

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 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

August 2023, Gothenburg

Data Saturday Gothenburg 2023

Sponsors



The after-party sponsor



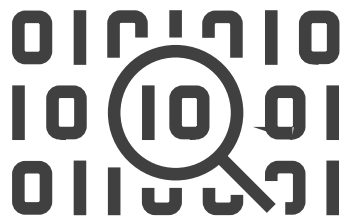
Tabular Editor



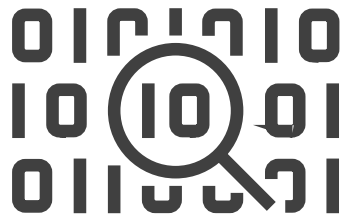
Code and slides are available through Github

- ▶ 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.

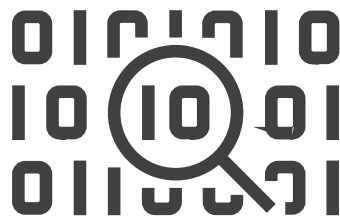
"IT Governance discovered 1,063 security incidents in 2022, which accounted for 480,014,323 breached records. That represents an 14.8% decrease in security incidents compared to 2021 (1,243)."



"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."



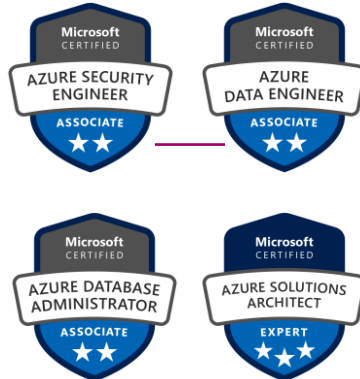
"Stay out of these statistics!"



Any security officer, any company, anywhere in the world

Reitse Eskens

Technical Consultant Axians Business Analytics

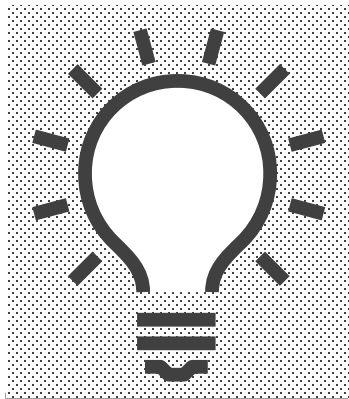


SQL: DBA, Performance tuning
Azure: architect, developer, admin
SQL Classes
Public speaker
Photography, cycling, chronicl
volunteer

Twitter: @2meterDBA
LinkedIn: /in/reitseeskens/
Reitse.eskens@axians.com
<https://sqlreitse.com>



