CODE, DEPLOY AND MAINTAIN YOUR AZURE (DATA) INFRASTRUCTURE WITH CONFIDENCE

Have you been deploying your Azure databases and all connected resources through the portal?
Are you fed-up with clicking, weird resource naming and mostly, with having to deal with changes manually?

If you are working in Azure and you have anything to do with data and the infrastructure, this session is for you!

Azure Infrastructure as Code offers a plethora of possibilities, but the first time I checked it out, all I saw were Azure Resource Manager (ARM) templates. Hard to read, harder to write. They gave me headaches. It seems I wasn't the only one with that problem, because there are excellent tools to help you out! My favourite, and the one I'm using in this session is Terraform.

Now why is this presenter talking about this? I've deployed a number of customer environments with this language. Whenever there's a security update, like a new policy for example, I can deploy this to all customers in minutes. I'll only have to code this once and can easily deliver it many times, saving them time and money. Resources we can spend in other areas like ETL, ELT etc.

During the session, I'll demonstrate the basics of a data deployment, following the spirit of the Microsoft Well Architected Framework. I'll show you my way of working, the structure and and the end result. There is no need to try and photograph what's happening on screen, all the scripts will be available after the session.

Deploying your data infrastructure with confidence

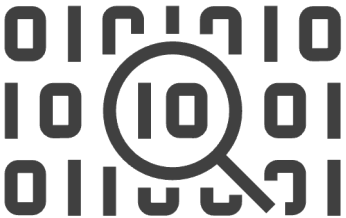
Reitse Eskens

axians

Code and slides are available through Github

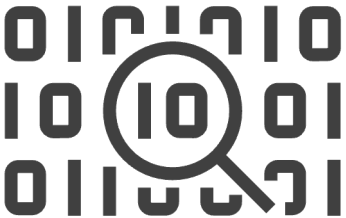
- The code is provided as is, without any warranty for your personal or company Azure Tenant
- Think, read, evaluate and then run
- Review the deployment before adding ANY data to it
- The code is intended as a demo and can function as a starting point for your own deployment. It is **not** production grade.

"IT Governance discovered 1,063 security incidents in 2022, which accounted for 480,014,323 breached records. That represents an 14.8% decrease in security incidents compared to 2021 (1,243)."



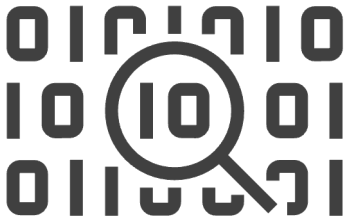
https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2022-408-million-breached-records

"The Dutch authority for personal data reported 21.151 data leaks and 1826 cyberattacks in 2022. In the last 5 years, 114,258 data leaks were reported."



https://www.autoriteitpersoonsgegevens.nl/uploads/2023-06/AP_Rapportage_datalekken_2022.pdf

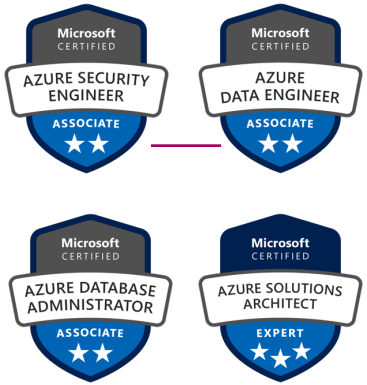
“Stay out of these statistics!”



Any security officer, any company, anywhere in the world

Reitse Eskens

Technical Consultant Axians Business Analytics



SQL: DBA, Performance tuning

Azure: architect, developer, admin

SQL Classes

Speaker

Photography, cycling, chronical volunteer

Twitter: @2meterDBA

LinkedIn: /in/reitseeskens/

Reitse.eskens@axians.com

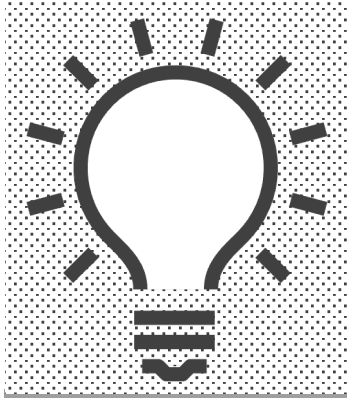
https://sqlreitse.com

Microsoft® MVP Most Valuable Professional

redgate 100 MOST INFLUENTIAL IN THE DATABASE COMMUNITY 2022

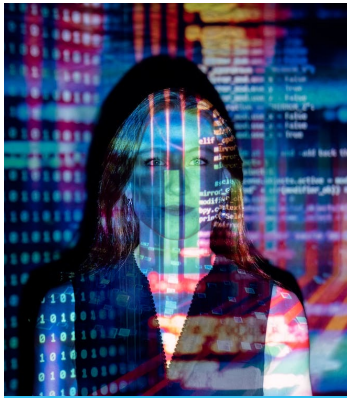
Microsoft CERTIFIED TRAINER MCT

Let’s start our journey

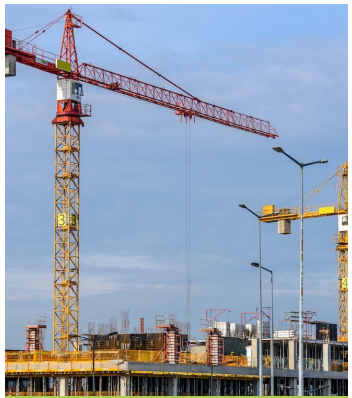


Big idea, let’s move this data solution to the cloud!

Architect for security



Learn and use infrastructure as code



Start building your solution

Architect for security

- More than just resource security
- More than user security
- Assume Breach, Zero Trust, Well Architected Framework

More then resource security

- Create policies to prevent unwanted changes or deployments
- Add locks to prevent accidental changes or deletes

axians

More than user security

- 2FA or MFA should be the default
- Enable Just in Time access
- Enable Priviliged Identity Management

axians

Assume breach, Zero Trust, WAF/CAF

- What can you do to prevent this breach?
- Hackers are constantly scanning for open ports
- Always deny traffic, unless
- Use the guidelines, don’t take them literally

Infrastructure as Code

- What is it?
- Which flavors are available
- Azure DevOps and GitHub
- Review before release

What is it?

- Easiest way to deploy resources in the cloud
- Repeatable without differences
- Configurable with parameters

Flavors

- ARM templates
- AZ Powershell commandlets
- Bicep, Azure Automation
- Terraform / Terragrunt
- Pulumi, Ansible, CrossPlane
- Bring your own hybrid

axians

Azure DevOps and GitHub

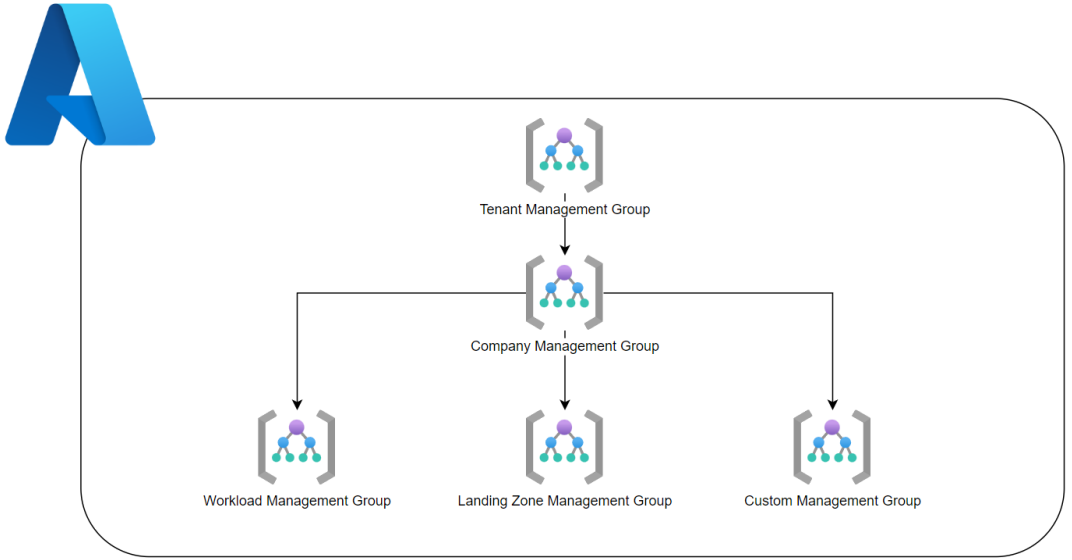
- Code repositories
- Kanban boards to support Agile and Scrum ways of working
- Pipelines to do the heavy lifting
- Pull requests to enforce review of the code before it gets released

