Microsoft

AZ-140

Tag 3

Configuring and Operating Azure Virtual Desktop

Guten Morgen!

AZ-140 Agenda

Role
- Permission Mgmt Resource
- Permission Data

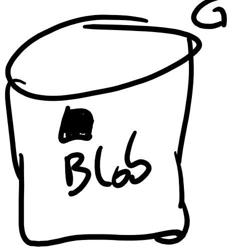
Lab

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

SA

LRS
↓
GRS



Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

RBAC

Roles

"Owner"
"Contributor"
"Reader"

Perm verwalten ✓

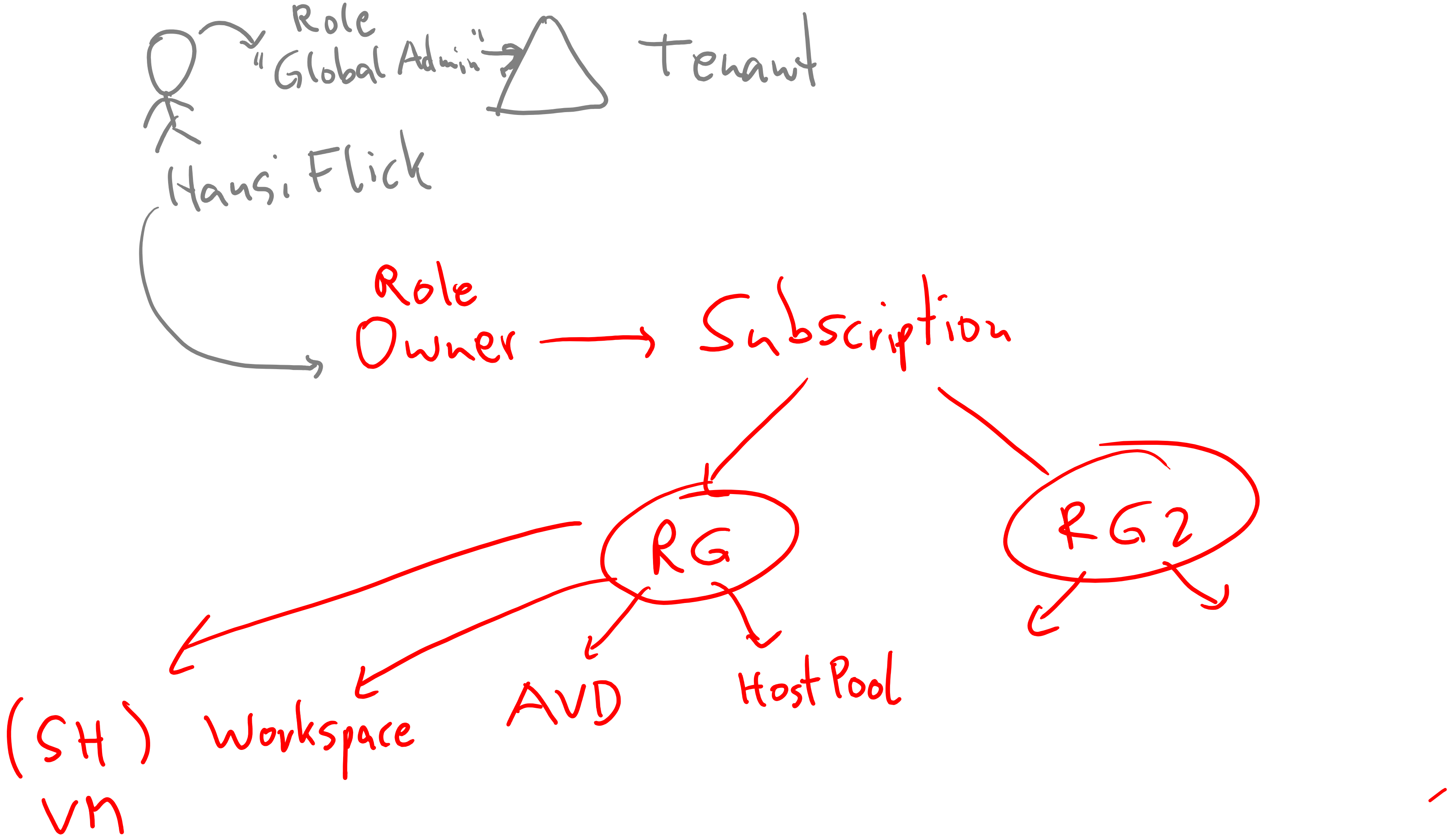
P~~er~~m verwalten

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Plan for disaster recovery
14. Automate Azure Virtual Desktop management tasks
15. Monitor and manage performance and health


