



Windows Virtual Desktop krok za krokem

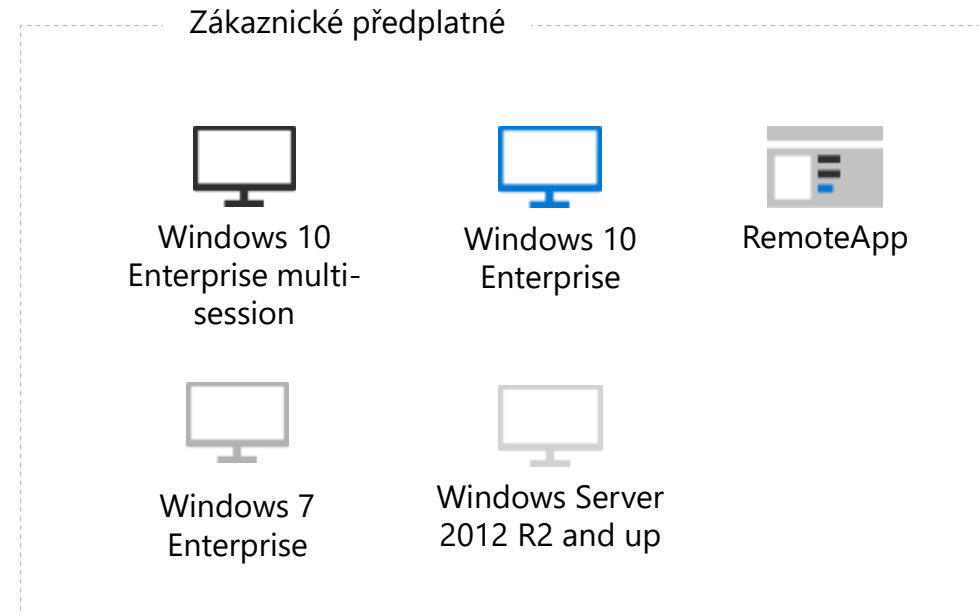
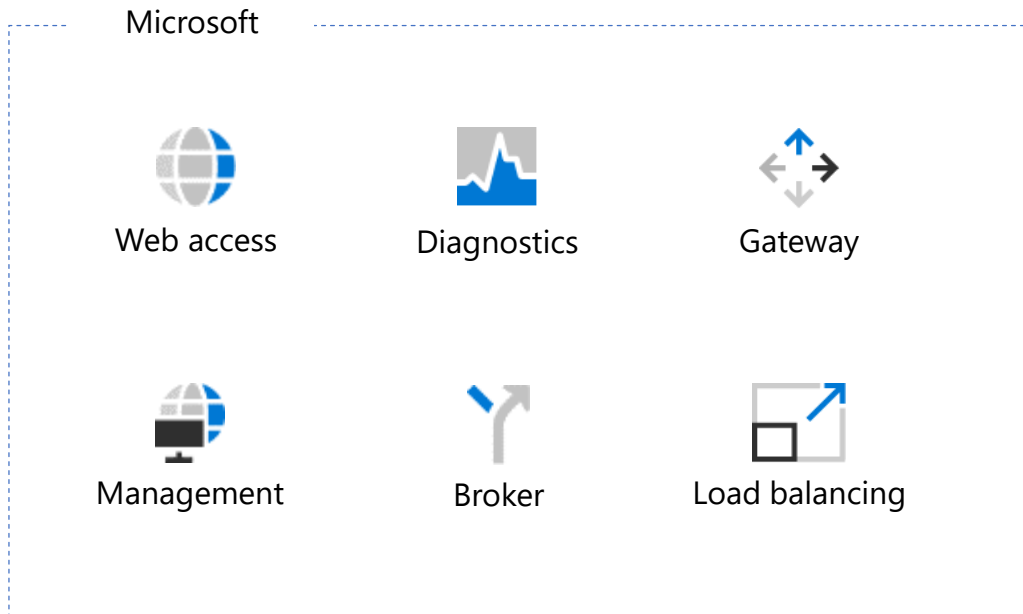
Lukáš Patka
pro DAQUAS a jeho partnery