Building your solution

- From the ground up
- Management group with policy
- From subscription to resourcegroup
- Networking first
- Private endpoints only
- No public access
- VPN and Bastion
- Encryption everywhere

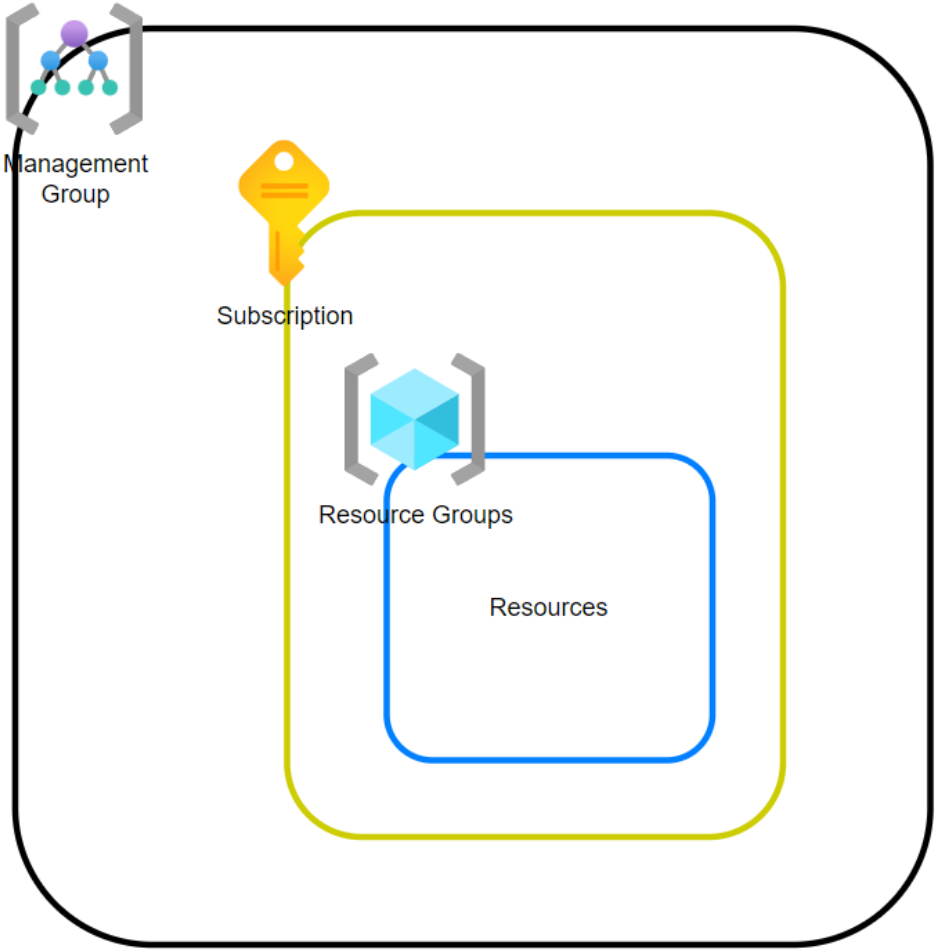
Management group with Policies

- Example policy:
  - restrict VM sizes
  - Allow west europe only



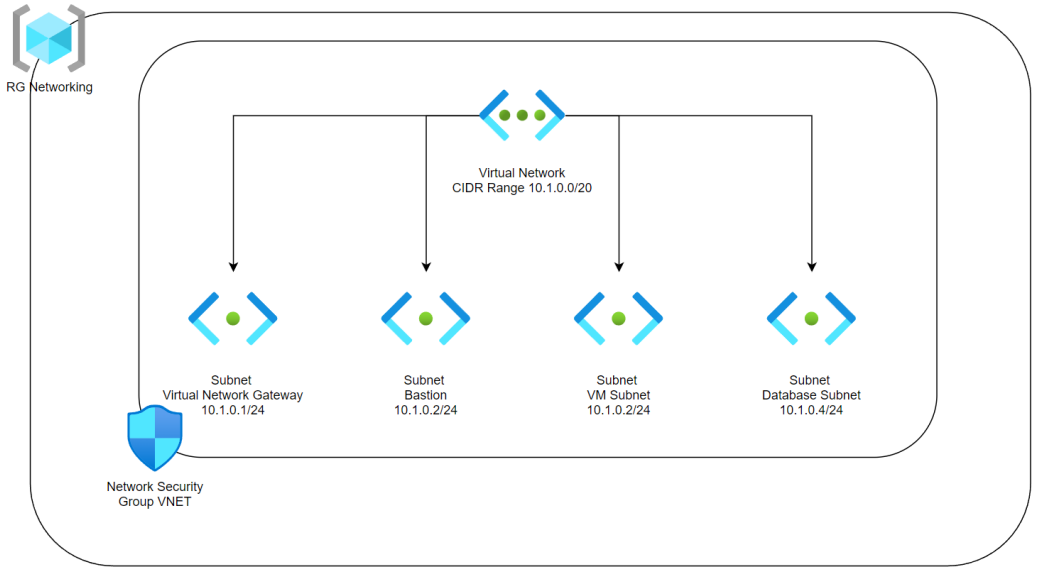
Management Group to Resource Group

- Remember permission inheritance
- One to many relationship



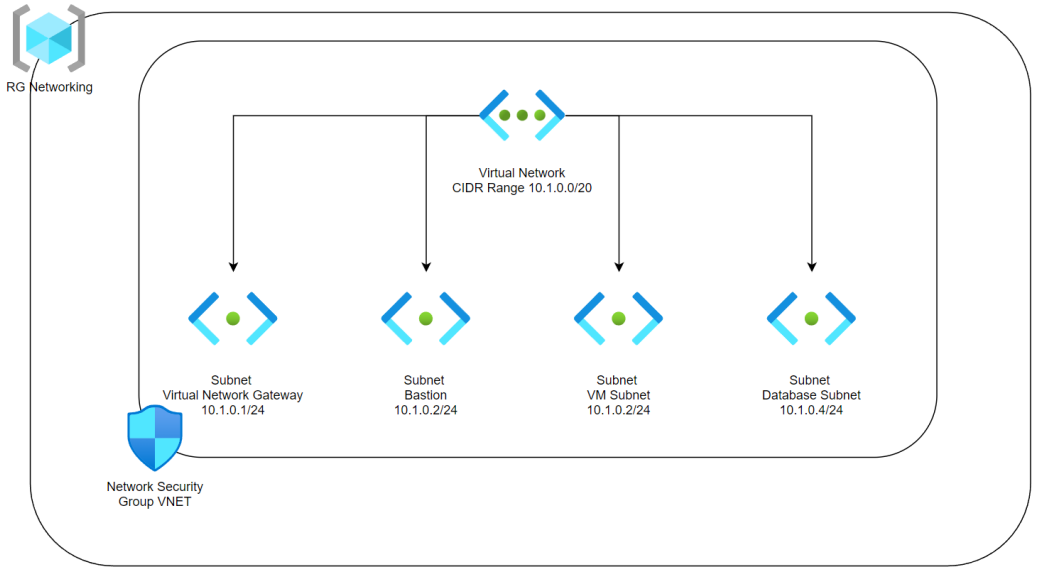
Networking first

- Local Virtual Network, think about your CIDR range
- Subnets matter!
- Secure subnets with a Network Security Group



