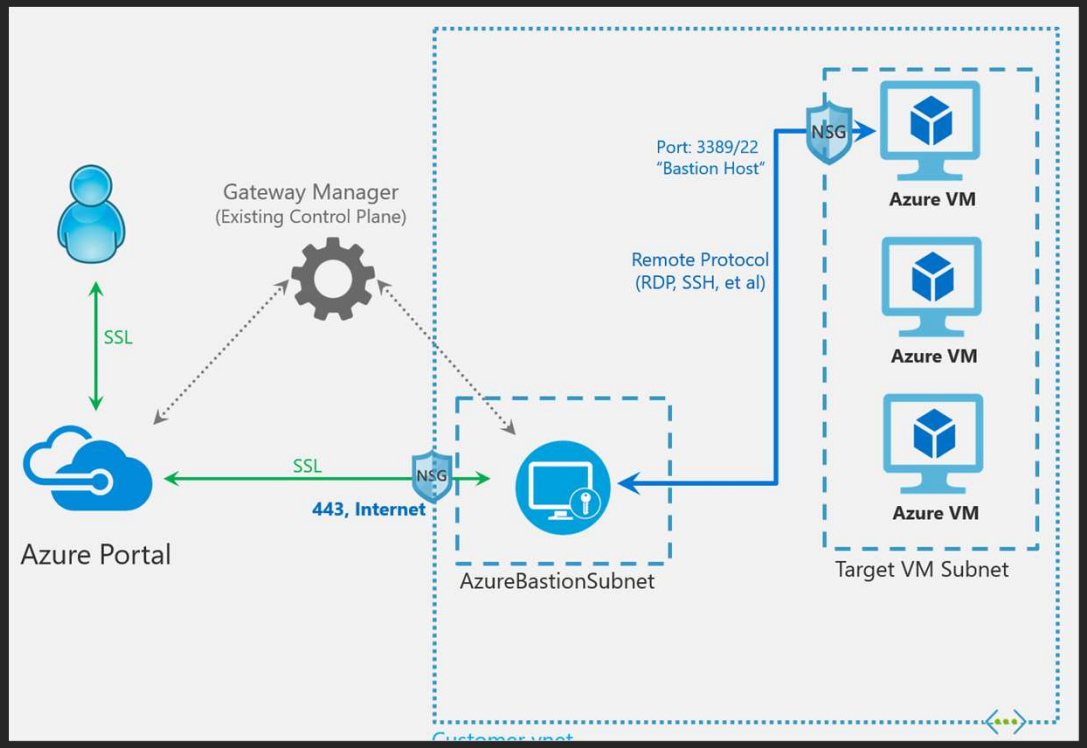


Secure access to Azure VMs with Azure Bastion

by Gregor Reimling

Menti

Gregor Reimling


Cloud Consultant @Sepago


Cloud and Datacenter, Governance


Azure Infrastructure (Governance, IaaS, Security)


