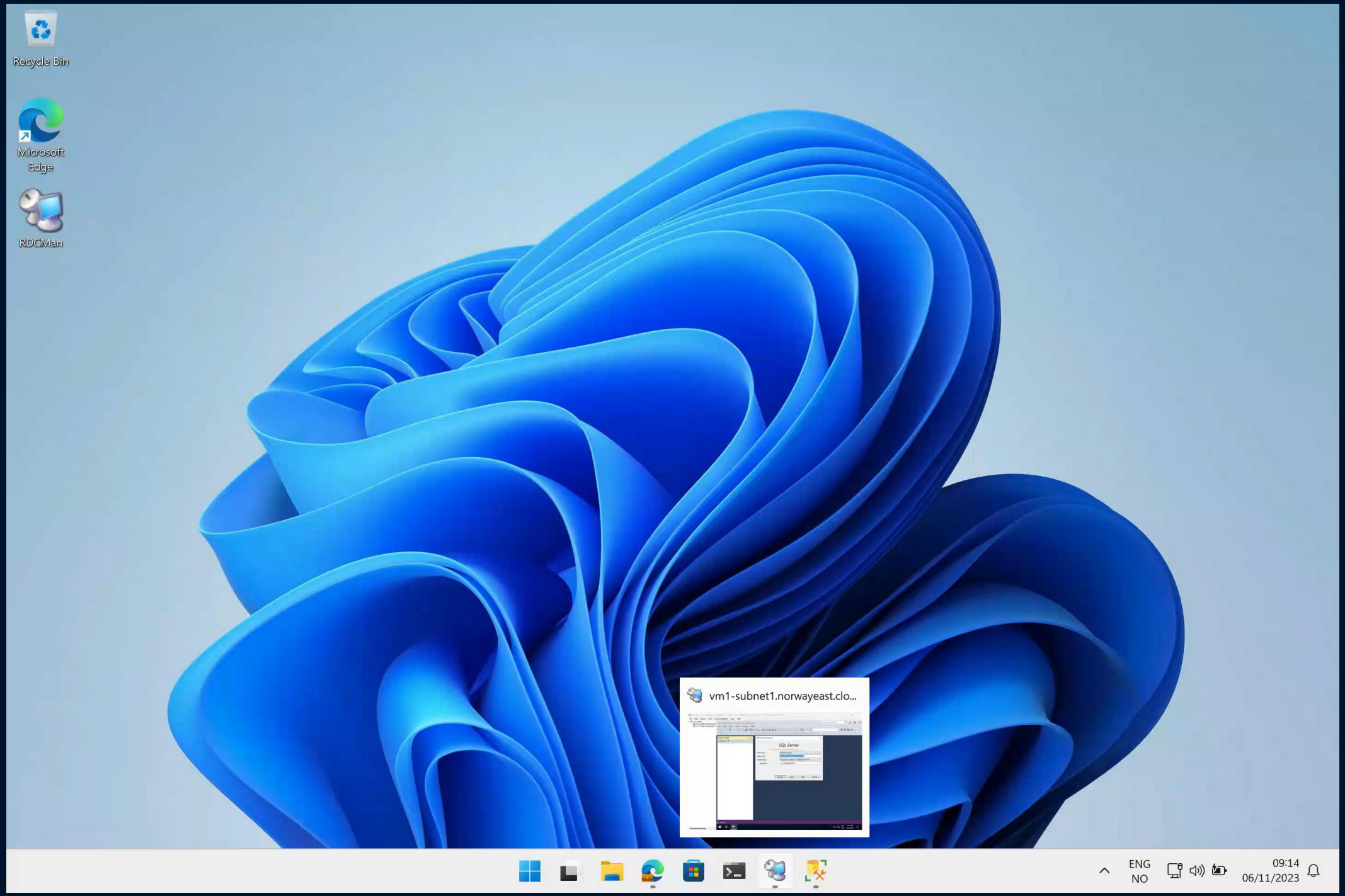
mydatabase.database.windows.net







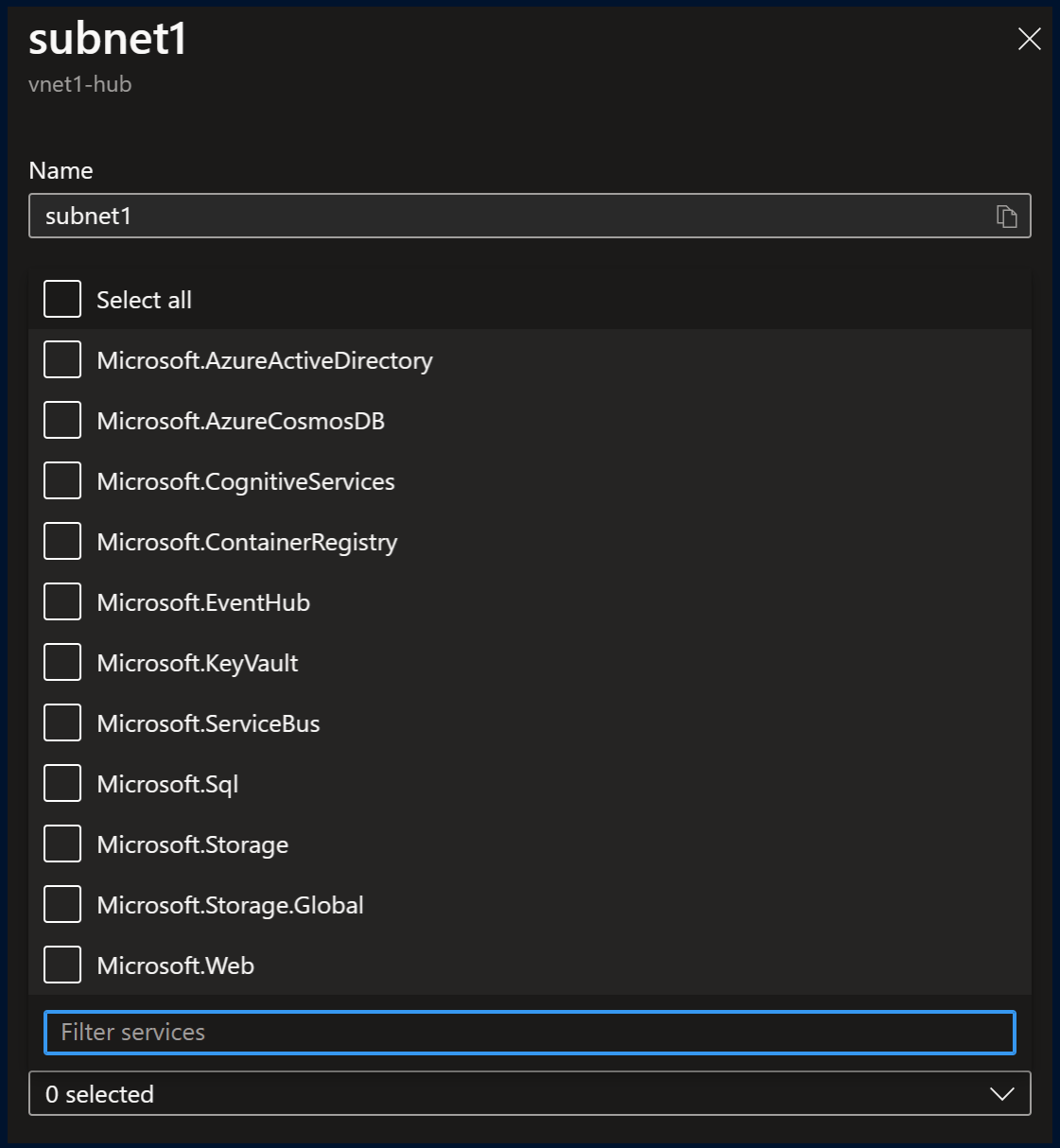



Recycle Bin
Microsoft Edge
RDCMan
vm1-subnet1.norwayeast.clo...
SQL Server
ENG
NO
09:14
06/11/2023

nic Cloud Connect

Service Endpoints

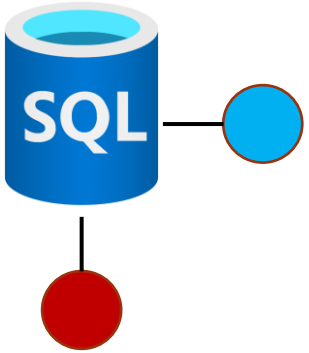
- Most used services support it
- Mostly around Compute services
- Performance gain
- Easiest way of securing network traffic
- No additional costs