Let's start a story



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 than resource security

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

More than user security

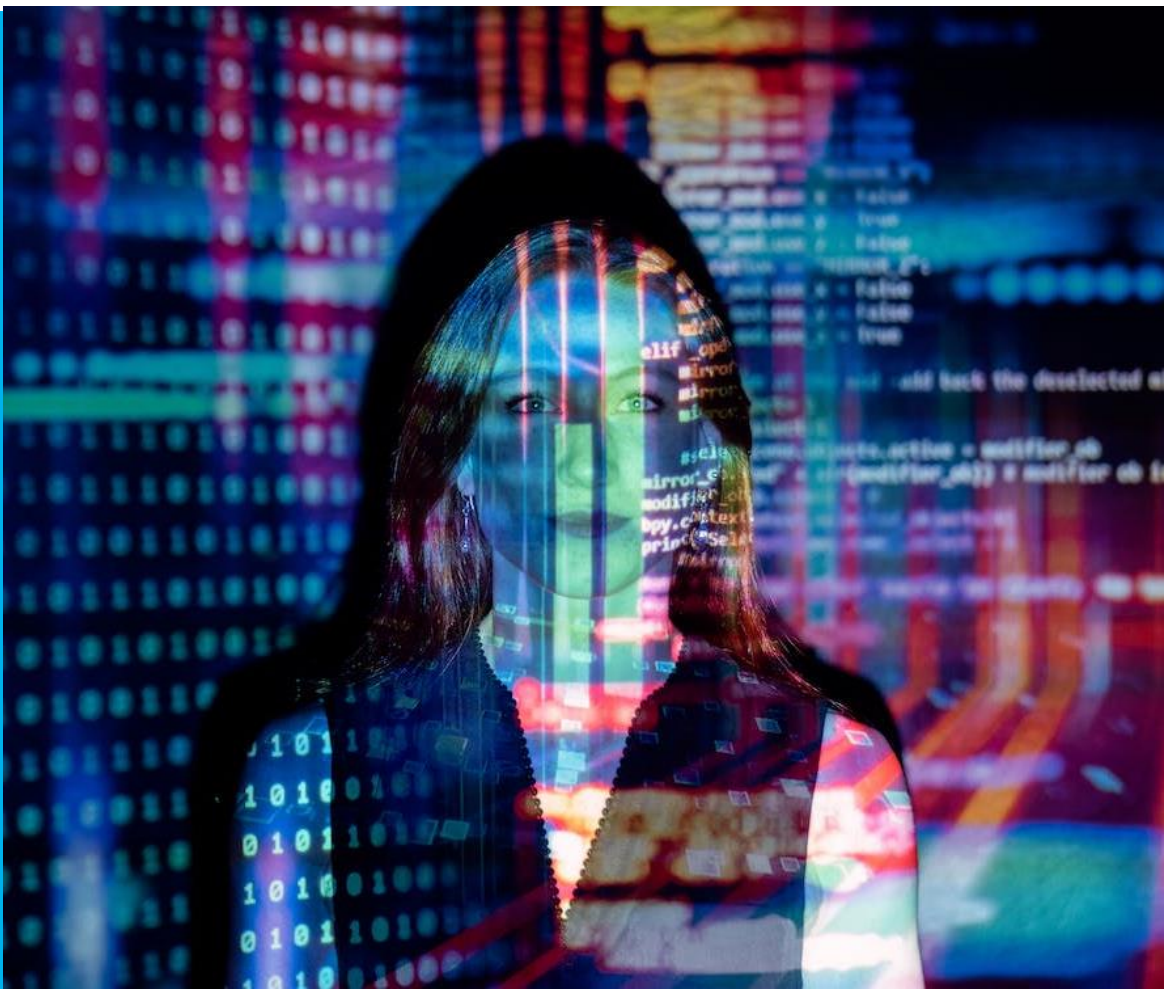
- 2FA or MFA should be the default
- Enable Just in Time access
- Enable Privileged Identity Management
- Educate your key users
- Enforce security tools like Key Vault

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
- Terraform / Terragrunt
- Bring your own hybrid

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

The demos

- Created in Terraform, with PowerShell acting as support act
- Not better or worse than Bicep, just different
- No DevOps included to prevent information overload