info@reimling.eu


@GregorReimling | @AzureBonn


www.reimling.eu | www.neutralien.com

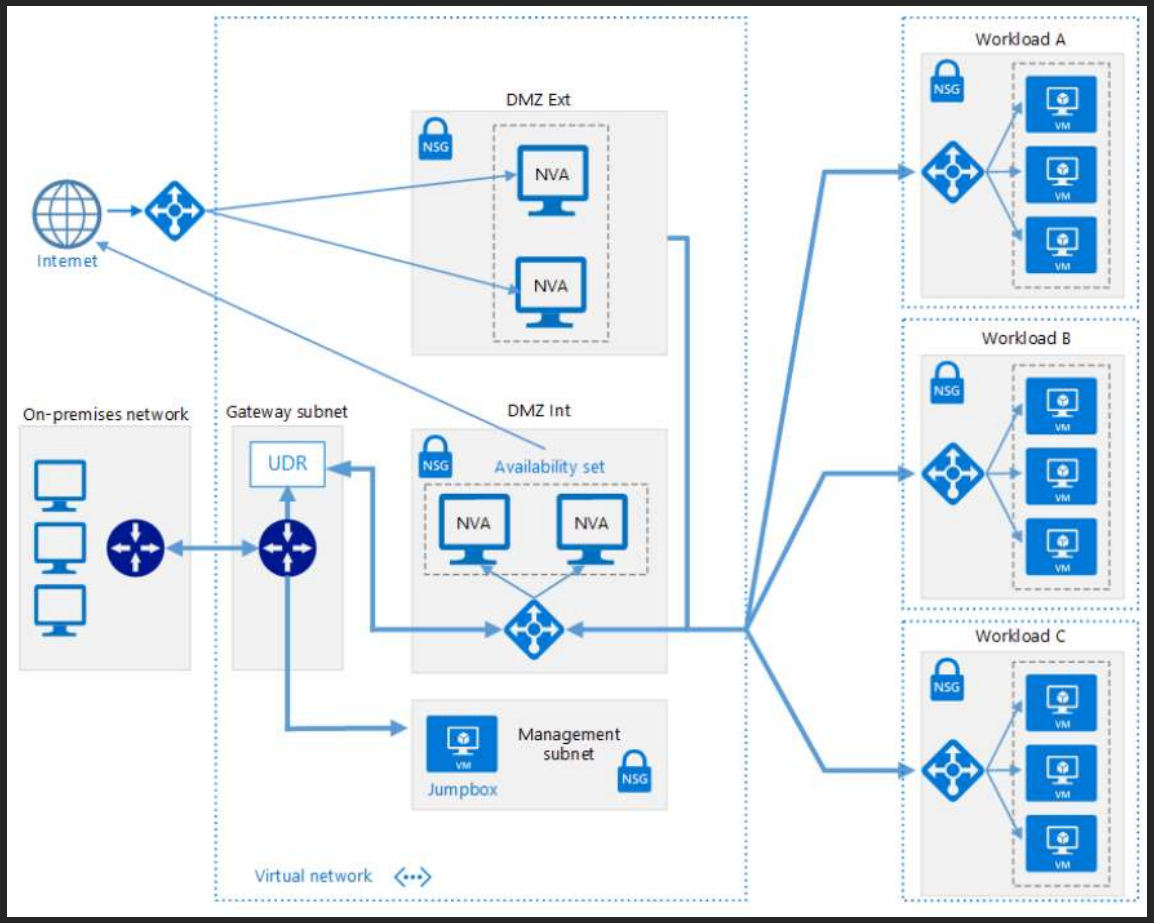
Identity Summit 2020
follow @IdentitySummit
on Twitter

www.AzureBonn.de

Azure Bastion - Agenda

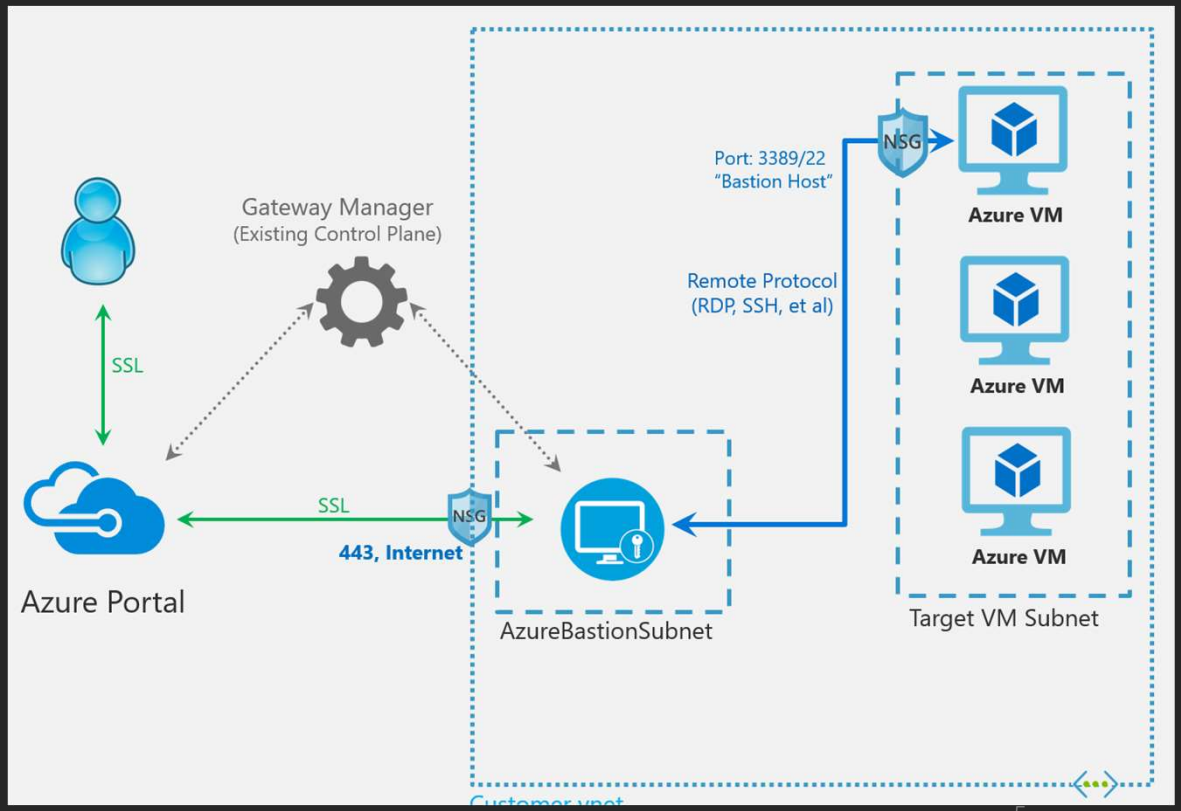
- Overview
- Requirements
- Demo
- Hardening
- Pricing & SLA
- Roadmap