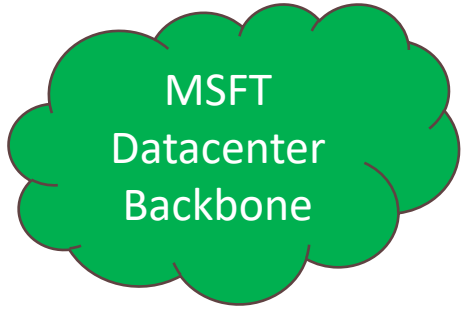


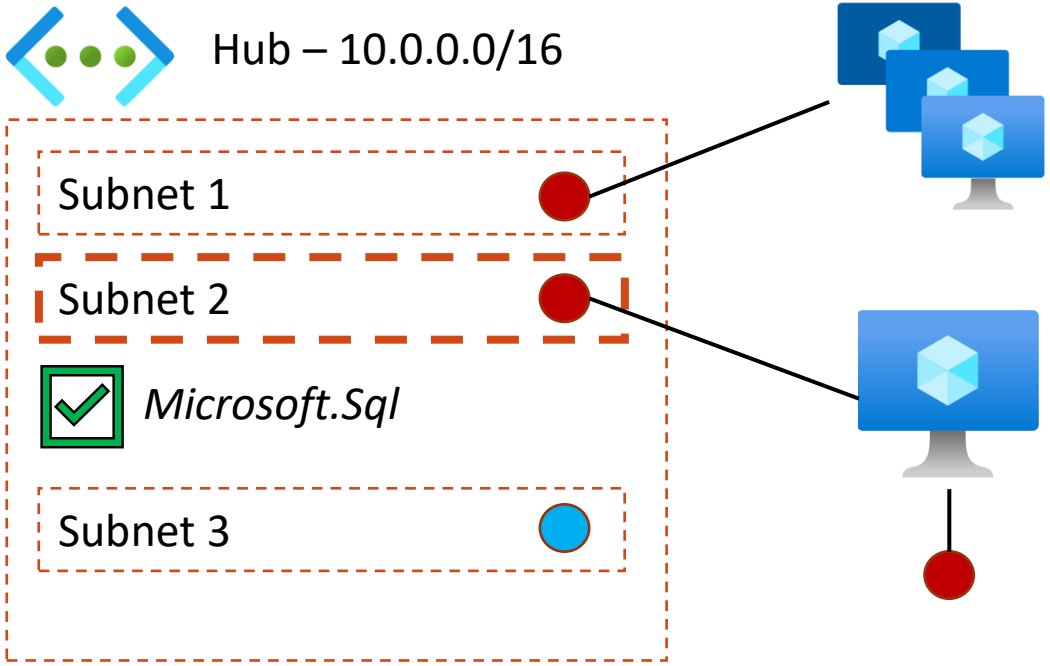
Private Endpoints

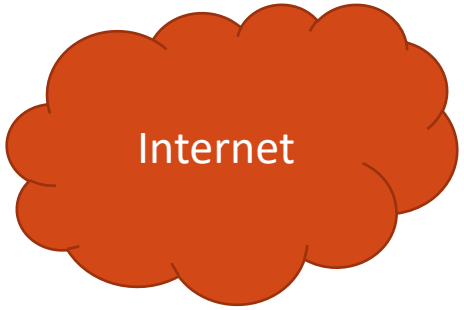
MyDatabaseServer

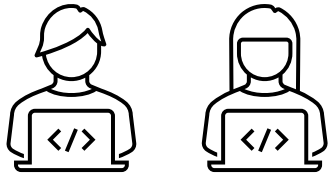
mydatabase.database.windows.net

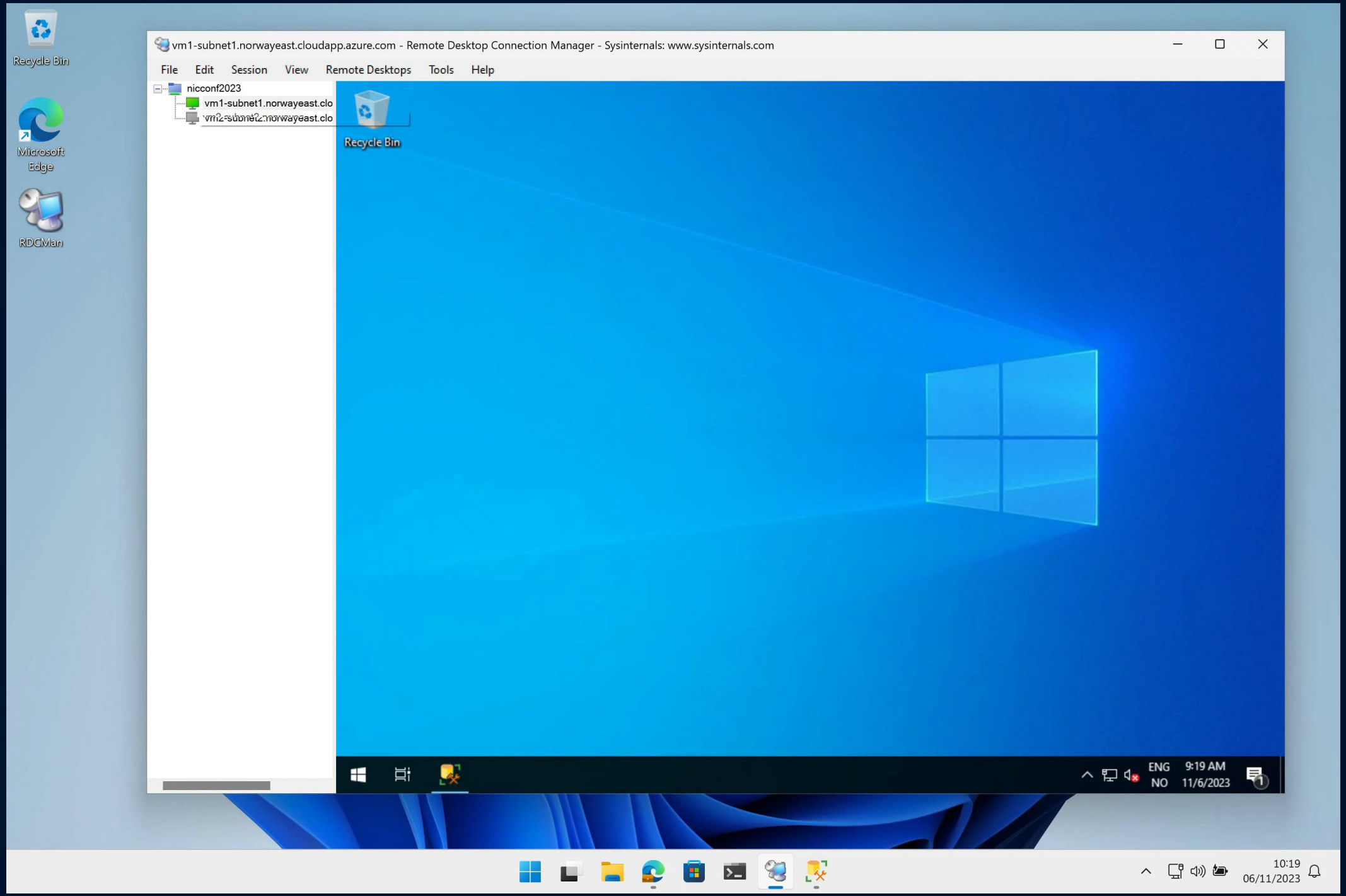











Recycle Bin
Microsoft Edge
RDCMan
vm1-subnet1.norwayeast.cloudapp.azure.com - Remote Desktop Connection Manager - Sysinternals: www.sysinternals.com
File
Edit
Session
View
Remote Desktops
Tools
Help
nicconf2023
vm1-subnet1.norwayeast.clo
Recycle Bin
ENG
NO
9:19 AM
11/6/2023
10:19
06/11/2023