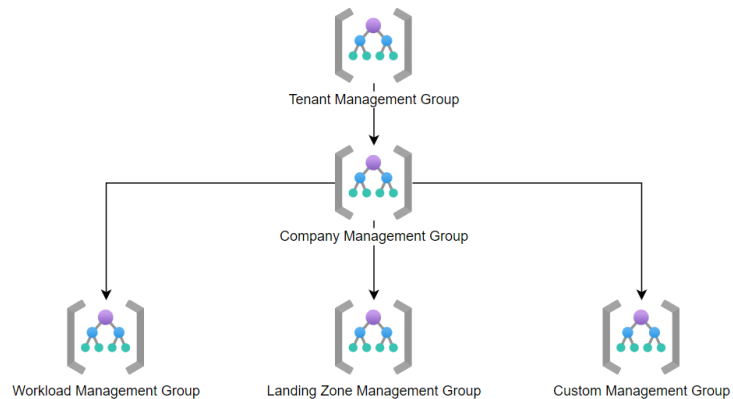
Building your solution

- 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

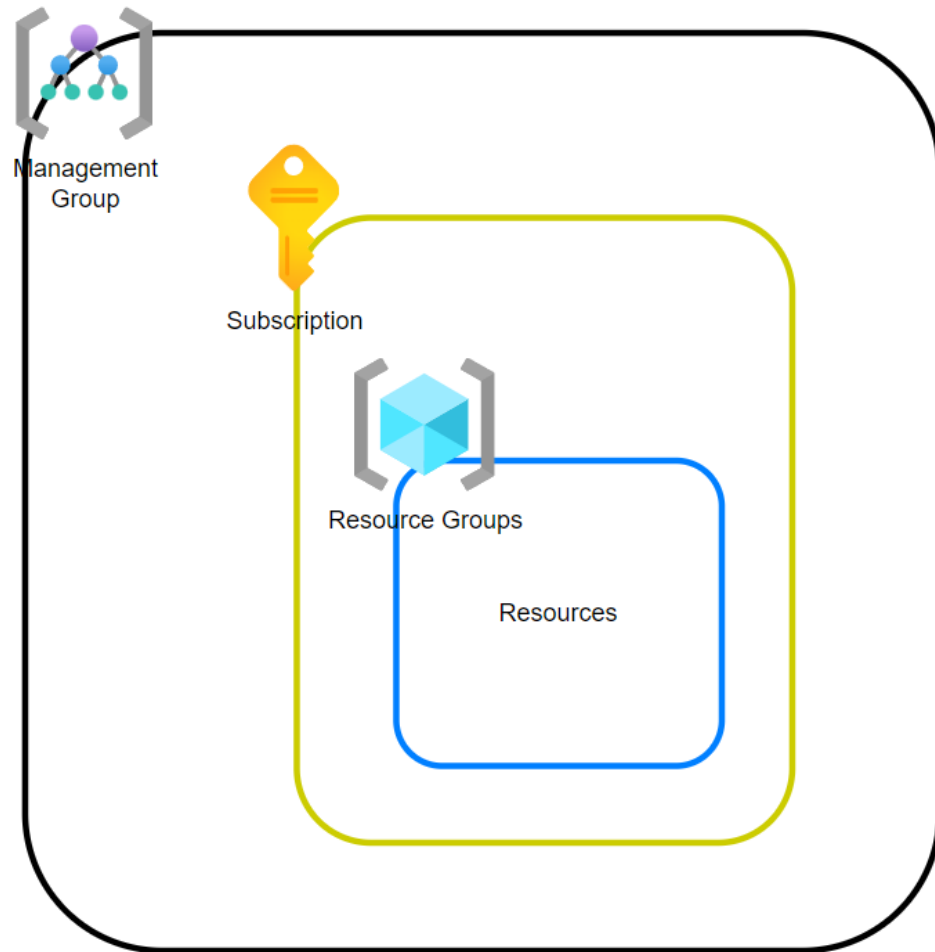


Management group with Policies

- Example policy: restrict VM sizes

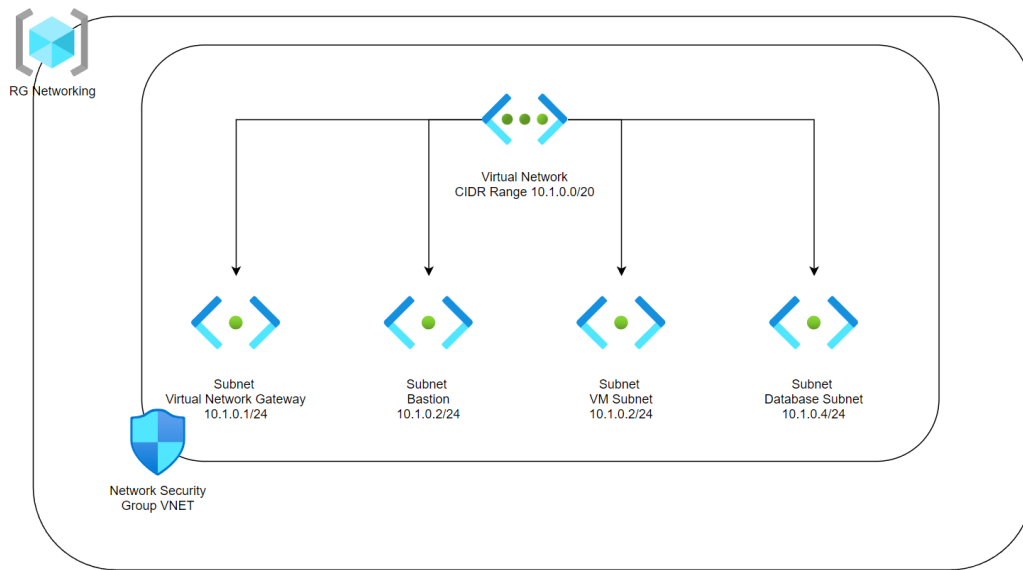


Subscription to Resource Group