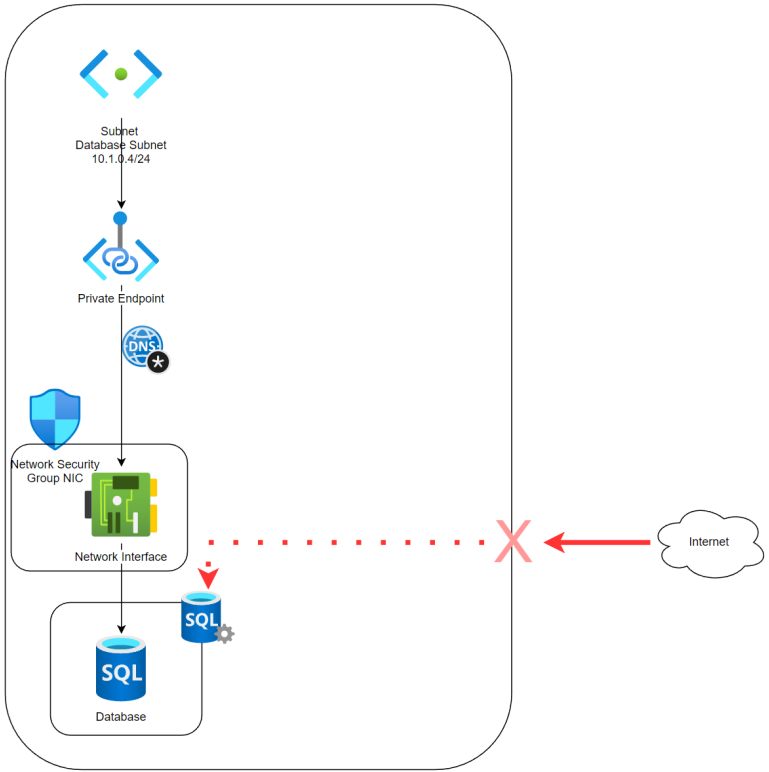
Networking first

- Secure each Network Interface Card and Private Endpoint with it's own NSG
- Add a useful description to each NSG rule



Private endpoints only

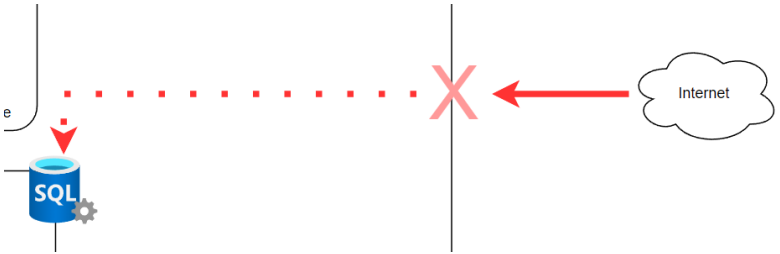
- Azure DNS entries
- Check if the ‘outside’ connection is denied



axians

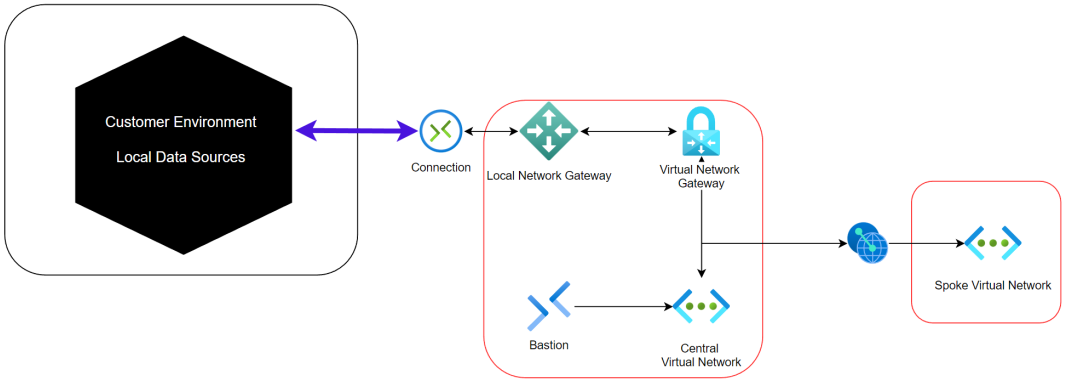
No public access

- Create a policy if you can
- Check each resource if this can be turned off
- Try and connect to each resource to check!



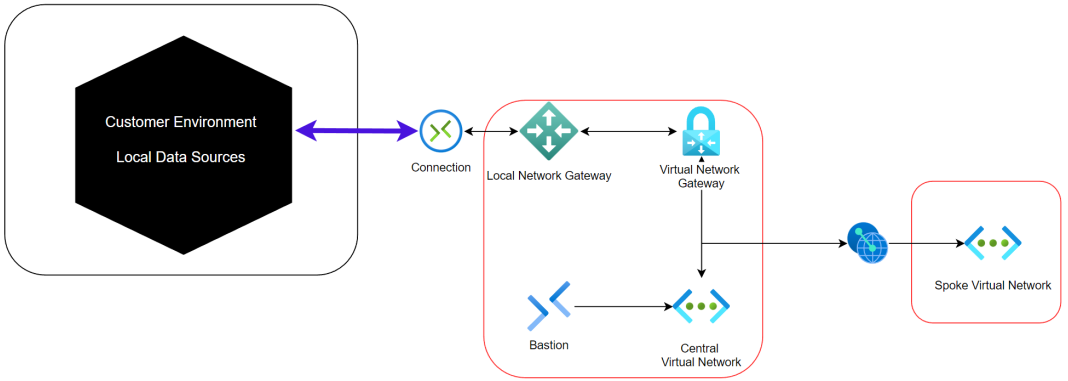
VPN and Bastion

- VPN is hard, but worth the effort
- Make sure you allow the correct CIDR Ranges
- You CAN lose the Azure Firewall if ALL traffic goes through the on-premises firewall.



VPN and Bastion

- Use Bastion if you need RDP access from the Azure Portal
- Always secure these resources with a Network Security Group
- Distance matters (Latency!)