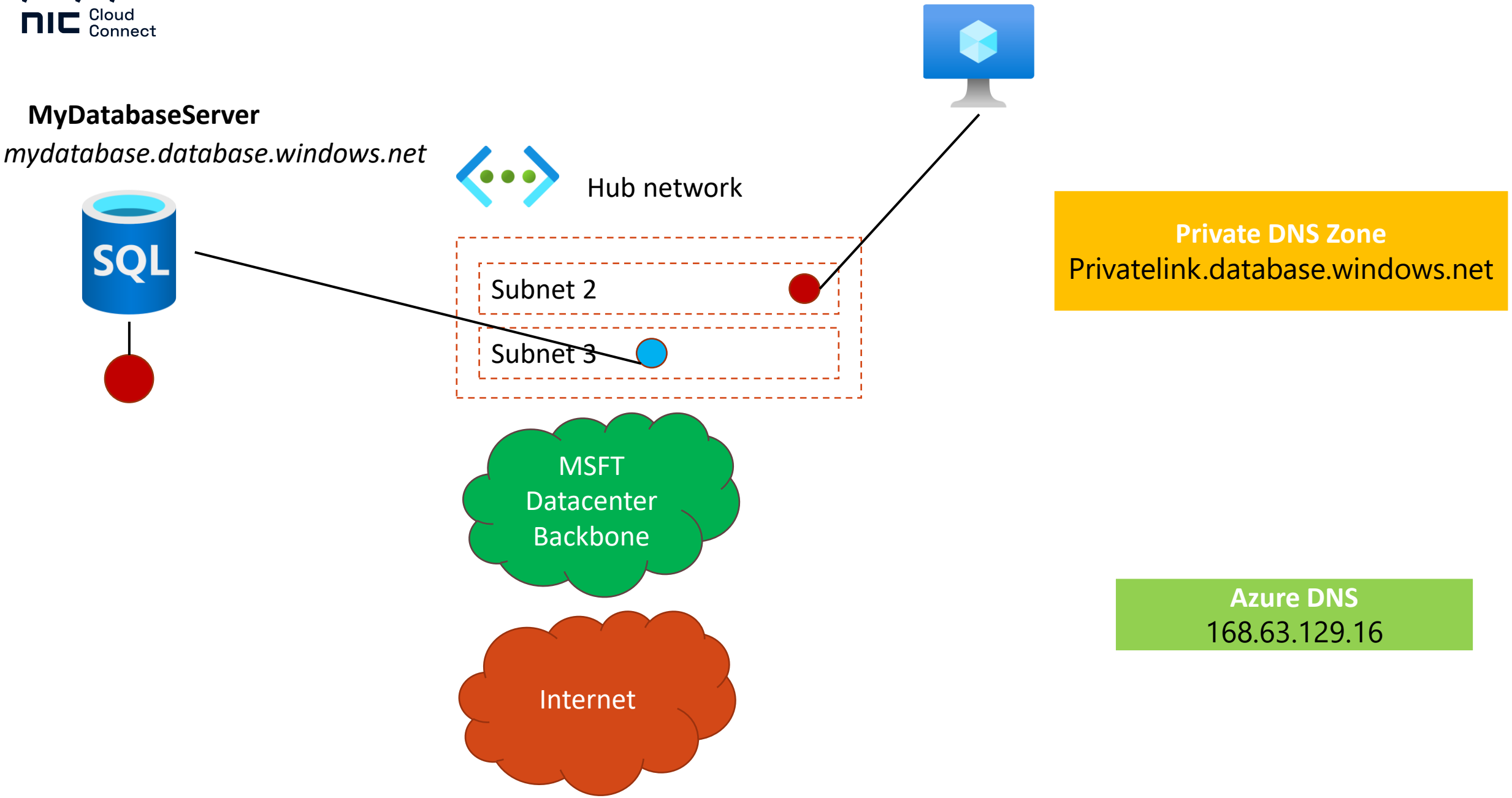
Cloud Connect

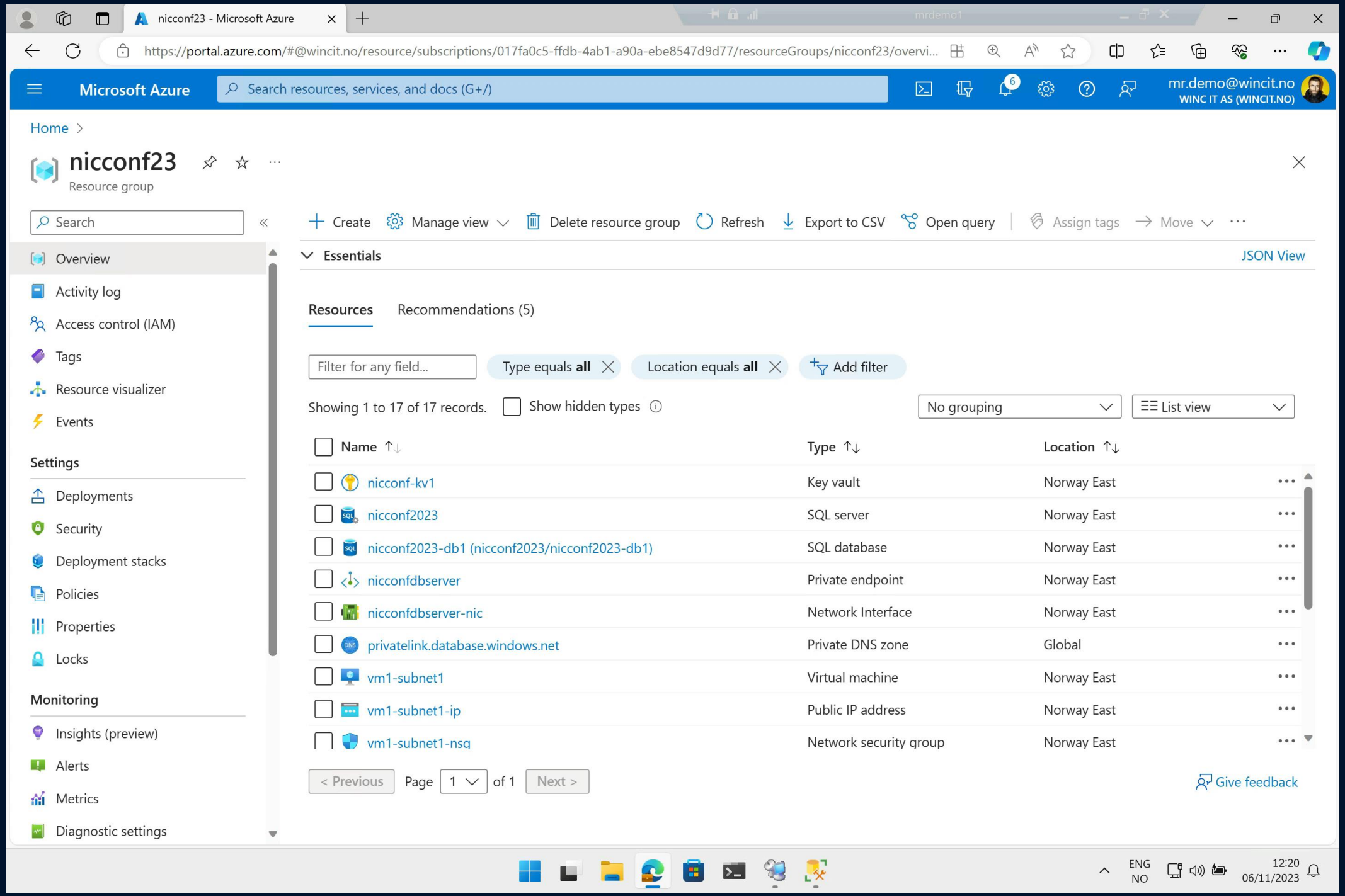
Private Endpoints

- Secure endpoint in your VNET subnet
- All main services supported
- Comes with a cost
  (~82,- NOK / month per endpoint + traffic)
- Is for traffic *TO* a service, not *FROM*
- Cross subscriptions/tenants

Cloud Connect

Private DNS Zones


MyDatabaseServer
mydatabase.database.windows.net
SQL
Hub network
Subnet 2
Subnet 3
MSFT
Datacenter
Backbone
Internet
Private DNS Zone
Privatelink.database.windows.net
Azure DNS
168.63.129.16


nicconf23 - Microsoft Azure
https://portal.azure.com/#@wincit.no/resource/subscriptions/017fa0c5-ffdb-4ab1-a90a-ebe8547d9d77/resourceGroups/nicconf23/overvi...
Microsoft Azure
Search resources, services, and docs (G+/)
mr.demo@wincit.no
WINC IT AS (WINCIT.NO)
Home
nicconf23
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Monitoring
Insights (preview)
Alerts
Metrics
Diagnostic settings
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Essentials
JSON View
Resources
Recommendations (5)
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 17 of 17 records.
Show hidden types
No grouping
List view
Name
Type
Location
nicconf-kv1 Key vault Norway East
nicconf2023 SQL server Norway East
nicconf2023-db1 (nicconf2023/nicconf2023-db1) SQL database Norway East
nicconfdbserver Private endpoint Norway East
nicconfdbserver-nic Network Interface Norway East
privatelink.database.windows.net Private DNS zone Global
vm1-subnet1 Virtual machine Norway East
vm1-subnet1-ip Public IP address Norway East
vm1-subnet1-nsg Network security group Norway East
< Previous
Page 1 of 1
Next >
Give feedback
ENG
NO
12:20
06/11/2023