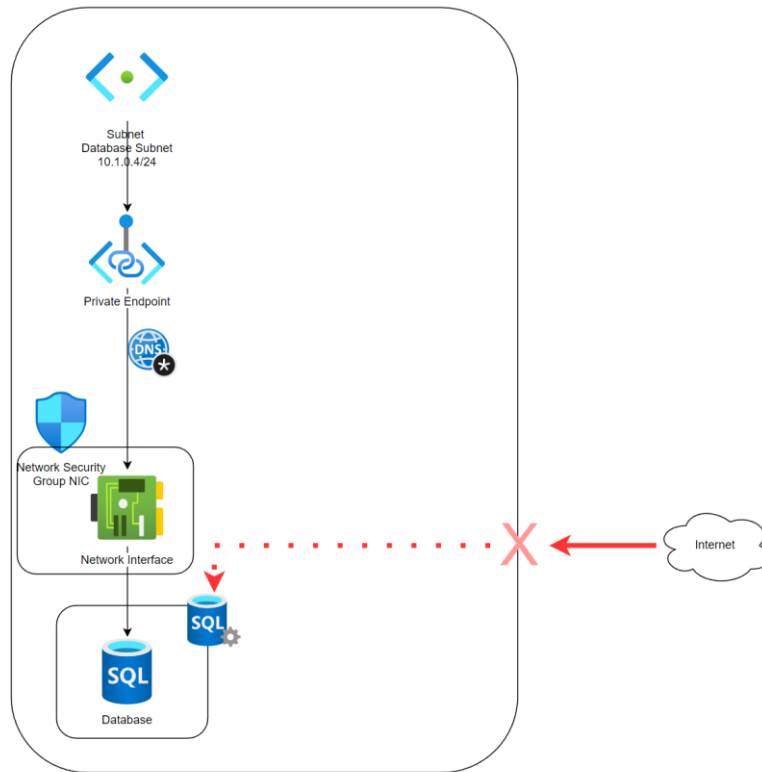
Networking first

- Local Virtual Network, think about your CIDR range
- Subnets matter!
- Secure the subnet with a Network Security Group
- Secure each Network Interface Card and Private Endpoint with it's own NSG
- Add a useful description to each NSG rule