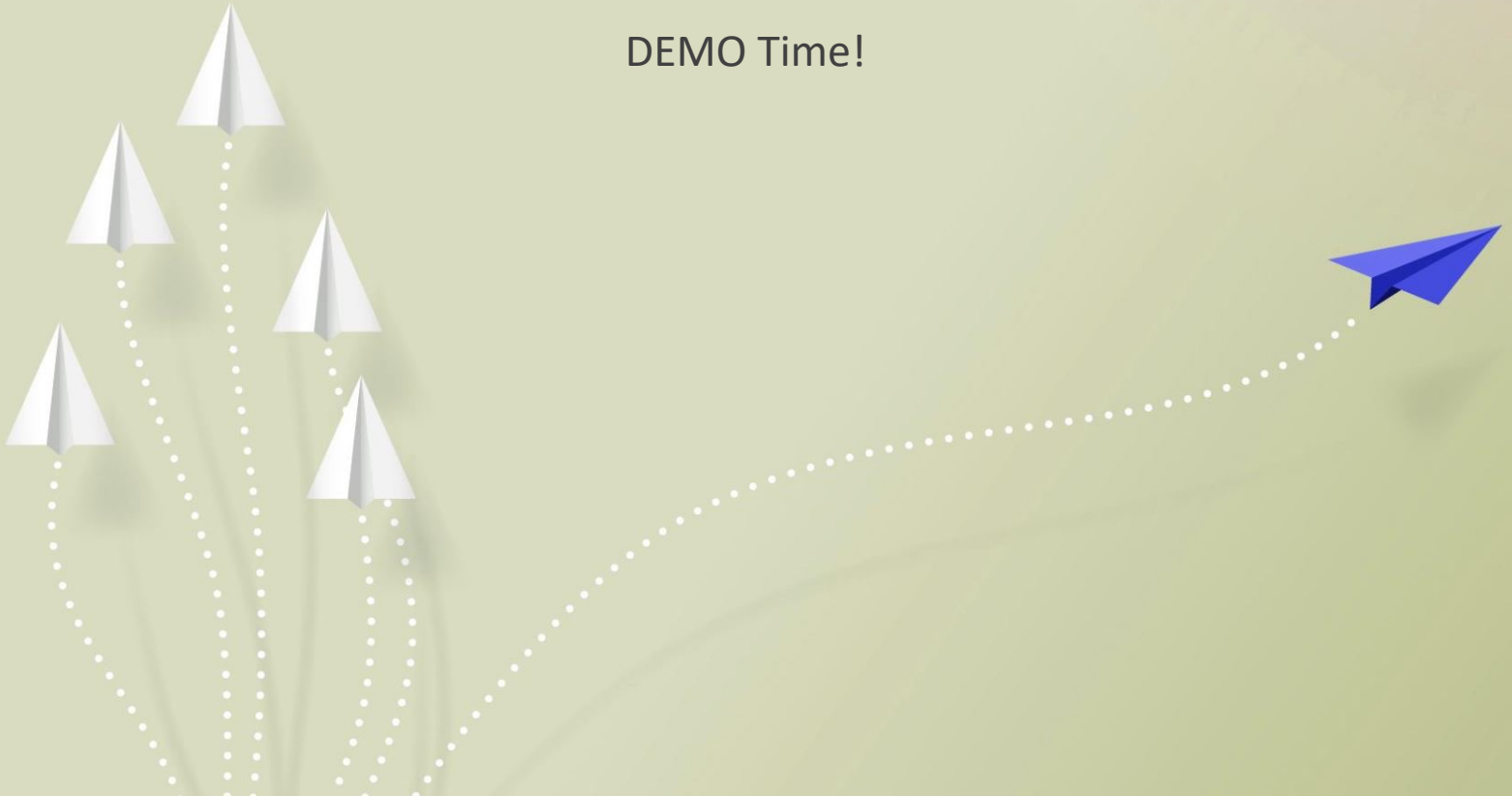


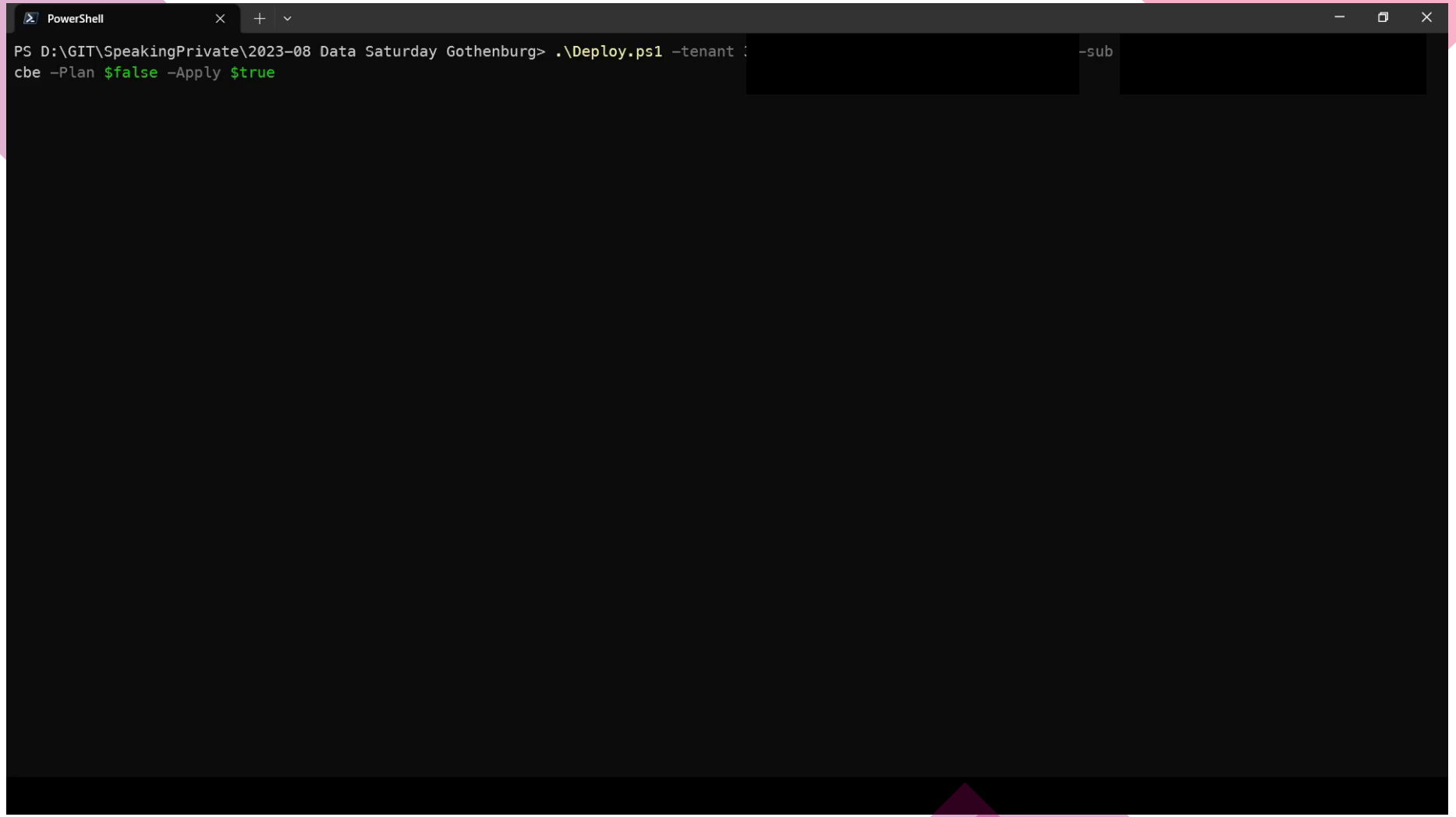
axians

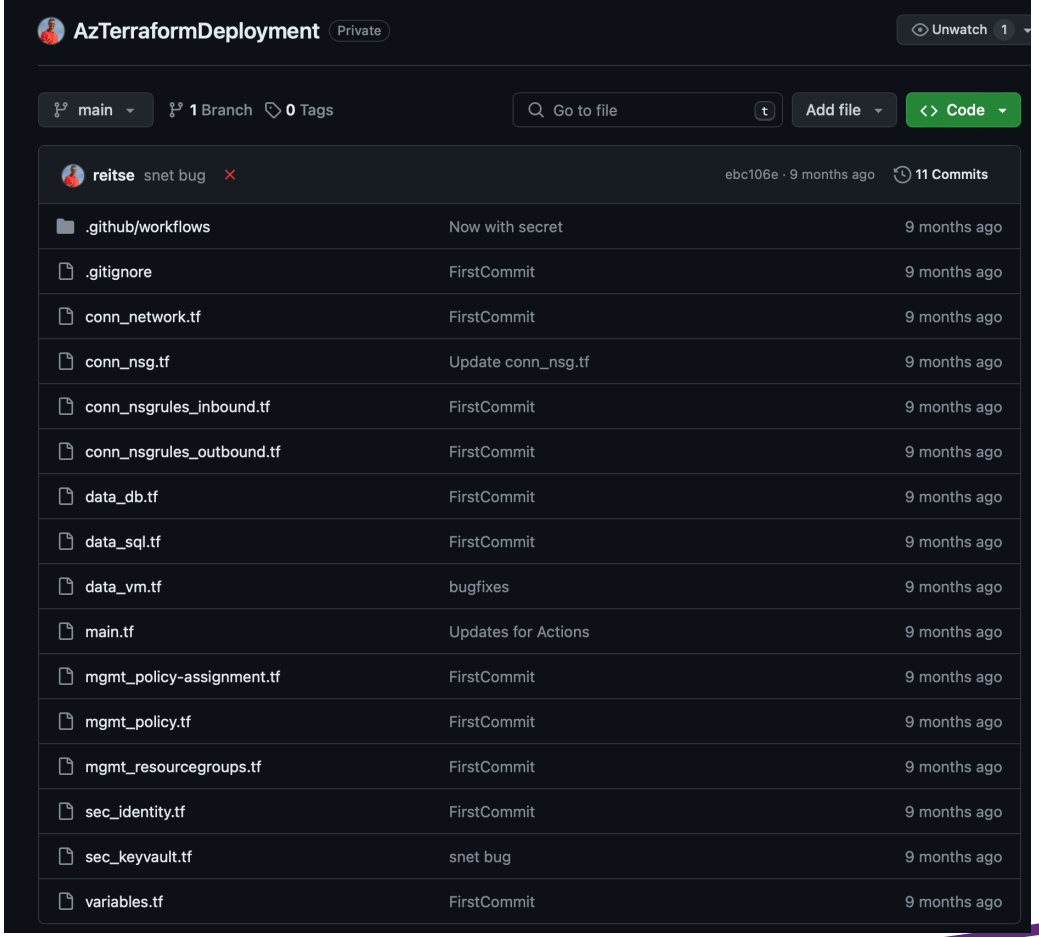
Encryption everywhere

- Databases have Transparent Database Encryption enabled by default
- Add your own certificate to add to the connection security
- Disk encryption is enabled by default, but make sure your Key Vault can store the keys

DEMO Time!