Role
"Global Admin"
Tenant
Hansi Flick
Role
Owner
Subscription
RG
RG2
(SH)
VM
Workspace
AVD
Host Pool

Manage access for Azure Virtual Desktop

Introduction

1. RBAC for Azure Virtual Desktop
2. Plan and implement Azure roles and RBAC for Window Virtual Desktop
3. Using Azure Virtual Desktop with Intune
4. Enabling screen capture protection for Azure Virtual Desktop

AZ-140: Manage access and security (10-15%)

Manage access

- Conceptual knowledge of Azure compute solutions
- Working experience with virtual machines, virtual networks, and app service.

RBAC for Azure Virtual Desktop

TODO

New Teams in AVD

Microsoft Graph

KQL Kusto (Sentinel)

Data Lake

RBAC for Azure Virtual Desktop

Portal IAM

Desktop Virtualization Contributor

The Desktop Virtualization Contributor role lets you manage all aspects of the deployment.

Desktop Virtualization Reader

The Desktop Virtualization Reader role lets you view everything in the deployment but doesn't let you make any changes.

Host Pool Contributor

The Host Pool Contributor role lets you manage all aspects of host pools, including access to resources.

Host Pool Reader

The Host Pool Reader role lets you view everything in the host pool but won't allow you to make any changes.

Application Group Contributor

The Application Group Contributor role lets you manage all aspects of app groups.

Application Group Reader

The Application Group Reader role lets you view everything in the app group and will not allow you to make any changes.

Workspace Contributor

The Workspace Contributor role lets you manage all aspects of workspaces.

Workspace Reader

The Workspace Reader role lets you view everything in the workspace but won't allow you to make any changes.

User Session Operator

The User Session Operator role lets you send messages, disconnect sessions, and use the "logoff" function to sign sessions out of the session host.

Session Host Operator

The Session Host Contributor role lets you view and remove session hosts, as well as change drain mode.

Plan and implement Azure roles and RBAC for Window Virtual Desktop

Security principal

- Users
- User groups
- Service principals

Role definition

- Built-in roles
- Custom roles

Scope

- Host pools
- App groups
- Workspaces

To add Microsoft Entra users to an app group, run:

```
New-AzRoleAssignment -SignInName <userupn> -RoleDefinitionName "Desktop Virtualization User" -
ResourceName <appgroupname> -ResourceGroupName <resourcegroupname> -ResourceType
'Microsoft.DesktopVirtualization/applicationGroups'
```

To add Microsoft Entra user group to an app group, run:

```
New-AzRoleAssignment -ObjectId <usergroupobjectid> -RoleDefinitionName "Desktop Virtualization
User" -ResourceName <appgroupname> -ResourceGroupName <resourcegroupname> -ResourceType
'Microsoft.DesktopVirtualization/applicationGroups'
```

Azure CLI
az account ..

Using Azure Virtual Desktop with Intune

Azure Virtual Desktop is a desktop and app virtualization service that runs on Microsoft Azure.

- End users connect securely to a full desktop from any device.
- Secures and manages your Azure Virtual Desktop VMs with policy and apps at scale, after they're enrolled.
- Allows use of your existing configurations and secure the VMs with compliance policy and conditional access.

All VM limitations listed in Using Windows 10 virtual machines also apply to Azure Virtual Desktop VMs.

The following profiles aren't currently supported:

- Domain Join
- Wi-Fi

Windows 10 desktop device remote actions aren't supported for Azure Virtual Desktop VMs:

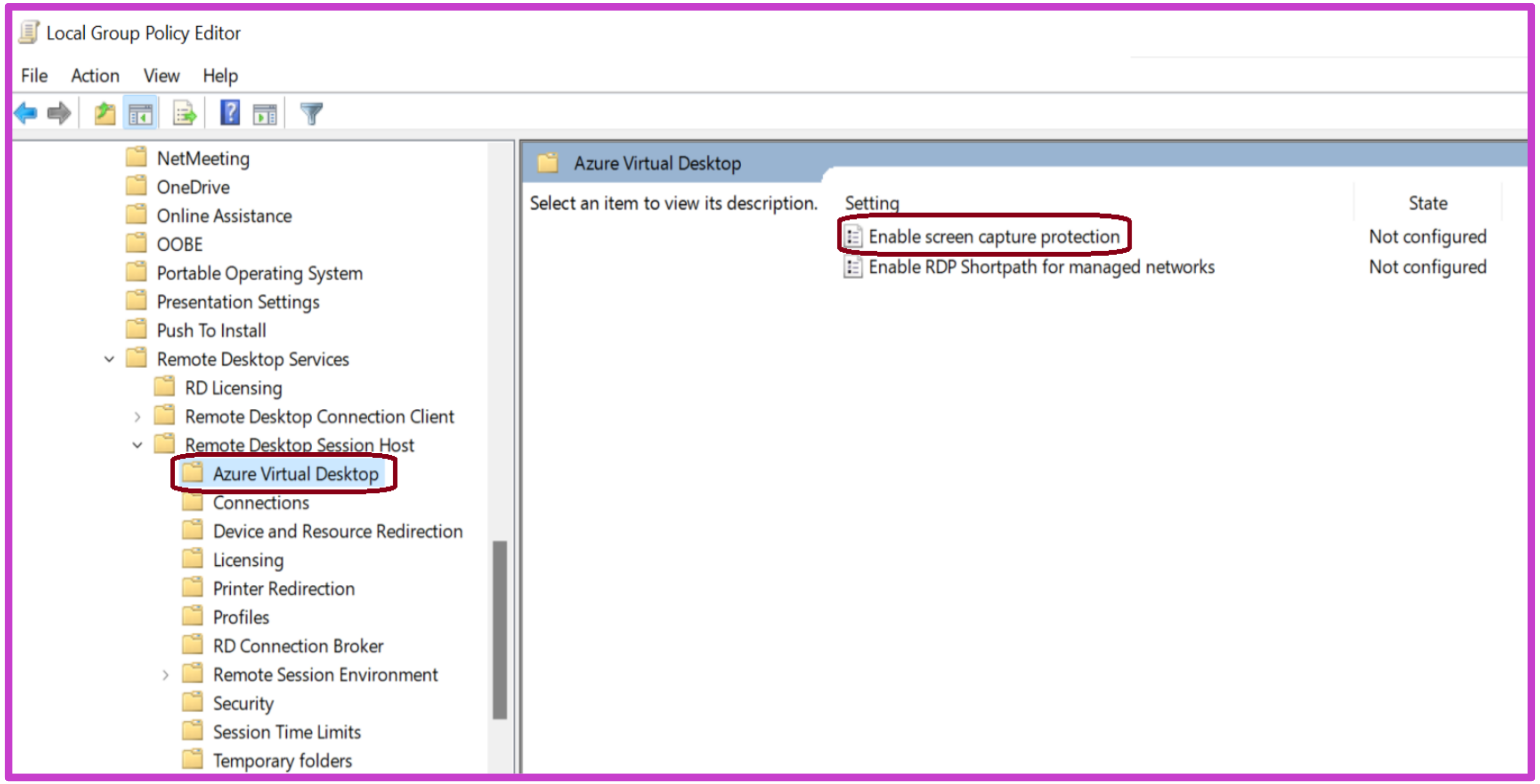
- Autopilot reset
- BitLocker key rotation
- Fresh Start
- Remote lock
- Reset password
- Wipe

Enabling screen capture protection for Azure Virtual Desktop

Screen capture protection for Azure Virtual Desktop

Screen capture protection prevents sensitive information from being captured at client endpoints.

- When enabled, the remote content will be automatically blocked or hidden in screenshots and screen shares.
- The Remote Desktop client hides content from malicious software attempting to capture the screen.



Setting	State
Enable screen capture protection	Not configured
Enable RDP Shortpath for managed networks	Not configured

Knowledge check and Summary

Check your knowledge

What you learned:

- Describe Azure role-based access controls (RBAC) for Azure Virtual Desktop.
- Plan and implement Azure roles and role-based access control (RBAC) for Azure Virtual Desktop.
- Describe how to configure Azure Virtual Desktop with Intune.
- How to enable screen capture protection for Azure Virtual Desktop.

End of presentation