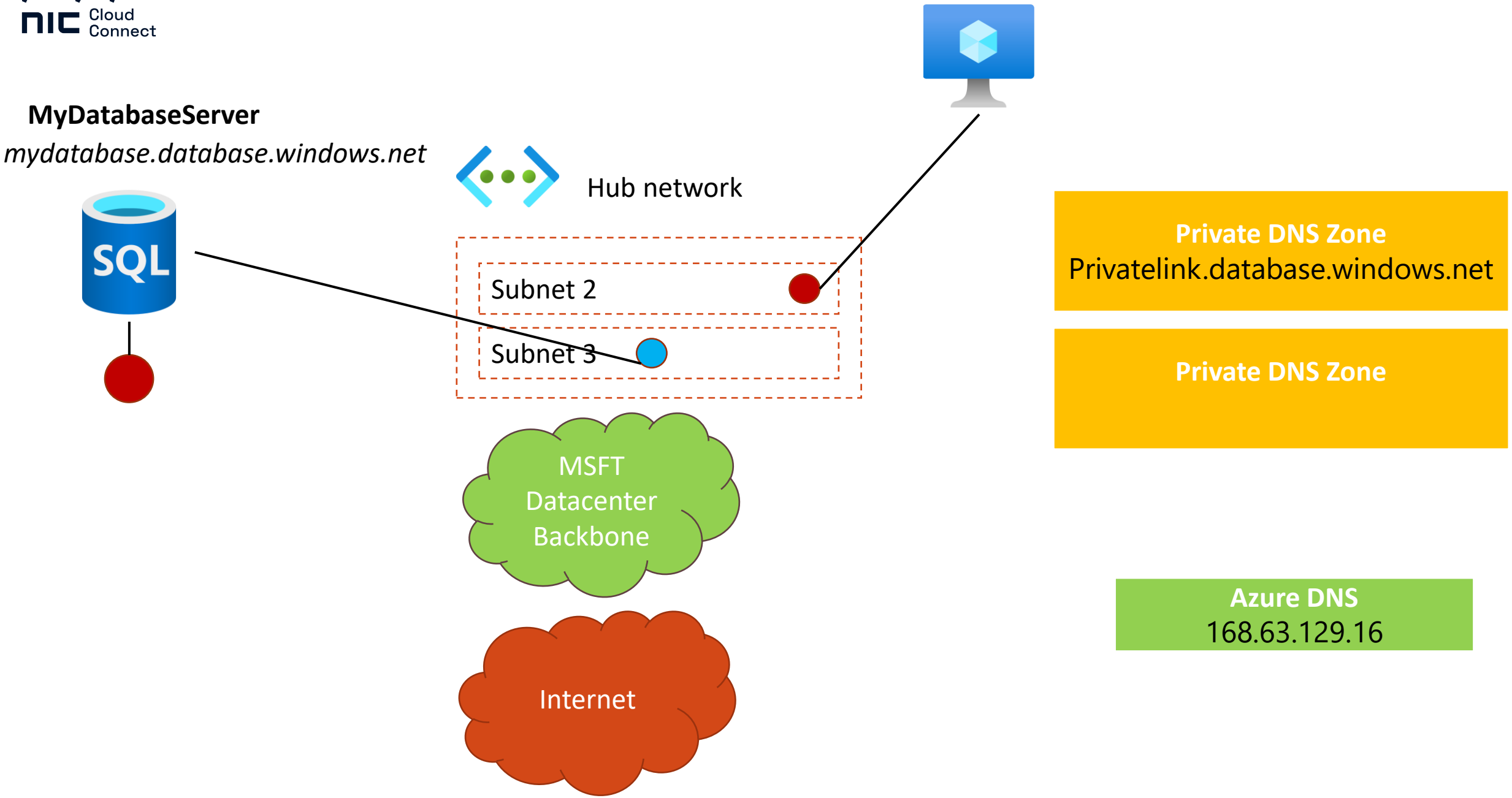
nic Cloud Connect

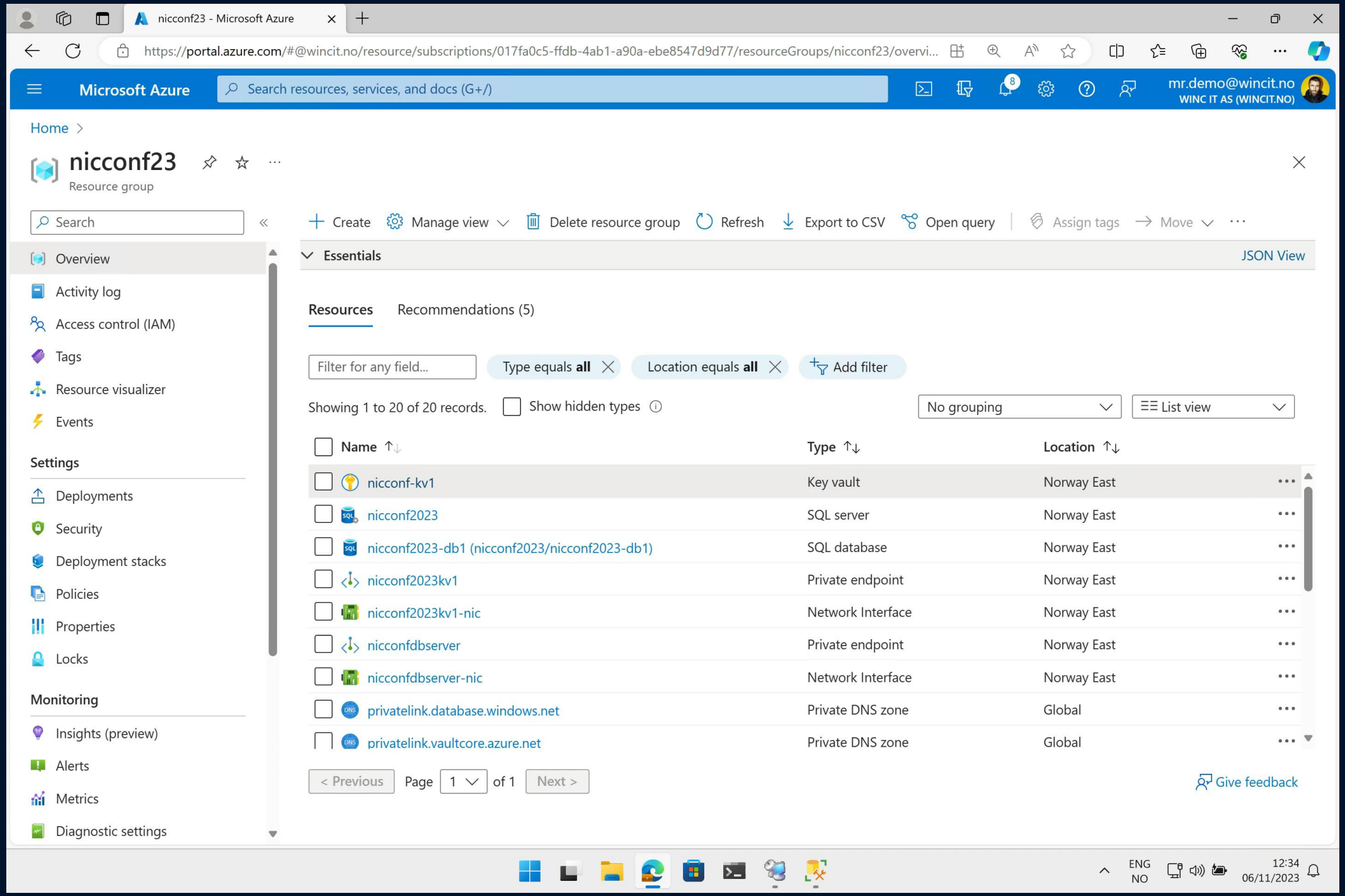
Private DNS Zones

- A private DNS zone per service
- List of Private DNS zones

Cloud Connect

Custom Private DNS Zones


MyDatabaseServer
mydatabase.database.windows.net
Hub network
Subnet 2
Subnet 3
MSFT
Datacenter
Backbone
Internet
Private DNS Zone
Privatelink.database.windows.net
Private DNS Zone
Azure DNS
168.63.129.16


nicconf23 - Microsoft Azure
https://portal.azure.com/#@wincit.no/resource/subscriptions/017fa0c5-ffdb-4ab1-a90a-ebe8547d9d77/resourceGroups/nicconf23/overvi...
Microsoft Azure
Search resources, services, and docs (G+/)
mr.demo@wincit.no
WINC IT AS (WINCIT.NO)
Home
nicconf23
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Monitoring
Insights (preview)
Alerts
Metrics
Diagnostic settings
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Essentials
JSON View
Resources
Recommendations (5)
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 20 of 20 records.
Show hidden types
No grouping
List view
Name
Type
Location
nicconf-kv1 Key vault Norway East
nicconf2023 SQL server Norway East
nicconf2023-db1 (nicconf2023/nicconf2023-db1) SQL database Norway East
nicconf2023kv1 Private endpoint Norway East
nicconf2023kv1-nic Network Interface Norway East
nicconfdbserver Private endpoint Norway East
nicconfdbserver-nic Network Interface Norway East
privatelink.database.windows.net Private DNS zone Global
privatelink.vaultcore.azure.net Private DNS zone Global
< Previous
Page 1 of 1
Next >
Give feedback
ENG
NO
12:34
06/11/2023

nic Cloud Connect

Custom Private DNS Zones

- Can be whatever you want
- Works the same as normal DNS
  (so choose your name wisely)

VNET Peering (IP)

VNET Peering (without hub-spoke)

- Before you start doing this… Find your network guy/girl/person.
- Even more “fun” when you start cross-region peering.
- Can not have overlapping IP-ranges (!)