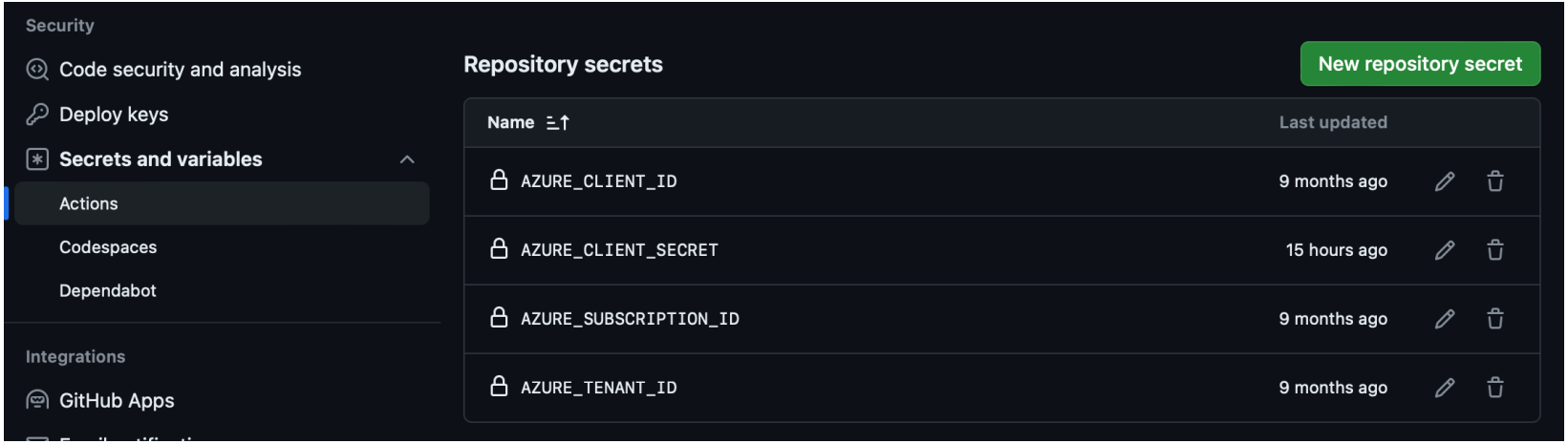

PowerShell
PS D:\GIT\SpeakingPrivate\2023-08 Data Saturday Gothenburg> .\Deploy.ps1 -tenant
-sub
cbe -Plan $false -Apply $true


AzTerraformDeployment
Private
Unwatch 1
main
1 Branch
0 Tags
Go to file
t
Add file
Code
reitse snet bug
ebc106e · 9 months ago
11 Commits
.github/workflows
Now with secret
9 months ago
.gitignore
FirstCommit
9 months ago
conn_network.tf
FirstCommit
9 months ago
conn_nsg.tf
Update conn_nsg.tf
9 months ago
conn_nsgrules_inbound.tf
FirstCommit
9 months ago
conn_nsgrules_outbound.tf
FirstCommit
9 months ago
data_db.tf
FirstCommit
9 months ago
data_sql.tf
FirstCommit
9 months ago
data_vm.tf
bugfixes
9 months ago
main.tf
Updates for Actions
9 months ago
mgmt_policy-assignment.tf
FirstCommit
9 months ago
mgmt_policy.tf
FirstCommit
9 months ago
mgmt_resourcegroups.tf
FirstCommit
9 months ago
sec_identity.tf
FirstCommit
9 months ago
sec_keyvault.tf
snet bug
9 months ago
variables.tf
FirstCommit
9 months ago

```yaml
name: 'Azure Terraform deployment'

on:
  push:
    branches: [ "main" ]
  pull_request:

permissions:
      id-token: write
      contents: read

jobs:
  Windows-latest:
      runs-on: windows-latest
      steps:
        - name: 'Azure Login'
          uses: azure/login@v1
          with:
            client-id: ${{ secrets.AZURE_CLIENT_ID }}
            tenant-id: ${{ secrets.AZURE_TENANT_ID }}
            subscription-id: ${{ secrets.AZURE_SUBSCRIPTION_ID }}
            enable-AzPSSession: true

        - name: 'Get resource group with PowerShell action'
          uses: azure/powershell@v1
          with:
             inlineScript: |
               Get-AzResourceGroup
               az account set -s ${{ secrets.AZURE_SUBSCRIPTION_ID }}
               az group create --location "westeurope" --name rgtfdeployment
```

```yaml
on:
  push:
    branches: [ "main" ]
  pull_request:
```

```
with:
  client-id: ${{ secrets.AZURE_CLIENT_ID }}
  tenant-id: ${{ secrets.AZURE_TENANT_ID }}
  subscription-id: ${{ secrets.AZURE_SUBSCRIPTION_ID }}
  enable-AzPSSession: true

name: 'Get resource group with PowerShell action'
uses: azure/powershell@v1
with:
  inlineScript: |
    Get-AzResourceGroup
    az account set -s ${{ secrets.AZURE_SUBSCRIPTION_ID }}
    if(az group exists --name rgtfdeployment)
    {
      write-host "Resource Exists, moving on" -Foregroundcolor green
    }
```


Security
Code security and analysis
Deploy keys
Secrets and variables
Actions
Codespaces
Dependabot
Integrations
GitHub Apps
Repository secrets
New repository secret
Name
Last updated
AZURE_CLIENT_ID
9 months ago
AZURE_CLIENT_SECRET
15 hours ago
AZURE_SUBSCRIPTION_ID
9 months ago
AZURE_TENANT_ID
9 months ago


terraform.yml
on: push
Windows-latest
1m 3s
terraform

Home >

Resource groups

Default Directory

+ Create | Manage view | Refresh | Export to CSV | Open query | Assign tags

Filter for any field... | Subscription equals **all** | Location equals **all** | Deployment equals **Terraform** | Add filter

Showing 1 to 4 of 4 records.