Agenda

- Architektura
- Zprovoznění WVD
- Nástroje pro zálohování, správu WVD a aplikací
- Sizing a cena

WVD = hostované pracovní prostředí Windows



Podporované OS

Windows 10 Enterprise Multi-session

Windows 10 Enterprise Single-Session

Windows 7 Single-Session

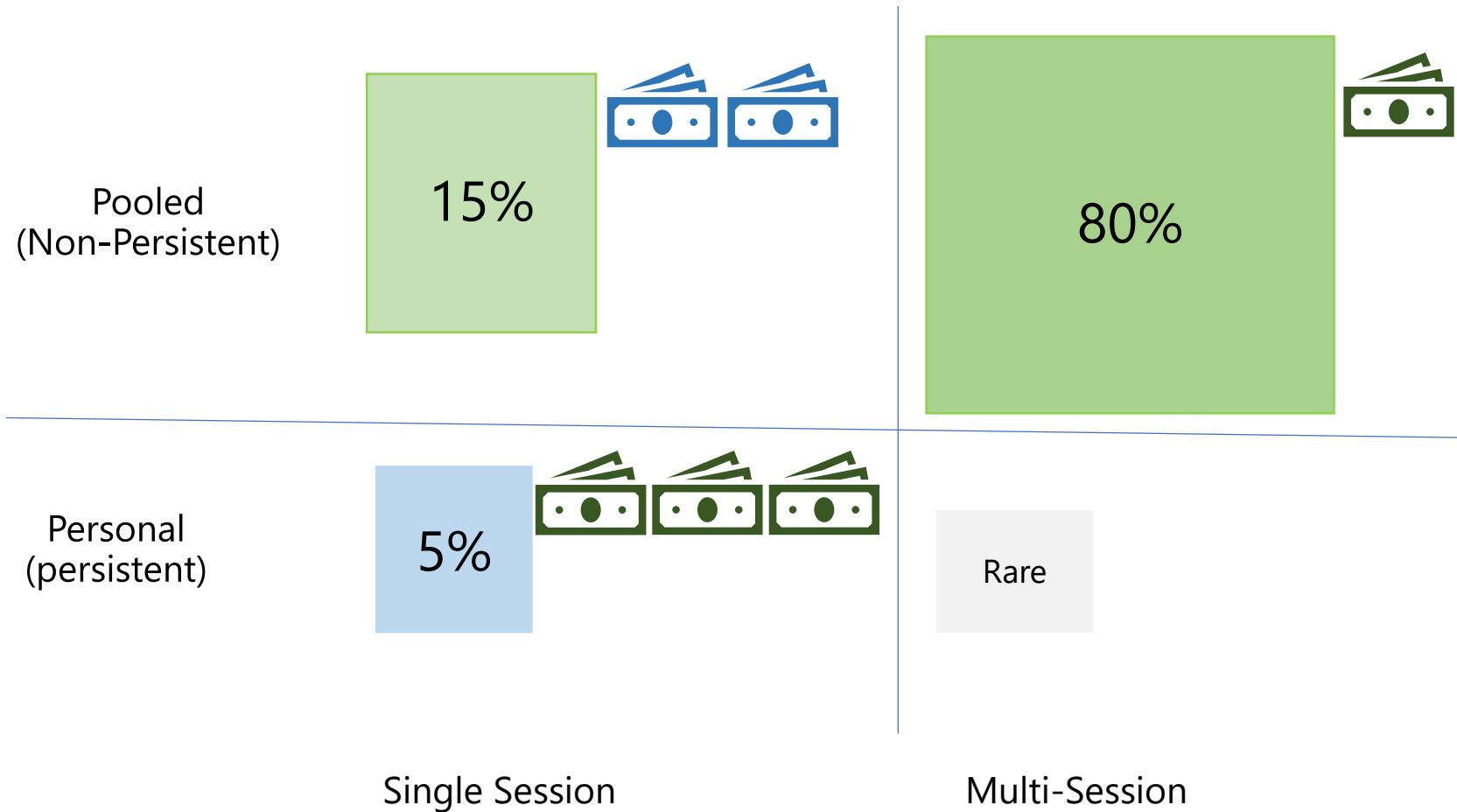
Windows Server 2019

Windows Server 2016

Windows Server 2012 R2



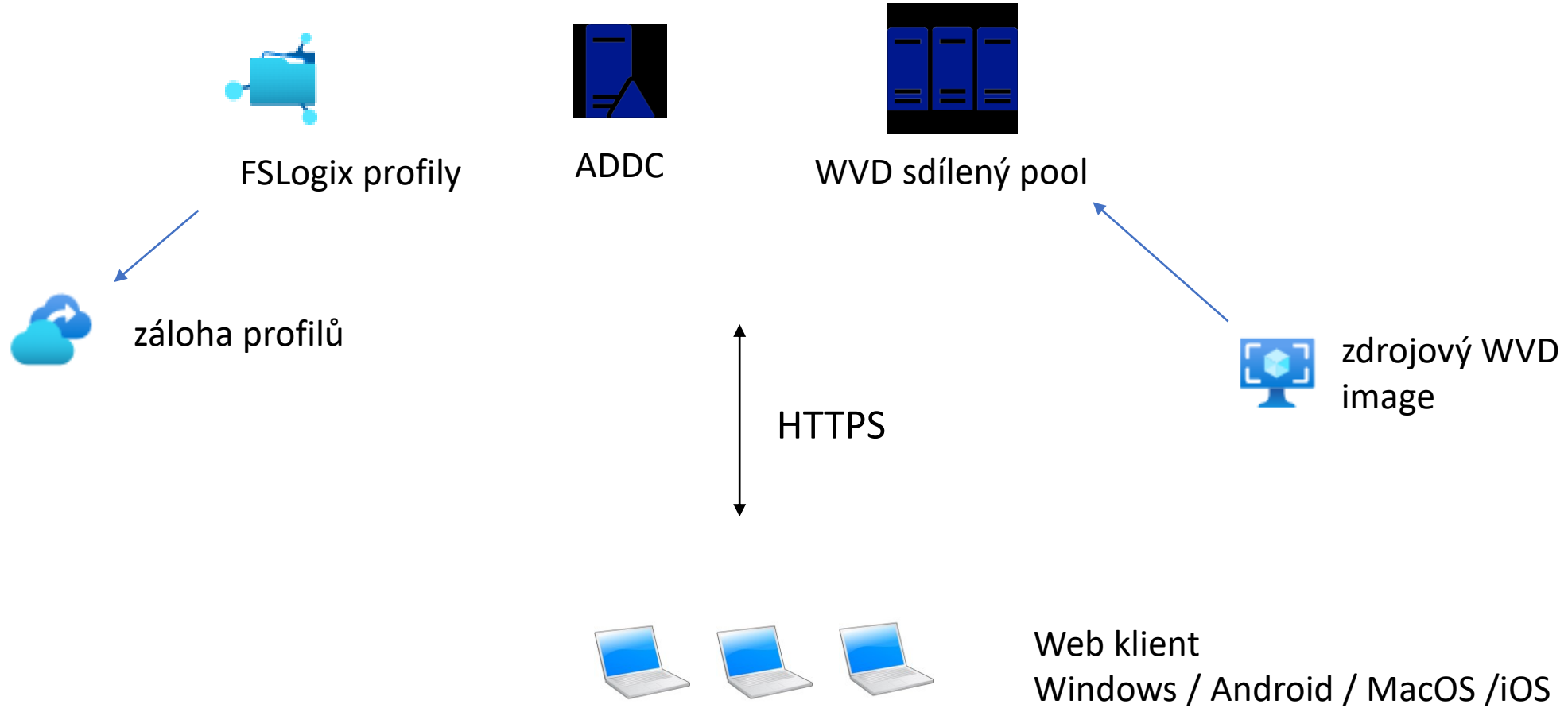
Způsoby nasazení WVD



Doporučený způsob nasazení - sdílený desktop

- Proč Desktop a ne server ?
 - Uživatelé jsou zvyklí na desktop prostředí
 - Desktop prostředí nevyžaduje RDS CALy
- Proč celý desktop a ne remoteapp ?
 - Uživatelé si na desktopu mohou nechat rozdělanou práci a připojit se k němu odkudkoliv, z libovolného zařízení
- Proč sdílený desktop a ne personální počítač pro každého ?
 - W10 Enterprise Multisession umožňuje připojení více uživatelů k jednomu stroji, čímž významně šetří náklady na provoz