Azure VNET Best Practices



Azure Bastion - Overview

- Fully-managed PaaS Service by Microsoft
- Replace Management of own Jumphosts
- Avoid bind Public IP on VM for Management purposes
- RDP and SSH directly inside the Azure Portal
- No need for an Agent inside VM
- Easy to deploy



Azure Bastion – General Notes

Region availability

West US, East US, South Central US

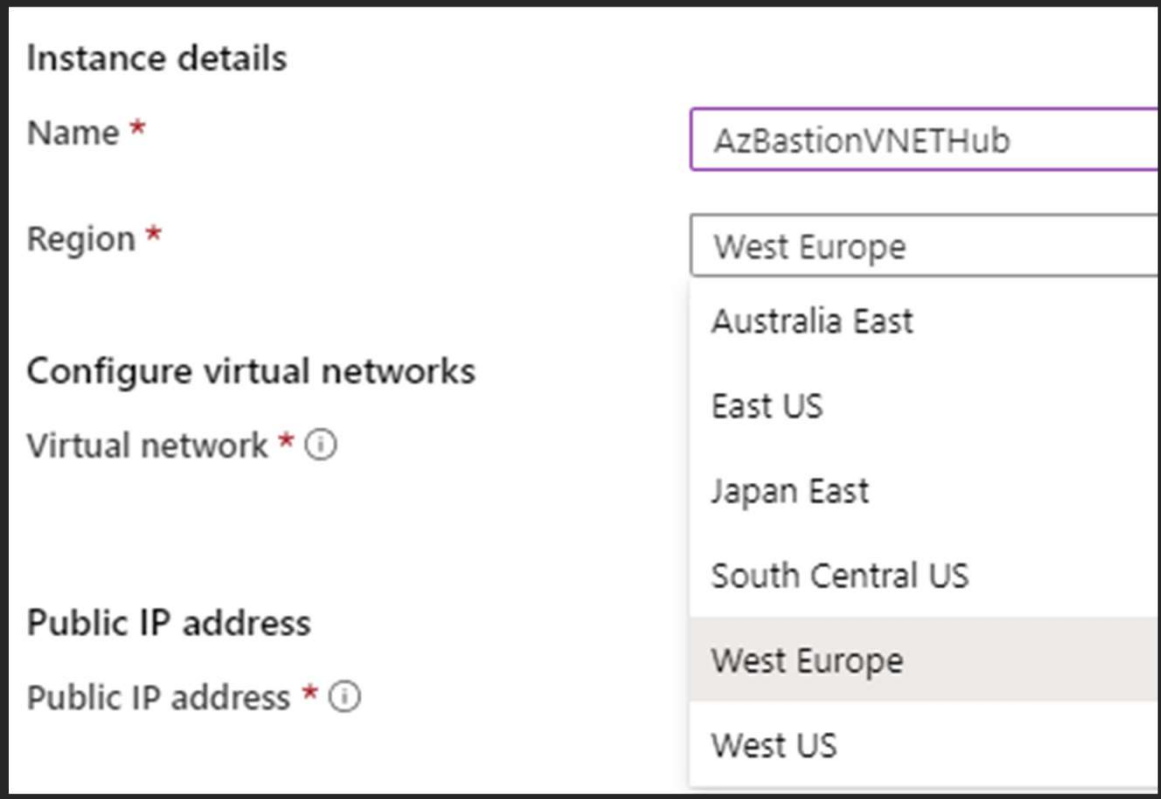
West Europe

Australia East & Japan East – take a look at https://docs.microsoft.com/en-us/azure/bastion/bastion-overview#which-regions-are-available