Name	Subscription
rg_connectivity	Visual Studio Enterprise-abonnement
rg_data	Visual Studio Enterprise-abonnement
rg_identity	Visual Studio Enterprise-abonnement
rg_security	Visual Studio Enterprise-abonnement

Tags (edit)

Cost_Center : TBD

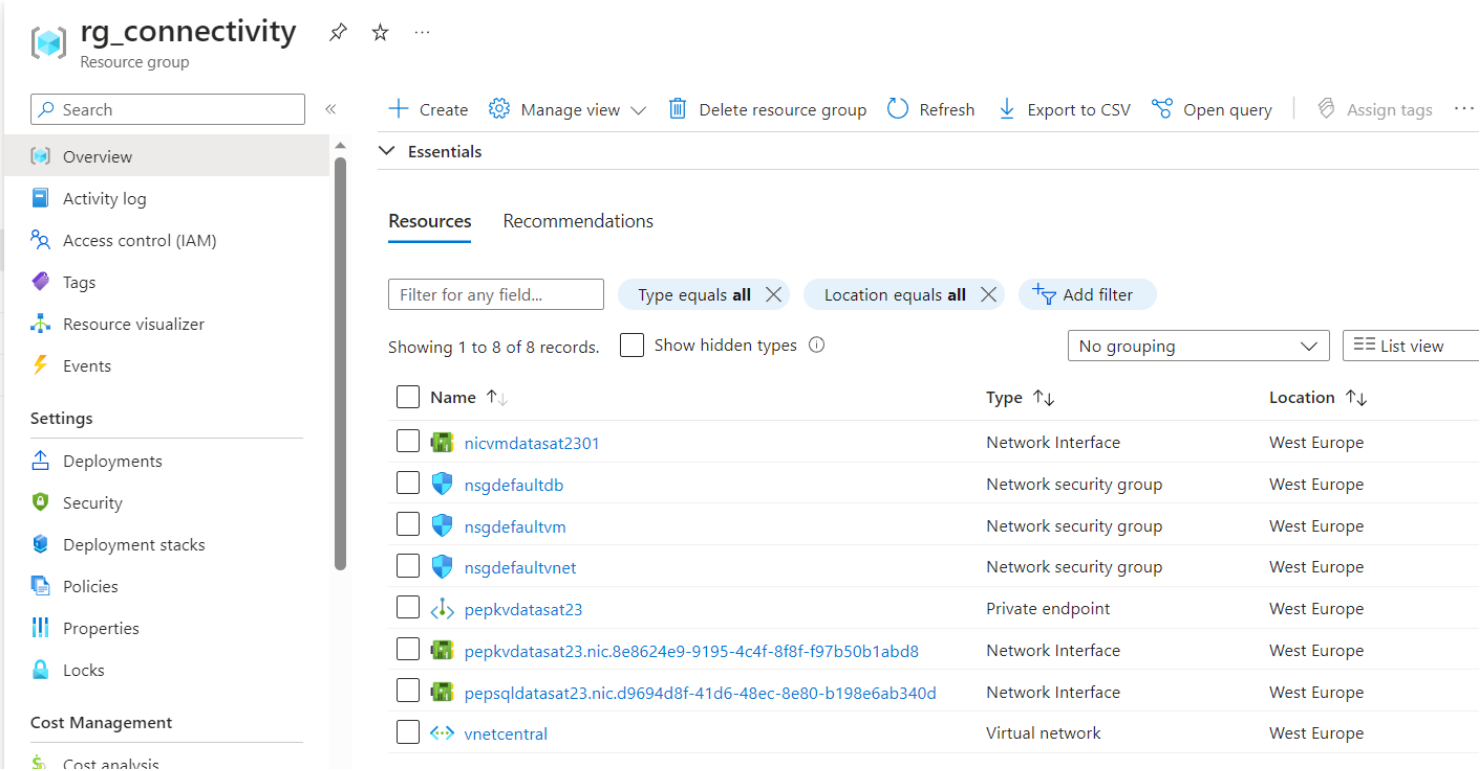
Deployment : Terraform

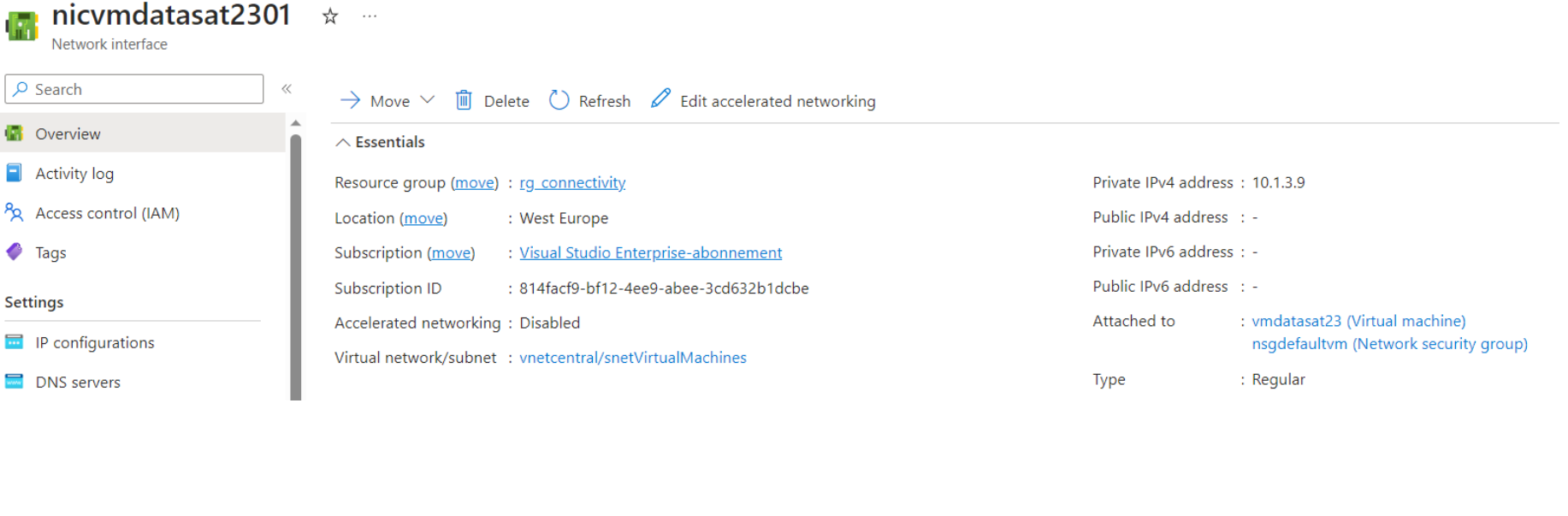
Environment : Data Saturday Demo

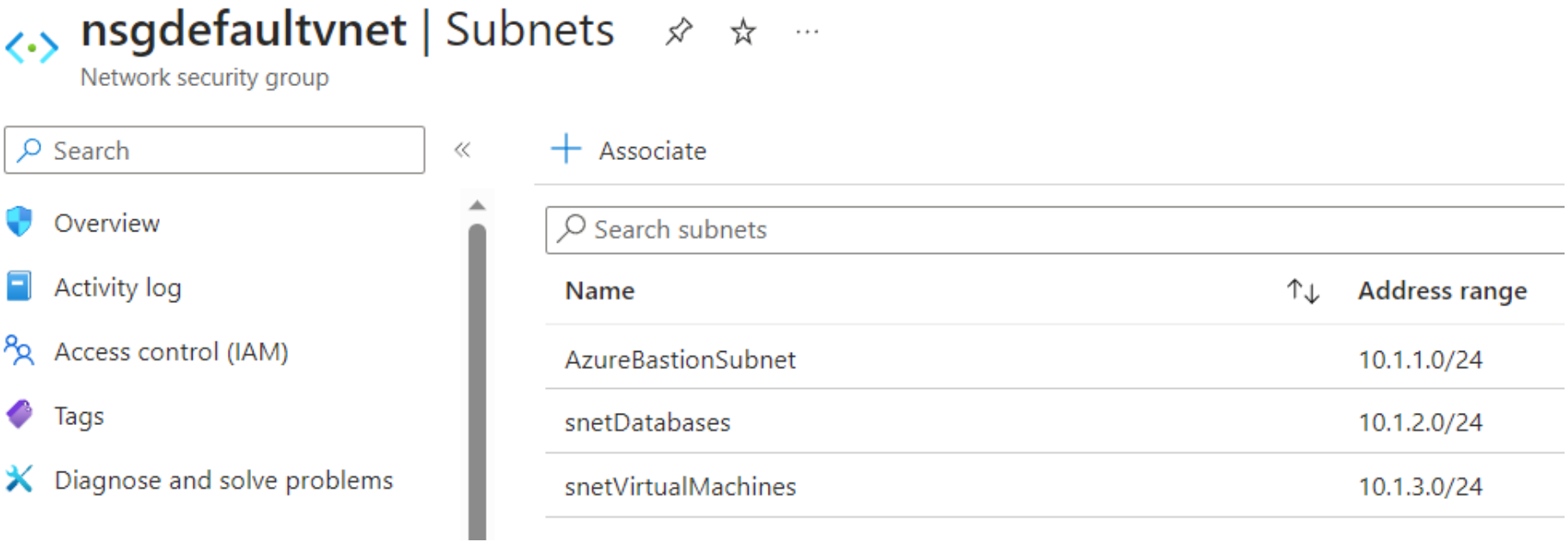
Landing_Zone : Analytics

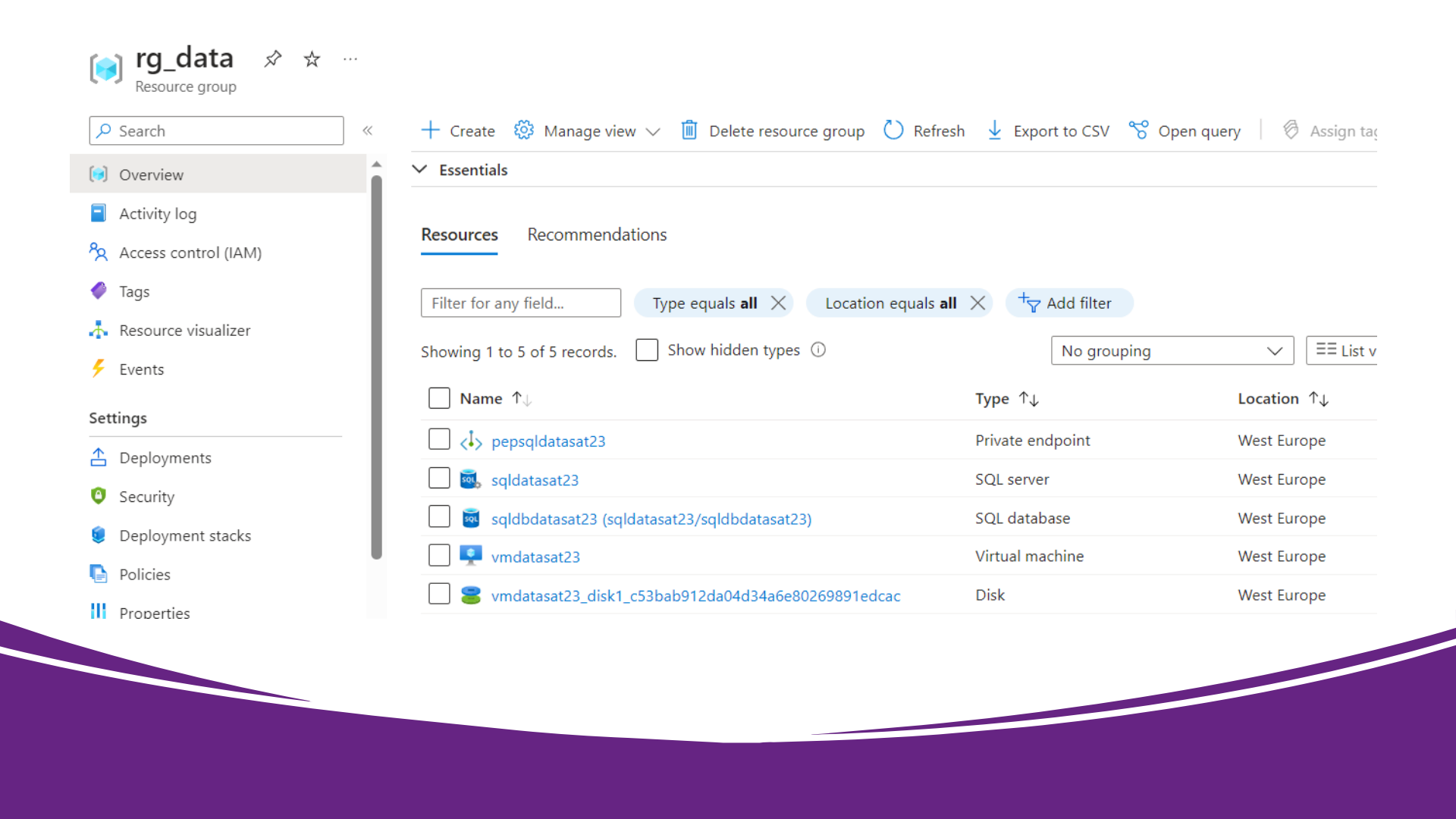
Owner : Reitse Eskens

Less


rg_connectivity
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Cost Management
Cost analysis
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Essentials
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 8 of 8 records.
Show hidden types
No grouping
List view
Name
Type
Location
nicvmdatasat2301 Network Interface West Europe
nsgdefaultdb Network security group West Europe
nsgdefaultvm Network security group West Europe
nsgdefaultvnet Network security group West Europe
pepkvdatasat23 Private endpoint West Europe
pepkvdatasat23.nic.8e8624e9-9195-4c4f-8f8f-f97b50b1abd8 Network Interface West Europe
pepsqldatasat23.nic.d9694d8f-41d6-48ec-8e80-b198e6ab340d Network Interface West Europe
vnetcentral Virtual network West Europe


nicvmdatasat2301
Network interface
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
IP configurations
DNS servers
Move
Delete
Refresh
Edit accelerated networking
Essentials