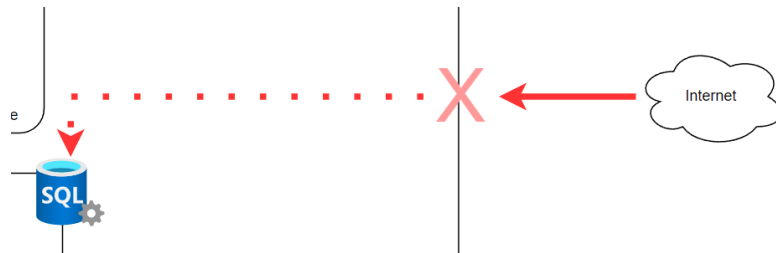
Private endpoints only

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



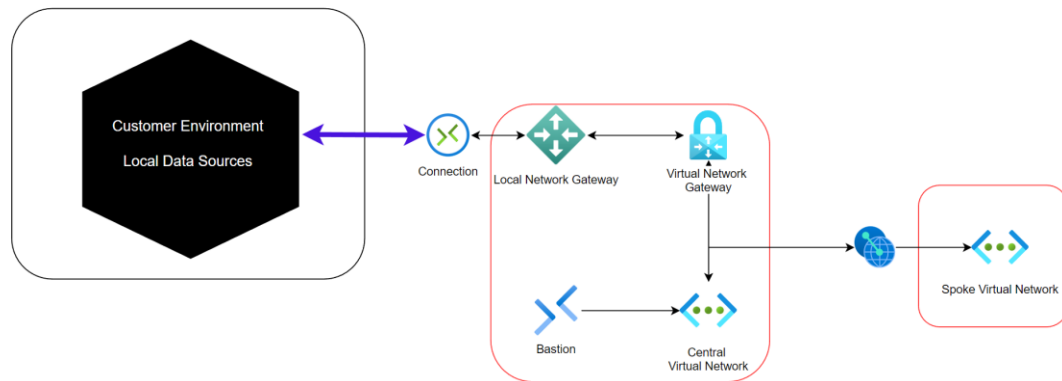
No public access

- 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

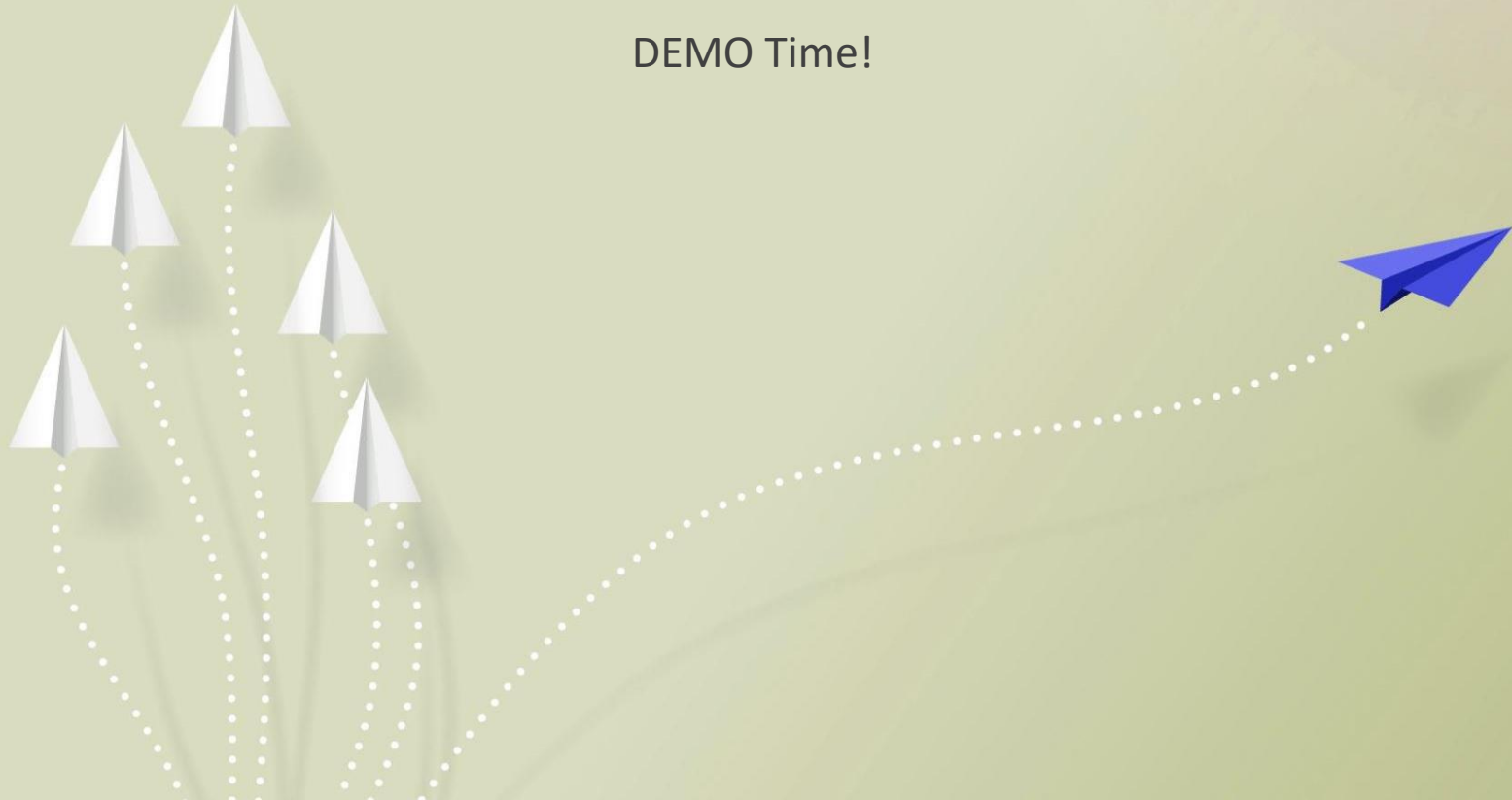
- VPN is hard, but worth the effort
- Make sure you allow the correct CIDR Ranges
- You CAN lose the Azure Firewall if ALL traffic goes through the on-premises firewall.
- Use Bastion if you need RDP access from the Azure Portal
- Always secure these resources with a Network Security Group



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!