Architektura



Architektura – body k diskuzi

- Proč ADDC a ne AAD ?
 - WVD nepodporuje přímo AAD, jen AADDS, které jsou relativně drahé
- Proč FSLogix a ne UPD ?
 - User Profile Disky nebudou do budoucna ve WVD podporovány
 - FSLogix jsou oproti UPD rychlejší a lépe řeší integraci s O365
- Proč Azure Files a ne klasický fileshare pro FSLogix profily ?
 - Azure Files nově podporují integraci s ADDS. Oproti klasickému fileshare se jedná o vysoce dostupnou službu pro jejíž provoz není potřeba žádný VM.

Napojení na ADDS / AAD DS



Možnosti



Klady



Zápory

A)

Hostování doménového řadiče v Azure (ADDS)

Známé prostředí doménového řadiče

Lze nasadit na zelené louce, nebo jako rozšíření stávající domény

Přístup ke kompletní správě domény

Levné řešení (21 EUR / DC / měsíc)

Doménu je nutné synchronizovat s AAD (prerokvazita pro WVD). Primárním zdrojem informací přitom zůstává ADDS a uživatelské atributy nelze měnit v AAD přes moderní online portály, ale musí se spravovat v AD.

Dodatečné náklady na správu virtuálního stroje, správu domény a správu synchronizace.

B)

Azure AD Domain Services

Jednoduché nasazení a správa

Automatické propsání identit z Azure AD

Vhodné hlavně pro cloud only zákazníky

AAD DS nelze vypnout => fixní náklady (min. 95EUR / měsíc)

Jedná se o izolovanou doménu, nikoliv rozšíření stávající WS AD

A) Příprava infrastruktury – AD DS

- Vytvoření virtuální sítě a doménového řadiče
 - [Jak správně nasadit AD DC v Azure](#)
 - Připojení k VM
 - [Point-to-site VPN](#), [Site-to-site VPN](#)
 - [Azure Bastion Host](#)
 - [Nastavení DNS](#) (custom DNS, ..)
 - [Synchronizace do AAD](#)
 - [Správa Windows aktualizací](#)
 - [Zálohování AD DS](#)

B) Příprava infrastruktury – AAD DS

- Vytvoření AAD Domain Services
 - [Jak správně nasadit Azure AD Domain Services](#)
 - [Nastavení DNS](#) (custom DNS, ..)

Zprovoznění WVD

- I) Vytvoření WVD tenantu
- II) Vytvoření WVD poolu
- III) Zřízení uživatelských profilů
- IV) Připojení

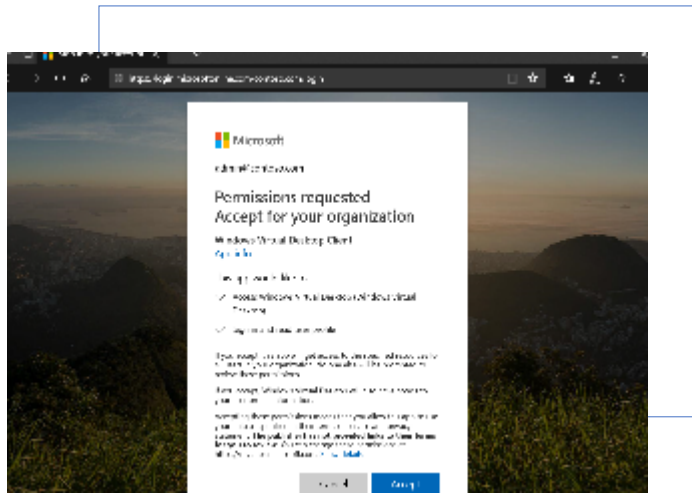
Pro konfiguraci budete potřebovat PowerShell

```
Install-Module -Name Microsoft.RDInfra.RDPowerShell
```