Resource group (move) : rg_connectivity
Location (move) : West Europe
Subscription (move) : Visual Studio Enterprise-abonnement
Subscription ID : 814facf9-bf12-4ee9-abee-3cd632b1dcbe
Accelerated networking : Disabled
Virtual network/subnet : vnetcentral/snetVirtualMachines
Private IPv4 address : 10.1.3.9
Public IPv4 address : -
Private IPv6 address : -
Public IPv6 address : -
Attached to : vmdatasat23 (Virtual machine)
nsgdefaultvm (Network security group)
Type : Regular


nsgdefaultvnet | Subnets
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Associate
Search subnets
Name
Address range
AzureBastionSubnet
10.1.1.0/24
snetDatabases
10.1.2.0/24
snetVirtualMachines
10.1.3.0/24


rg_data
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tag
Essentials
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 5 of 5 records.
Show hidden types
No grouping
List v
Name
Type
Location
pepsqldatasat23
Private endpoint
West Europe
sqldatasat23
SQL server
West Europe
sqldbdatasat23 (sqldatasat23/sqldbdatasat23)
SQL database
West Europe
vmdatasat23
Virtual machine
West Europe
vmdatasat23_disk1_c53bab912da04d34a6e80269891edcac
Disk
West Europe

sqldatasat23 | Networking

SQL server

Search

Properties

Locks

Data management

Backups

Deleted databases

Failover groups

Import/Export history

Security

Networking

Microsoft Defender for Cloud

Transparent Data Encryption

Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource th access this resource. Learn more