Managing Your IP Addresses with Azure Virtual Network Manager

Demo | In Seattle Only | Will Not Be Recorded

Wednesday, November 15

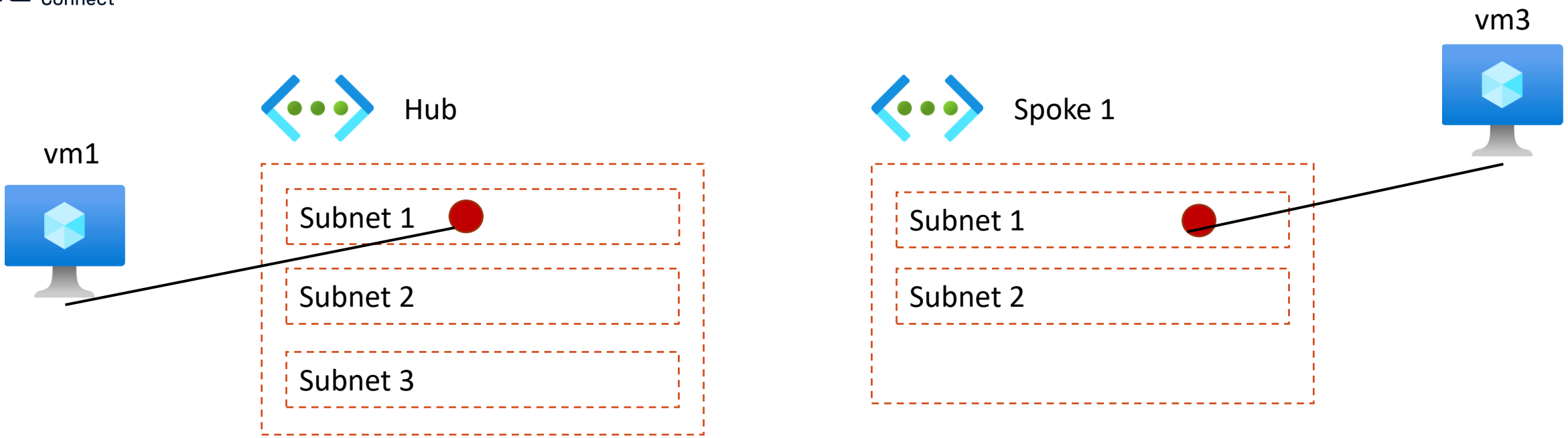
9:00 PM - 9:15 PM Central European Standard Time

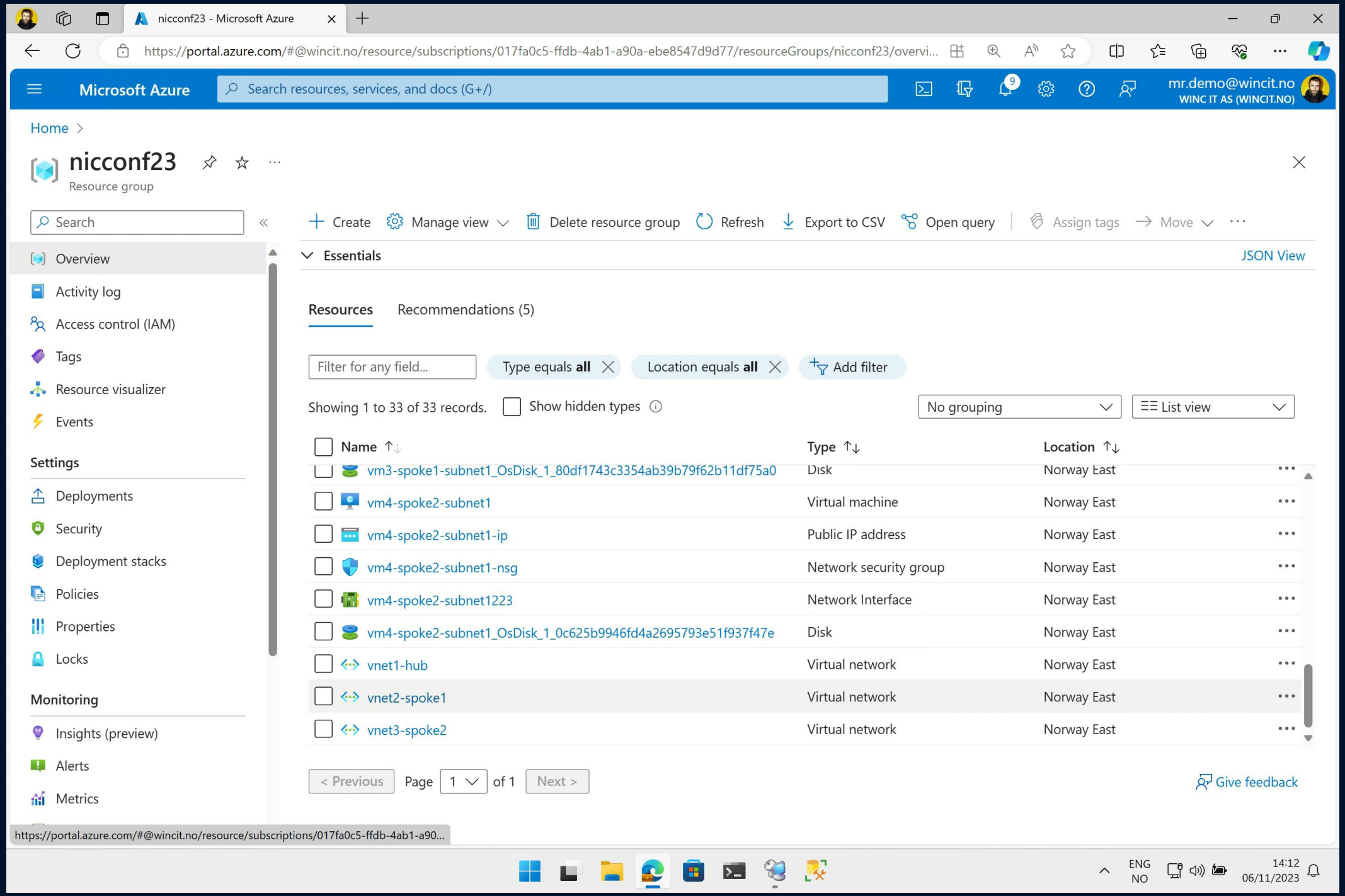
Join us for a live demo of a new IP address management (IPAM) service offered by Azure Virtual Network Manager. With IPAM, you can automate VNet creation from non-overlapping IPs, reserve and assign IPs, track IP usage, and more. See how our new solution simplifies the allocation, monitoring, and optimization of IP addresses in your network infrastructure to offer you visibility, flexibility, and scalability with your IPs. We also invite attendees to participate in our private preview.

Show less

AM Andrea Michael | Mi...