Browser compatibility

Chromium based (Edge Dev and Chrome)

Firefox also works

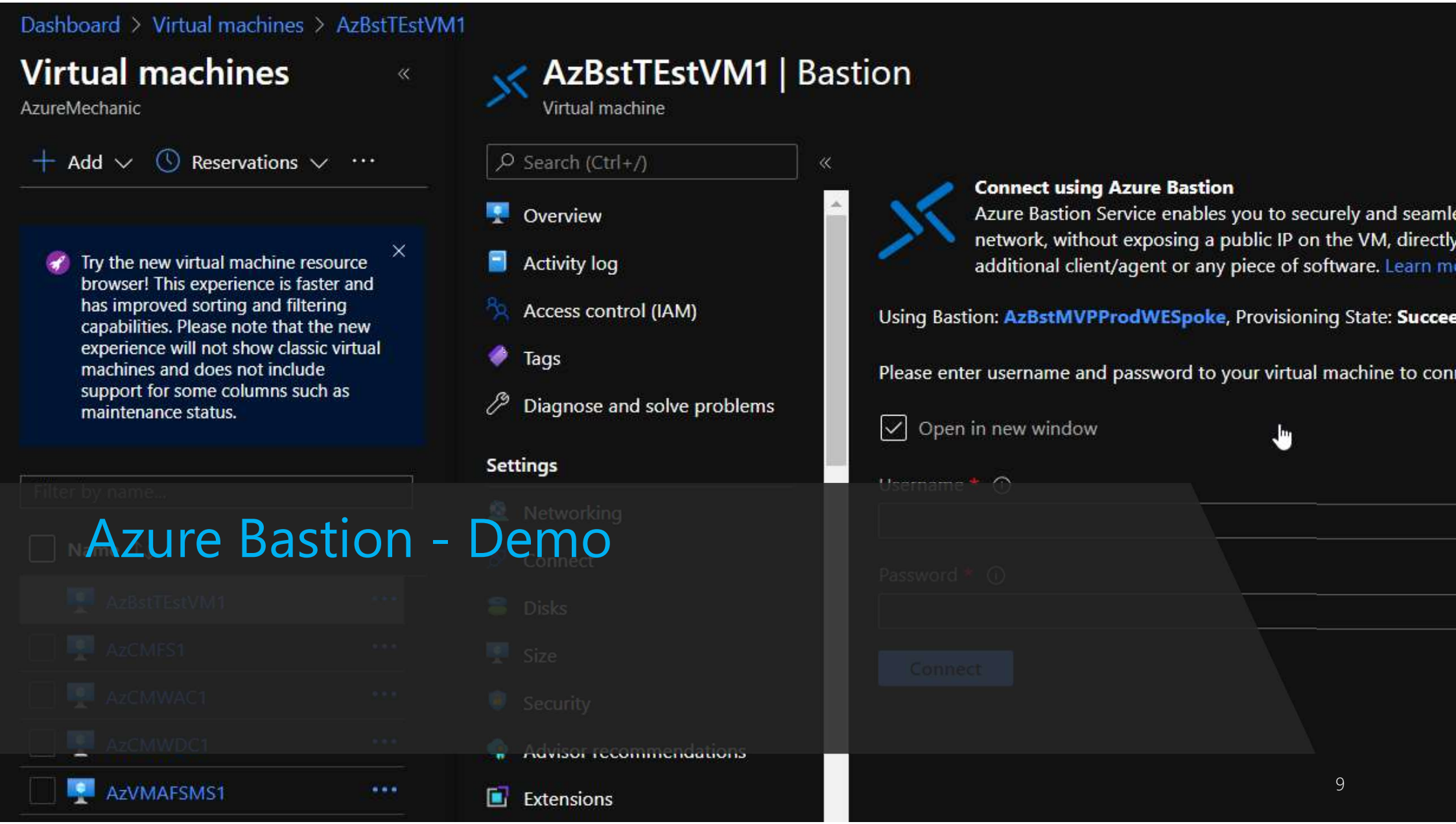


Azure Bastion – Requirements

- Minimum priviliges
  - Reader role on the VM
  - Reader role on the assigned NIC
  - Reader Role on the Azure Bastion resource
- Need an own Subnet inside the Virtual Network
  - subnet need at least /27 or larger subnet