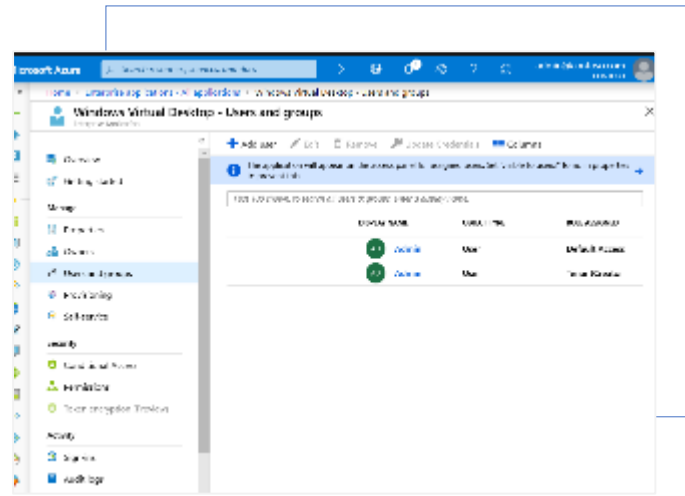
```
Import-Module -Name Microsoft.RDInfra.RDPowerShell
```

Tento modul nepodporuje PowerShell Core, nelze tedy spustit v Cloud Shell a na MacOS

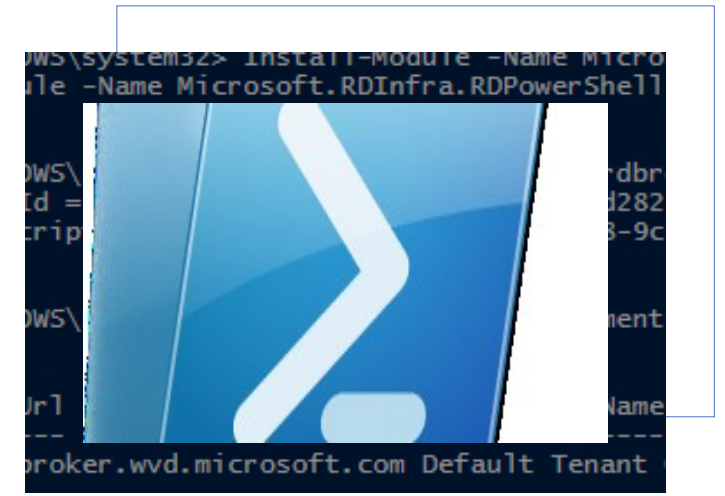
I) Vytvoření WVD tenantu



Povolení přístupu k AAD



Nastavení rolí pro správu



Vytvoření tenantu

Dokumentace: <https://docs.microsoft.com/en-us/azure/virtual-desktop/>

1) Povolení přístupu k AAD (Graph API)

<https://rdweb.wvd.microsoft.com/>

Consent pro Server App



admin@azlabszcz.onmicrosoft.com

Permissions requested Accept for your organization

Windows Virtual Desktop

[App info](#)

This app would like to:

- ✓ Read all users' full profiles
- ✓ Read all users' full profiles
- ✓ Read all groups
- ✓ Read directory data
- ✓ Read directory data
- ✓ Read all users' basic profiles
- ✓ Read all users' full profiles

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Cancel

Accept

+

Consent pro Client App



admin@azlabszcz.onmicrosoft.com

Permissions requested Accept for your organization

Windows Virtual Desktop Client

[App info](#)

This app would like to:

- ✓ Sign in and read user profile
- ✓ Access Windows Virtual Desktop (Windows Virtual Desktop)

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

If you accept, Windows Virtual Desktop will also have access to your user profile information.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)



Cancel

Accept

=>

 **Enterprise applications**
AZlabs CZ - Azure Active Directory

NAME

	Windows Virtual Desktop
	Windows Virtual Desktop Client

2) Přidělení oprávnění pro správu

Home > AZlabs CZ > Enterprise applications - All applications > Windows Virtual Desktop - Users and groups

Windows Virtual Desktop - Users and groups


Enterprise Application

 Edit Remove Update Credentials Columns

Home > AZlabs CZ > Enterprise applications - All applications > Windows Virtual Desktop - Users and groups > Add Assignment

Add Assignment

AZlabs CZ

 Groups are not available for assignment due to your Active Directory plan level.