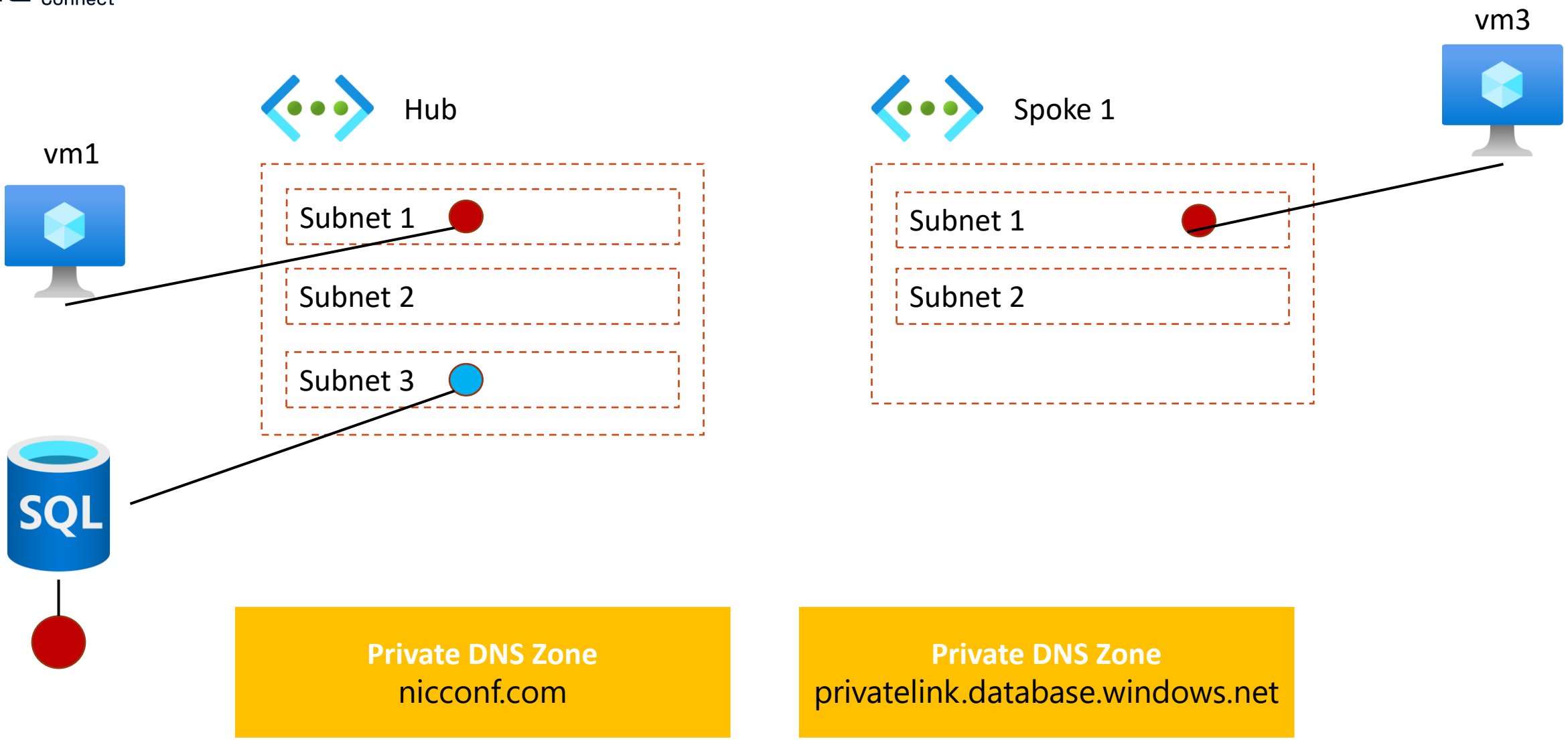
JL Jay Li | Microsoft

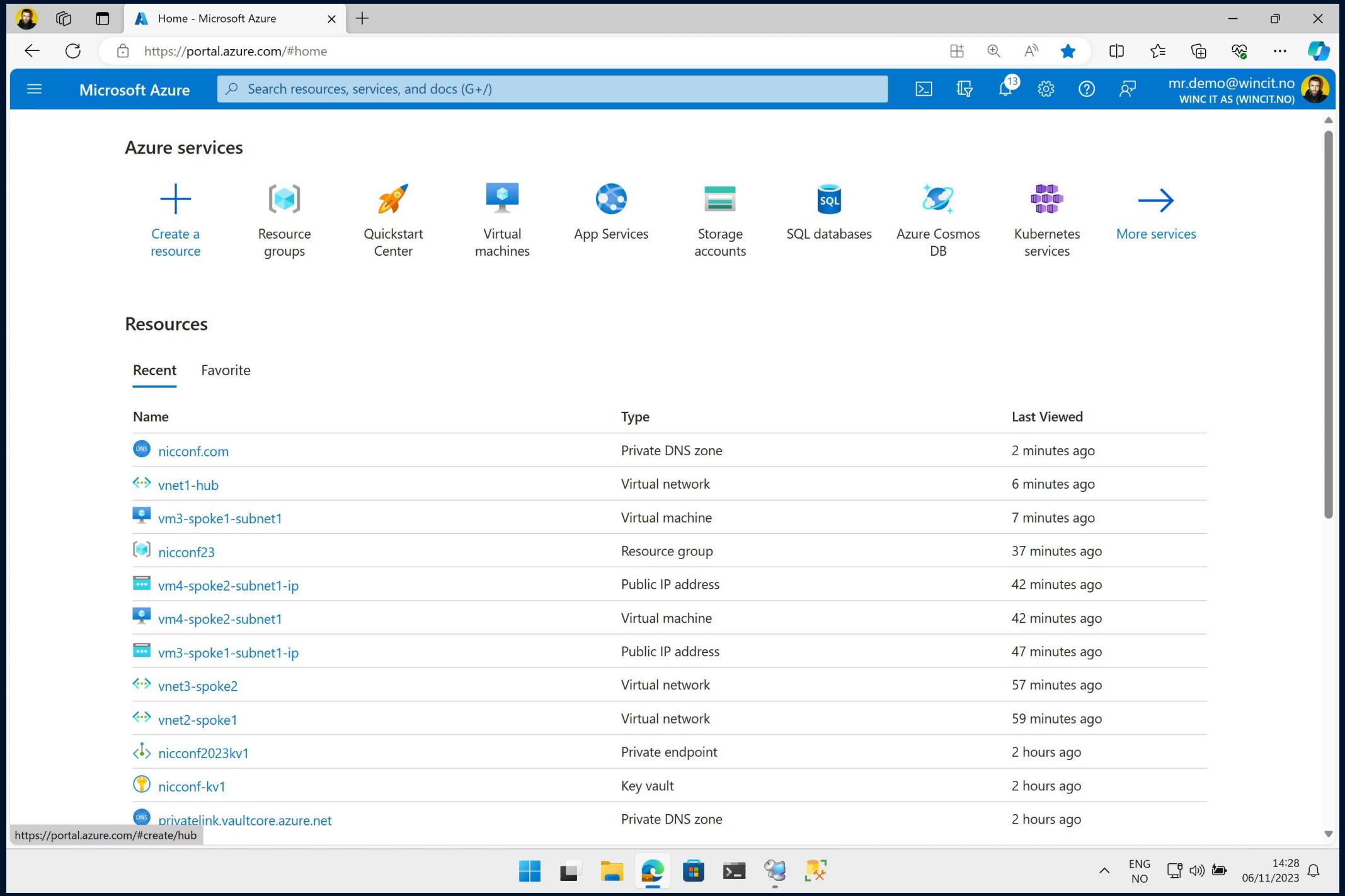

vm3
Hub
Spoke 1
vm1
Subnet 1
Subnet 2
Subnet 3
Subnet 1
Subnet 2


nicconf23 - Microsoft Azure
https://portal.azure.com/#@wincit.no/resource/subscriptions/017fa0c5-ffdb-4ab1-a90a-ebe8547d9d77/resourceGroups/nicconf23/overvi...
Microsoft Azure
Search resources, services, and docs (G+/)
mr.demo@wincit.no
WINC IT AS (WINCIT.NO)
Home
nicconf23
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Monitoring
Insights (preview)
Alerts
Metrics
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Essentials
JSON View
Resources
Recommendations (5)
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 33 of 33 records.
Show hidden types
No grouping
List view
Name
Type
Location
vm3-spoke1-subnet1_OsDisk_1_80df1743c3354ab39b79f62b11df75a0 Disk Norway East
vm4-spoke2-subnet1 Virtual machine Norway East
vm4-spoke2-subnet1-ip Public IP address Norway East
vm4-spoke2-subnet1-nsg Network security group Norway East
vm4-spoke2-subnet1223 Network Interface Norway East
vm4-spoke2-subnet1_OsDisk_1_0c625b9946fd4a2695793e51f937f47e Disk Norway East
vnet1-hub Virtual network Norway East
vnet2-spoke1 Virtual network Norway East
vnet3-spoke2 Virtual network Norway East
< Previous
Page 1 of 1
Next >
Give feedback
https://portal.azure.com/#@wincit.no/resource/subscriptions/017fa0c5-ffdb-4ab1-a90...
ENG
NO
14:12
06/11/2023