Azure Bastion – How it works

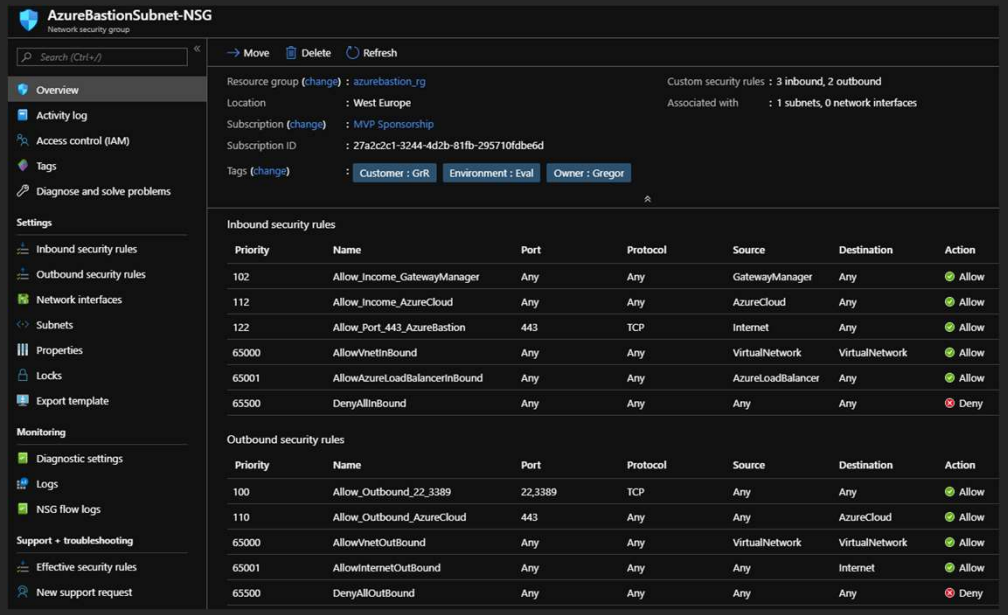
- Deploy a HTML 5 based Webclient
- RDP and SSH direct over the Portal
- Forward SSH/RDP over SSL
- Only accessible via the Portal
- Can`t access the Public IP directly



Azure Bastion - Demo

Azure Bastion – Hardening

- Harden Bastion Subnet with NSG
- Must define Inbound and Outbound Rules



https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg

Azure Bastion – Pricing & SLA

- In all regions same pricinig
- €uro: 0,081€ per hour x 730 hours = 116,97€
- $ 0,095$ per hour x 730 hours = 138,70$
- SLA: Azure Bastion will be available at least 99.95%

Azure Bastion - Summary

Pro

- Easy do deploy
- Secure your VNET
- Forget Jumphosts
- Can see and manage connections

Contra

- Need an own subnet
- Region availability
- Doesn´t support multi keystrongs
- No file copy inside the remote session

Additional Details

- VNET Peering is coming (Planned availability end of 2020)
- More regions coming soon (Germany West Central end of 2020)
- Alternative to Azure Bastion?
  - Azure VPN Gateway with P2S Connection and Azure AD authentication
- Check Azure Private Link for secure connection to PaaS

Azure Bastion – Links

- Azure Bastion Documentation Microsoft Docs
  - https://azure.microsoft.com/en-us/services/azure-bastion/
- What is Azure Bastion
  - https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
- Azure Bastion Feedback
  - https://feedback.azure.com/forums/217313-networking?query=bastion
- Secure Azure Bastion Subnet
  - https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg
- Blog Article about Azure Bastion
  - https://www.reimling.eu/2020/01/azure-bastion-how-to-secure-access-azure-vms-via-ssh-rdp-without-public-ip-or-jumphosts/
- Azure VPN Gateway AAD authentication
  - https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant-multi-app
- Azure Private Link (Secure PaaS in Azure)
  - https://www.reimling.eu/2020/06/connect-and-secure-azure-paas-services-to-virtual-networks-with-private-link/

Q&A

Identity Summit 2020
follow @IdentitySummit
on Twitter

Thank you

@GregorReimling | @AzureBonn
www.reimling.eu | www.neutralien.com