Users
1 user selected.






Windows Virtual Desktop - Users and groups

Enterprise Application

+ Add user Edit Remove Update Credentials Columns

 The application will appear on the Access Panel for assigned users. Set 'visible to users?' t

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
 admin	User	Default Access
 admin	User	

3) Založení nového WVD tenantu / workspace

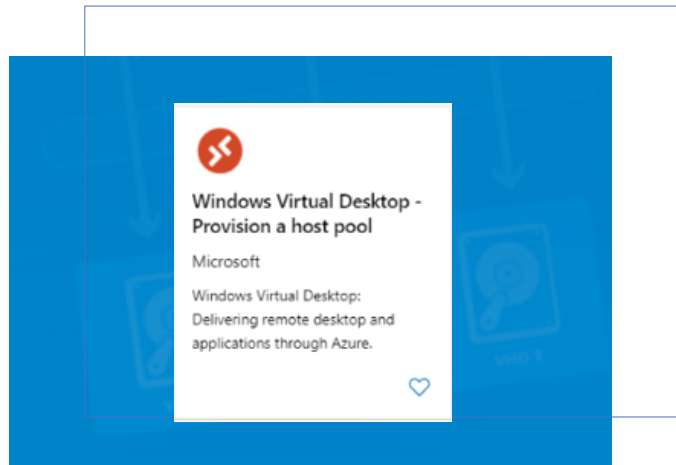
```
Add-RdsAccount -DeploymentUrl "https://rdbroker.wvd.microsoft.com"
```

```
New-RdsTenant -Name <TenantName> -AadTenantId <DirectoryID> -AzureSubscriptionId <SubscriptionID>
```

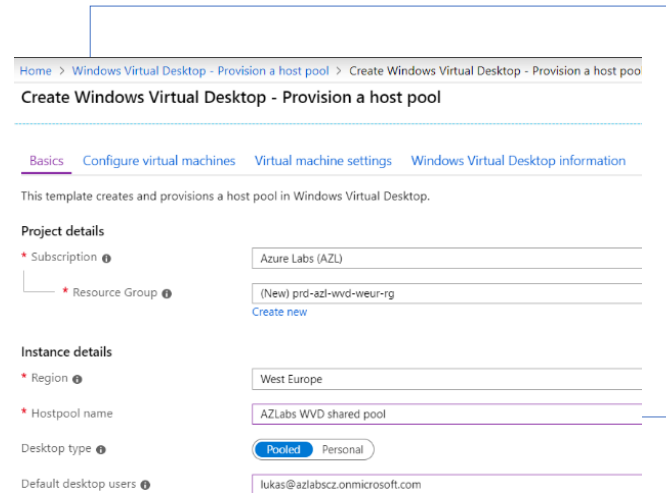
4) Nastavení dalších správců WVD

```
New-RdsRoleAssignment -RoleDefinitionName "RDS Owner" -SignInName <UPN> -TenantName <WVDTenant>
```


II) Vytvoření WVD poolu



Instalace z Markeplace

A screenshot of the Azure portal configuration page for creating a Windows Virtual Desktop host pool. The page title is 'Create Windows Virtual Desktop - Provision a host pool'. It includes navigation tabs: 'Basics', 'Configure virtual machines', 'Virtual machine settings', and 'Windows Virtual Desktop information'. Below the tabs, there is a description: 'This template creates and provisions a host pool in Windows Virtual Desktop.' The configuration is divided into sections: 'Project details' with fields for 'Subscription' (Azure Labs (AZL)) and 'Resource Group' ((New) prd-azl-wvd-weur-rg); 'Instance details' with fields for 'Region' (West Europe) and 'Hostpool name' (AZLabs WVD shared pool); 'Desktop type' (radio buttons for 'Pooled' and 'Personal', with 'Pooled' selected); and 'Default desktop users' (lukas@azlabsz.onmicrosoft.com).