Cloud Connect

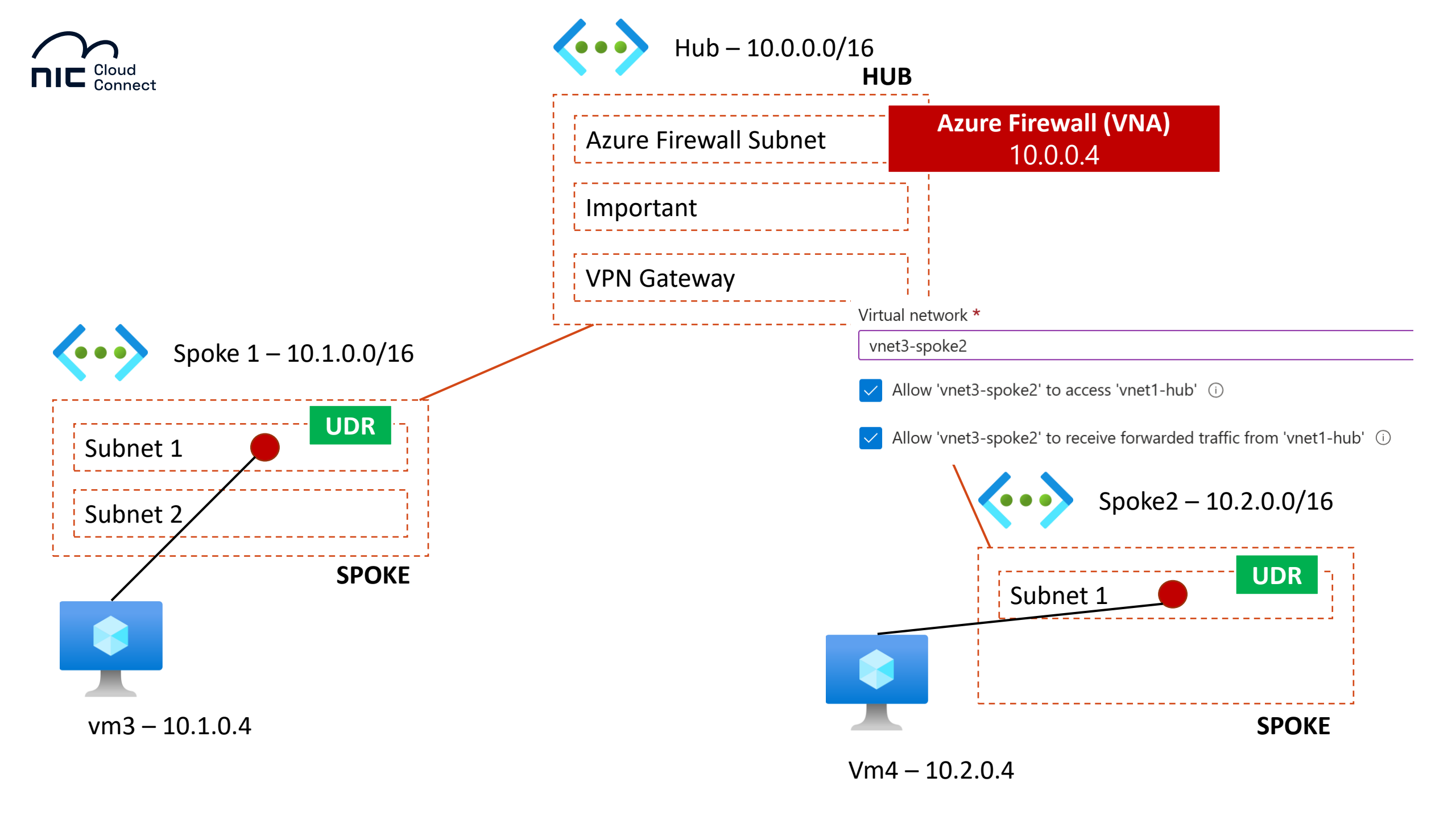
VNET Peering and Private DNS Zones

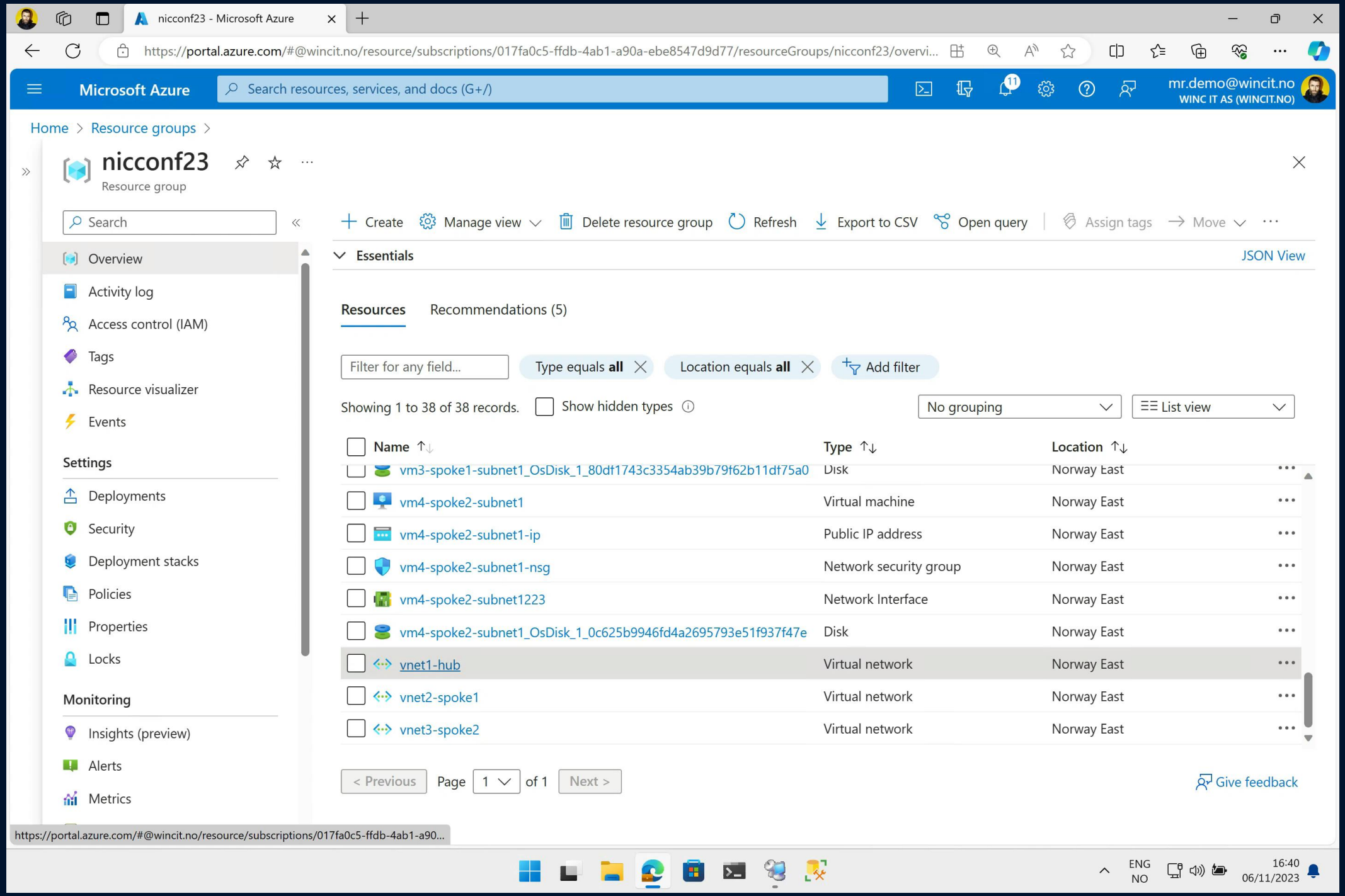

vm3
Hub
Spoke 1
vm1
Subnet 1
Subnet 2
Subnet 3
Subnet 1
Subnet 2
SQL
Private DNS Zone
nicconf.com
Private DNS Zone
privatelink.database.windows.net


Home - Microsoft Azure
https://portal.azure.com/#home
Microsoft Azure
Search resources, services, and docs (G+/)
mr.demo@wincit.no
WINC IT AS (WINCIT.NO)
Azure services
Create a resource
Resource groups
Quickstart Center
Virtual machines
App Services
Storage accounts
SQL databases
Azure Cosmos DB
Kubernetes services
More services
Resources
Recent
Favorite
Name
Type
Last Viewed
nicconf.com
Private DNS zone
2 minutes ago
vnet1-hub
Virtual network
6 minutes ago
vm3-spoke1-subnet1
Virtual machine
7 minutes ago
nicconf23
Resource group
37 minutes ago
vm4-spoke2-subnet1-ip
Public IP address
42 minutes ago
vm4-spoke2-subnet1
Virtual machine
42 minutes ago
vm3-spoke1-subnet1-ip
Public IP address
47 minutes ago
vnet3-spoke2
Virtual network
57 minutes ago
vnet2-spoke1
Virtual network
59 minutes ago
nicconf2023kv1
Private endpoint
2 hours ago
nicconf-kv1
Key vault
2 hours ago
privatelink.vaultcore.azure.net
Private DNS zone
2 hours ago
https://portal.azure.com/#create/hub
ENG
NO
14:28
06/11/2023

Cloud Connect

Hub-spoke vnets (IP-based)


Cloud Connect
Hub – 10.0.0.0/16
HUB
Azure Firewall Subnet
Azure Firewall (VNA)
10.0.0.4
Important
VPN Gateway
Virtual network *
vnet3-spoke2
Allow 'vnet3-spoke2' to access 'vnet1-hub'
Allow 'vnet3-spoke2' to receive forwarded traffic from 'vnet1-hub'
Spoke 1 – 10.1.0.0/16
UDR
Subnet 1
Subnet 2
SPOKE
vm3 – 10.1.0.4
Spoke2 – 10.2.0.0/16
UDR
Subnet 1
SPOKE
Vm4 – 10.2.0.4


nicconf23 - Microsoft Azure
https://portal.azure.com/#@wincit.no/resource/subscriptions/017fa0c5-ffdb-4ab1-a90a-ebe8547d9d77/resourceGroups/nicconf23/overvi...
Microsoft Azure
Search resources, services, and docs (G+/)
mr.demo@wincit.no
WINC IT AS (WINCIT.NO)
Home > Resource groups >
nicconf23
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Monitoring
Insights (preview)
Alerts
Metrics
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Essentials
JSON View
Resources
Recommendations (5)
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 38 of 38 records.
Show hidden types
No grouping
List view
Name
Type
Location
vm3-spoke1-subnet1_OsDisk_1_80df1743c3354ab39b79f62b11df75a0 Disk Norway East
vm4-spoke2-subnet1 Virtual machine Norway East
vm4-spoke2-subnet1-ip Public IP address Norway East
vm4-spoke2-subnet1-nsg Network security group Norway East
vm4-spoke2-subnet1223 Network Interface Norway East
vm4-spoke2-subnet1_OsDisk_1_0c625b9946fd4a2695793e51f937f47e Disk Norway East
vnet1-hub Virtual network Norway East
vnet2-spoke1 Virtual network Norway East
vnet3-spoke2 Virtual network Norway East
< Previous
Page 1 of 1
Next >
Give feedback
https://portal.azure.com/#@wincit.no/resource/subscriptions/017fa0c5-ffdb-4ab1-a90...
ENG
NO
16:40
06/11/2023