[Home](#) >

Resource groups ...

Default Directory

[+](#) Create [⚙️](#) Manage view [v](#) [🔄](#) 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



Create



Manage view



Delete resource group



Refresh



Export to CSV



Open query



Assign tags



Overview



Activity log



Access control (IAM)



Tags



Resource visualizer



Events

Settings



Deployments



Security



Deployment stacks



Policies



Properties



Locks

Cost Management



Cost analysis

Essentials

Resources

Recommendations

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



pepkvdatsat23

Private endpoint

West Europe



pepkvdatsat23.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



Move ▾



Delete



Refresh



Edit accelerated networking



Overview



Activity log



Access control (IAM)



Tags

Settings



IP configurations



DNS servers

^ 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



Associate



Overview



Activity log



Access control (IAM)



Tags



Diagnose and solve problems




Name	↑↓	Address range
AzureBastionSubnet		10.1.1.0/24
snetDatabases		10.1.2.0/24
snetVirtualMachines		10.1.3.0/24




 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

Type equals **all** 






Location equals **all** 

 Add filter

Showing 1 to 5 of 5 records. ☐ Show hidden types 

No grouping 

 List view

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/>  pepsqldatasat23	Private endpoint	West Europe
<input type="checkbox"/>  sqldatasat23	SQL server	West Europe
<input type="checkbox"/>  sqldbdatasat23 (sqldatasat23/sqldbdatasat23)	SQL database	West Europe
<input type="checkbox"/>  vmdatasat23	Virtual machine	West Europe
<input type="checkbox"/>  vmdatasat23_disk1_c53bab912da04d34a6e80269891edcac	Disk	West Europe



sqldatasat23 | Networking ☆ ...

SQL server

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 that access this resource. [Learn more](#)

Public network access

☐ Disable

☒ Selected networks

Connections from the IP addresses configured in the Firewall rules section below. [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

[Create](#)[Manage view](#) ▾[Delete resource group](#)[Refresh](#)[Export to CSV](#)[Open](#)[Overview](#)[Activity log](#)[Access control \(IAM\)](#)[Tags](#)[Resource visualizer](#)[Events](#)

Settings

[Deployments](#)


Essentials

[Resources](#)[Recommendations](#)[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](#)

 Search

 Overview

 Activity log

 Access control (IAM)





 Tags

 Resource visualizer

 Events

Settings

 Deployments


 Create  Manage view   Delete resource g


▼ 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



Generate/Import



Refresh



Restore Backup



View sample code



Manage deleted secrets



Overview



Activity log

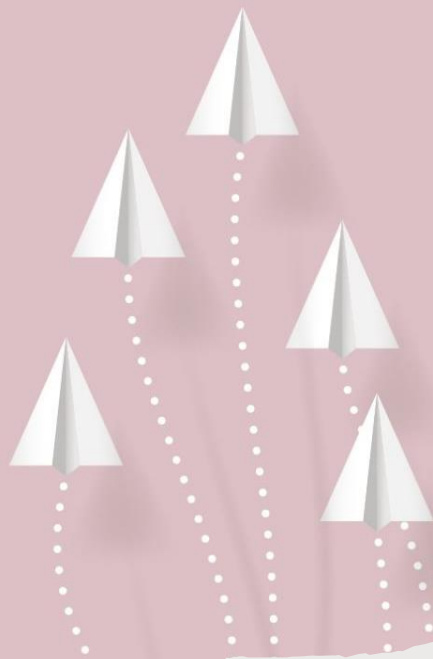


Access control (IAM)



Tags

Name	Type	Status
Sql-Administrator-Password		✓ Enabled
vmAdminPassword		✓ Enabled



THANK YOU!

Session
evaluation

Github
Repo