Public network access

- ○ Disable
- ◉ Selected networks

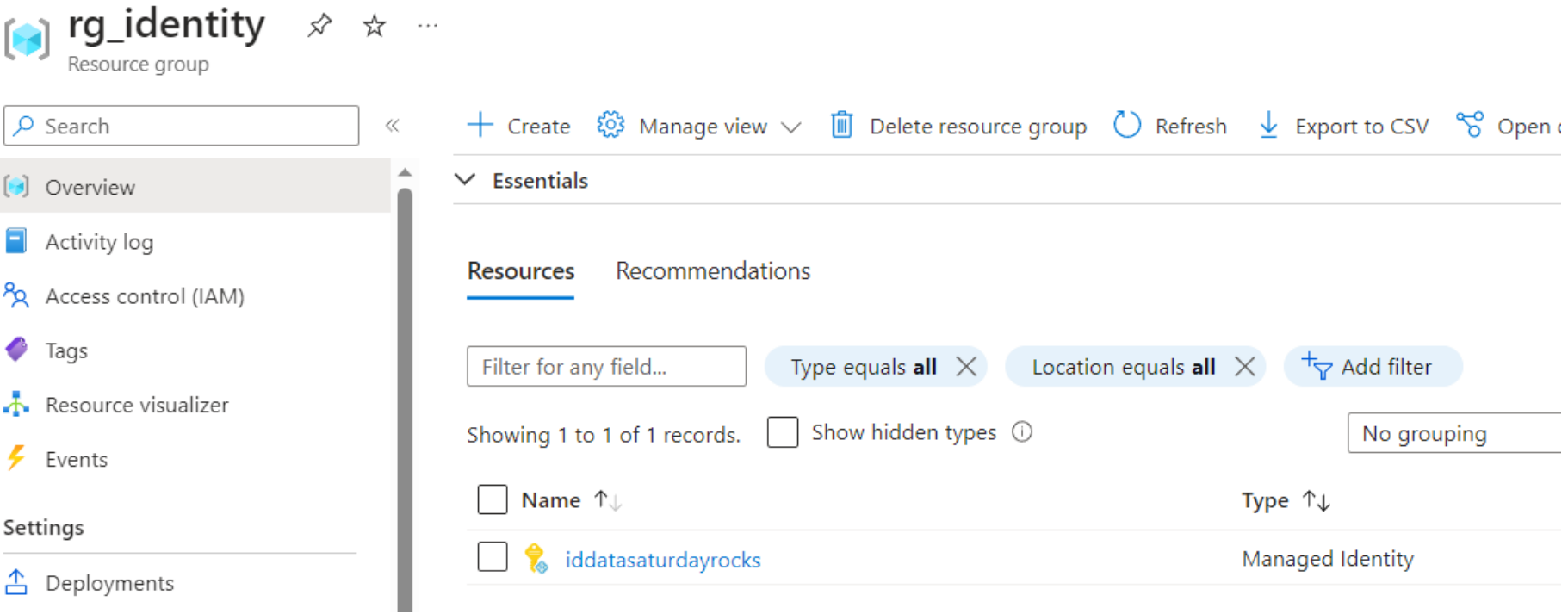
Connections from the IP addresses configured in the Firewall rules section bel more

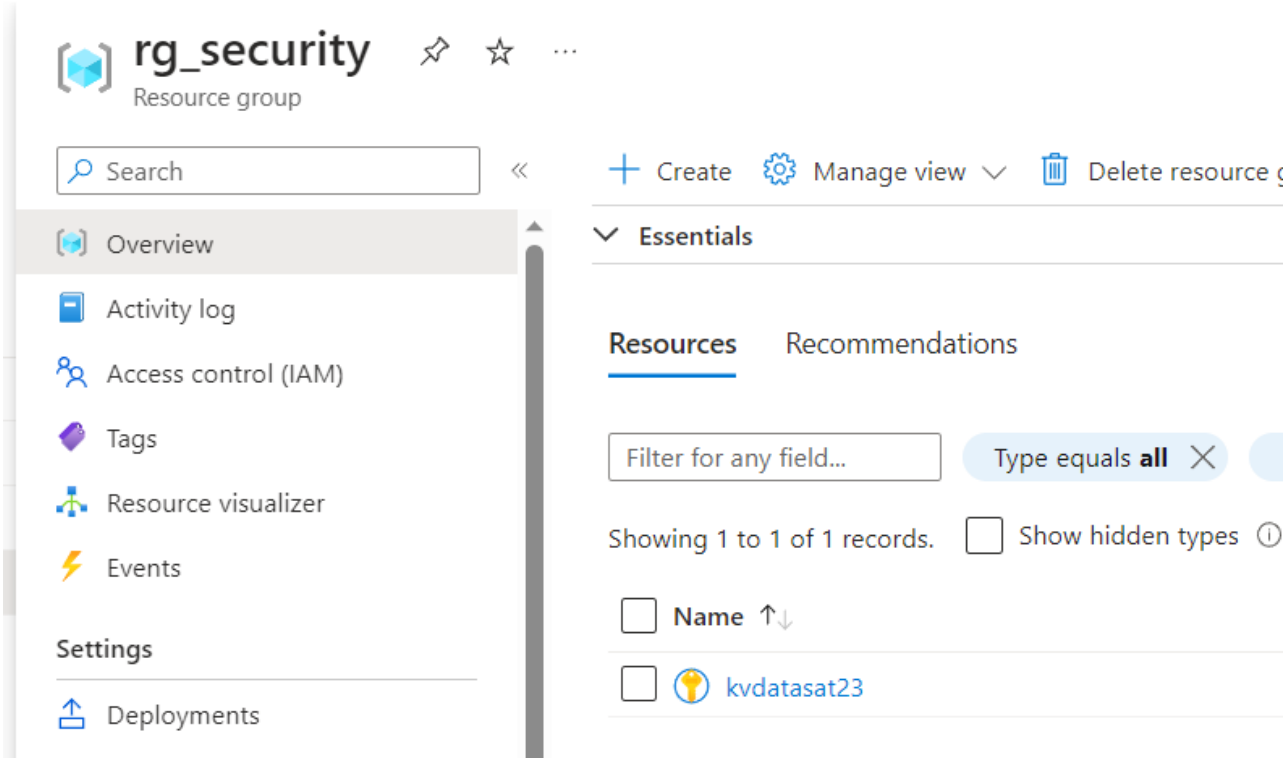
Virtual networks

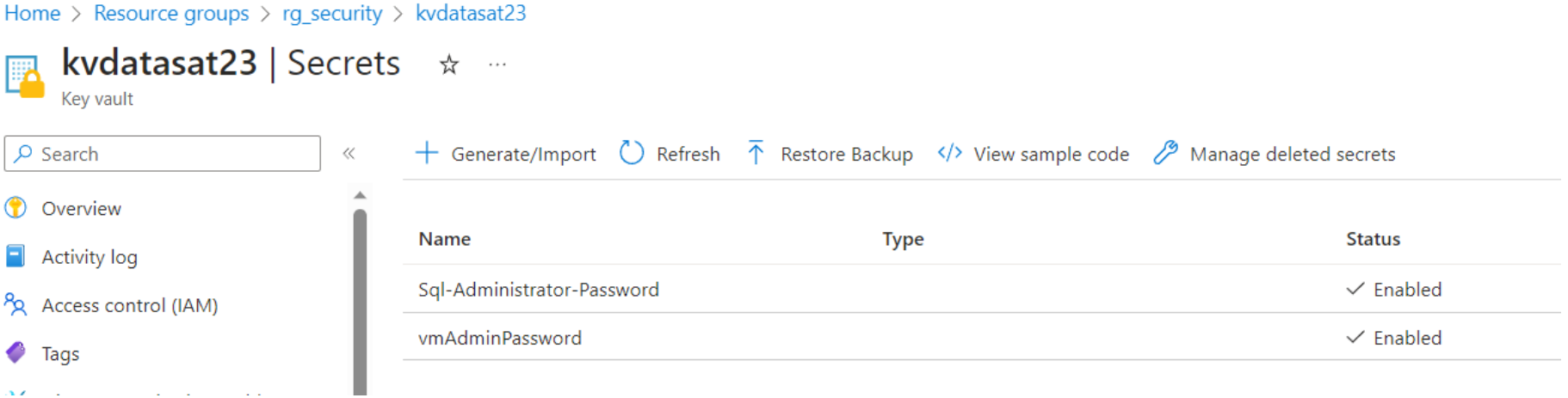
Allow virtual networks to connect to your resource using service endpoints. Learn more

+ Add a virtual network rule

Rule	Virtual network	Subnet	Address range	Endpoint status
sqldatasat23-vnet-rule	vnetcentral	snetVirtualMachines	10.1.3.0/24	Succeeded


rg_identity
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Create
Manage view
Delete resource group
Refresh
Export to CSV
Essentials
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 1 of 1 records.
Show hidden types
No grouping
Name
Type
iddatasaturdayrocks
Managed Identity


rg_security
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Create
Manage view
Delete resource
Essentials
Resources
Recommendations
Filter for any field...
Type equals all
Showing 1 to 1 of 1 records.
Show hidden types
Name
kvdatasat23


Home > Resource groups > rg_security > kvdatasat23
kvdatasat23 | Secrets
Key vault
Search
Overview
Activity log
Access control (IAM)
Tags
Generate/Import
Refresh
Restore Backup
View sample code
Manage deleted secrets
Name
Type
Status
Sql-Administrator-Password
Enabled
vmAdminPassword
Enabled

Session evaluation

Github Repo