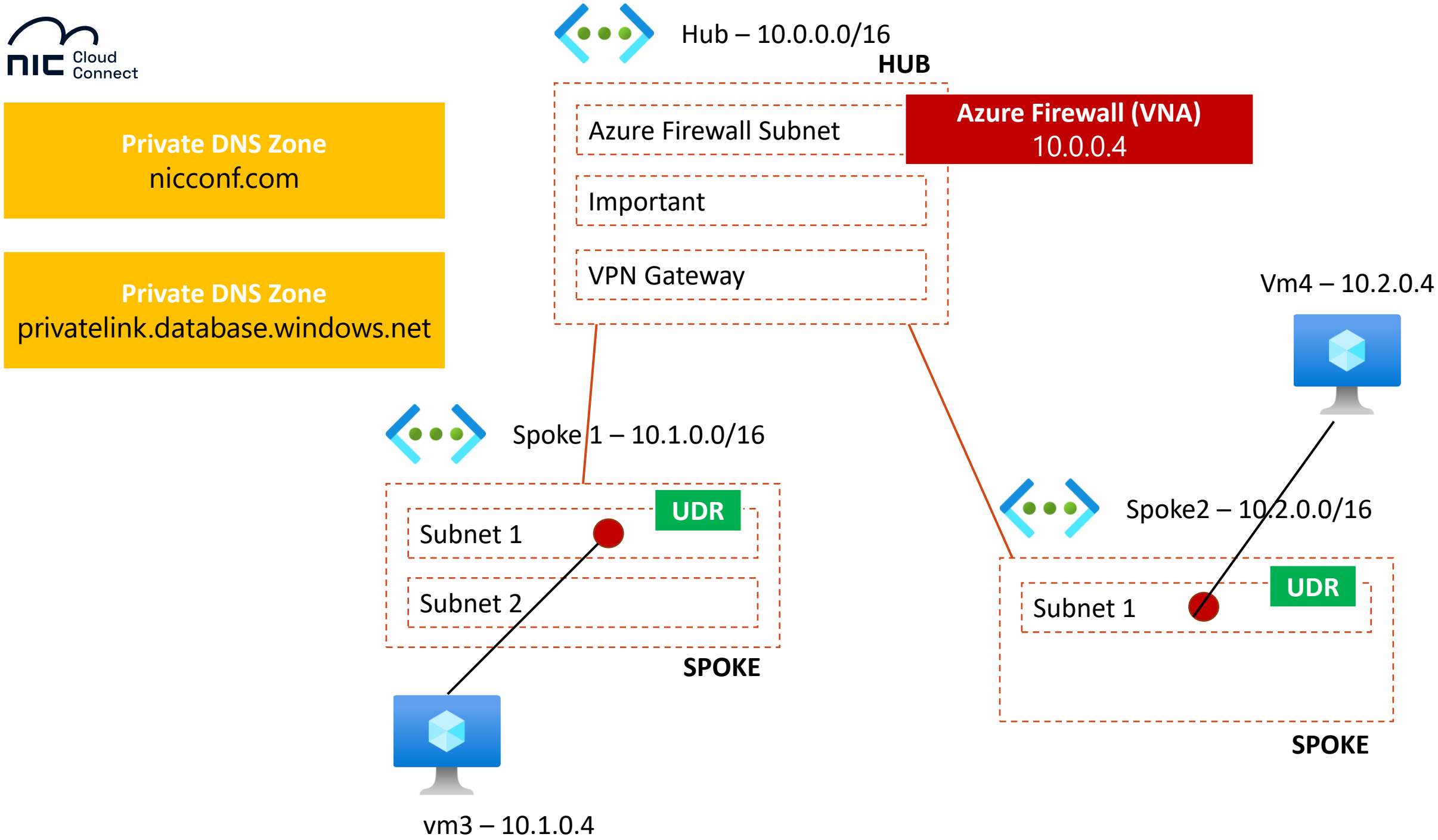
nic Cloud Connect

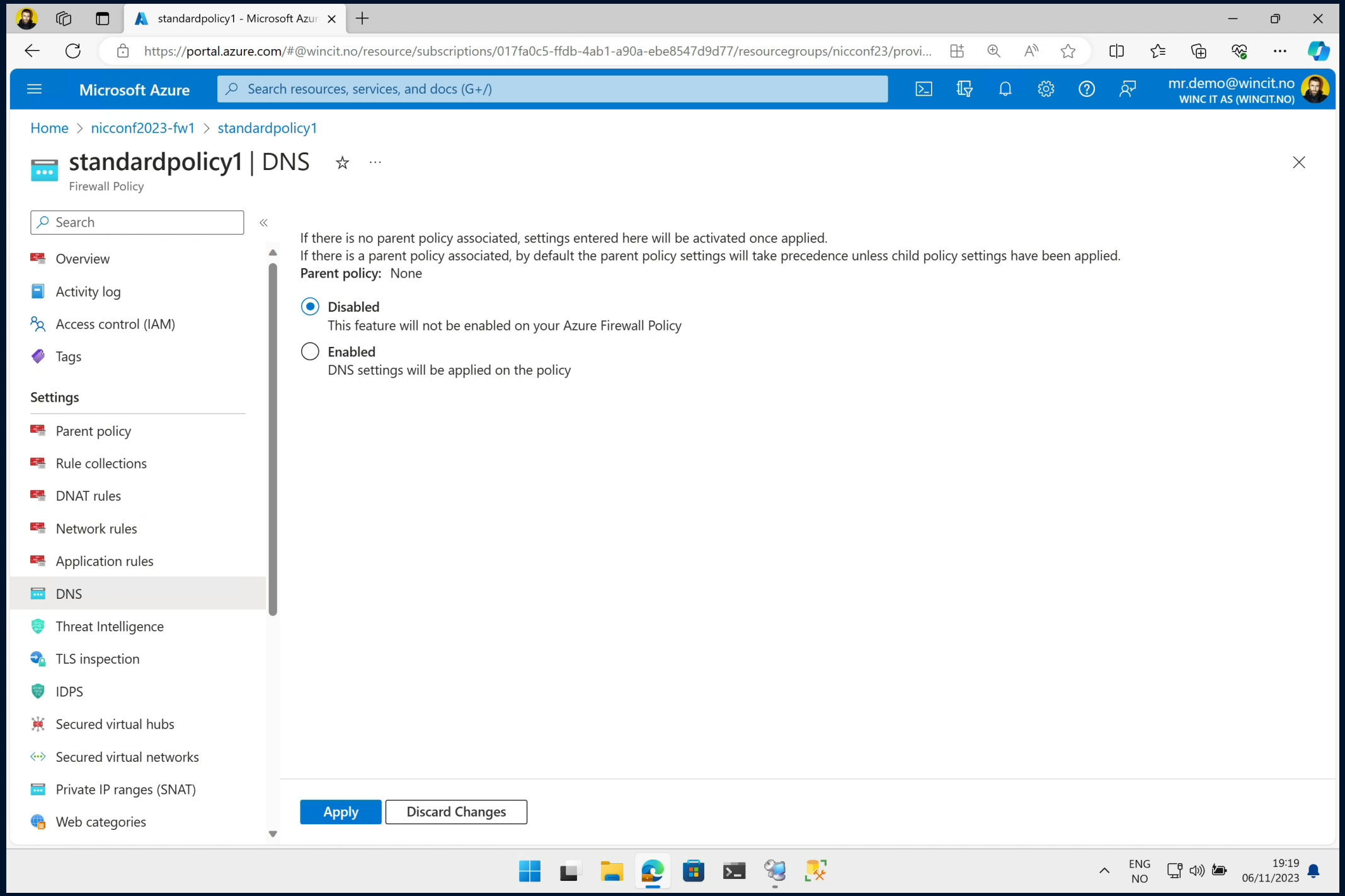
Hub-Spoke vnets (IP)

- Plan for peering
- Virtual Network Appliance (VNA) like Azure Firewall that can route your traffic between vnets.

Cloud Connect

Hub-spoke vnets (DNS)


Cloud Connect
Private DNS Zone
nicconf.com
Private DNS Zone
privatelink.database.windows.net
Hub – 10.0.0.0/16
HUB
Azure Firewall Subnet
Azure Firewall (VNA)
10.0.0.4
Important
VPN Gateway
Vm4 – 10.2.0.4
Spoke 1 – 10.1.0.0/16
UDR
Subnet 1
Subnet 2
SPOKE
Spoke2 – 10.2.0.0/16
UDR
Subnet 1
SPOKE
vm3 – 10.1.0.4


standardpolicy1 - Microsoft Azur
https://portal.azure.com/#@wincit.no/resource/subscriptions/017fa0c5-ffdb-4ab1-a90a-ebe8547d9d77/resourcegroups/nicconf23/provi...
Microsoft Azure
Search resources, services, and docs (G+/)
mr.demo@wincit.no
WINC IT AS (WINCIT.NO)
Home > nicconf2023-fw1 > standardpolicy1
standardpolicy1 | DNS
Firewall Policy
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Parent policy
Rule collections
DNAT rules
Network rules
Application rules
DNS
Threat Intelligence
TLS inspection
IDPS
Secured virtual hubs
Secured virtual networks
Private IP ranges (SNAT)
Web categories
If there is no parent policy associated, settings entered here will be activated once applied.
If there is a parent policy associated, by default the parent policy settings will take precedence unless child policy settings have been applied.
Parent policy: None
Disabled
This feature will not be enabled on your Azure Firewall Policy
Enabled
DNS settings will be applied on the policy
Apply
Discard Changes
ENG
NO
19:19
06/11/2023

nic Cloud Connect

Hub-Spoke vnets (DNS)

- Have a plan on how to manage your DNS zones
- Custom DNS server needed

Cloud Connect

That’s all folks!