Nastavení WVD

1) Instalace WVD z Marketplace

Home > New > Marketplace

Marketplace

My Saved List


Recently created

Service Providers

Categories

- Get Started
- AI + Machine Learning
- Analytics
- Blockchain
- Compute
- Containers


Showing All Results



Windows Virtual Desktop - Provision a host pool

Microsoft

Windows Virtual Desktop:
Delivering remote desktop and applications through Azure.



Home > Windows Virtual Desktop - Provision a host pool > Create Windows Virtual Desktop - Provision a host pool

Create Windows Virtual Desktop - Provision a host pool

Basics [Configure virtual machines](#) [Virtual machine settings](#) [Windows Virtual Desktop information](#)

This template creates and provisions a host pool in Windows Virtual Desktop.

Project details

- * Subscription ⓘ Azure Labs (AZL)
- * Resource Group ⓘ (New) prd-azl-wvd-weur-rg
[Create new](#)

Instance details

- * Region ⓘ West Europe
- * Hostpool name AZLabs WVD shared pool
- Desktop type ⓘ Pooled Personal
- Default desktop users ⓘ lukas@azlabscz.onmicrosoft.com

Windows Virtual Desktop stores information that is global in nature. Select the location you would like the service metadata to be stored.
[Learn more](#)

Service metadata location United States

2) Sizing a vlastnosti VM

Home > [Windows Virtual Desktop - Provision a host pool](#) > Create Windows Virtual Desk

Create Windows Virtual Desktop - Provision a host pool

Basics Configure virtual machines Virtual machine settings Windows Virtual

Usage Profile ⓘ Light Medium Heavy Custom

* Total users

* Virtual machine size **2x Standard B2ms**
2 vcpus, 8 GB memory
[Change size](#)

* Virtual machine name prefix ⓘ

Home > [Windows Virtual Desktop - Provision a host pool](#) > Create Windows Virtual Desktop - Provision a host pool

Create Windows Virtual Desktop - Provision a host pool

Basics [Configure virtual machines](#) Virtual machine settings [Windows Virtual Desktop information](#)

Image source ⓘ Blob storage Managed image Gallery

Image OS version

Disk Type

* AD domain join UPN ⓘ

* Admin Password ⓘ

* Confirm password

Specify domain or OU ⓘ No Yes

Domain to join ⓘ

(Optional) OU path ⓘ

Configure virtual networks

* Virtual network ⓘ
[Create new](#)

* vmSubnet ⓘ
[Manage subnet configuration](#)

3) Provázání poolu s WVD tenantem

Home > Windows Virtual Desktop - Provision a host pool > Create Windows Virtual Desktop - Provision a host pool

Create Windows Virtual Desktop - Provision a host pool

Basics [Configure virtual machines](#) [Virtual machine settings](#) [Windows Virtual Desktop information](#) [Review + create](#)

Windows Virtual Desktop tenant group name * ⓘ

Windows Virtual Desktop tenant name * ⓘ ✓

Windows Virtual Desktop tenant RDS Owner ⓘ

UPN * ⓘ ✓

Password * ⓘ ✓

Confirm password * ⓘ ✓



You cannot enter a user account that requires MFA. If you intend to use MFA, consider creating a service principal for this purpose. [↗](#)

III) Zřízení uživatelských profilů

FSLogix profily hostované na Azure Files

- Konfigurace se liší podle toho, zda jste WVD připojili do

- AAD DS: v GA od 08/2019 ve většine regionů

- <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable>

- ADDS: aktuálně (03/2020) v preview, ve vybraných regionech (NE west europe)

- <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable>

Tento návod se věnuje pouze připojení Azure Files do ADDS.
Postup pro AAD DS naleznete v dokumentaci viz odkaz výše.

1) Vytvoření storage account a file share

Home > Storage accounts > Create storage account

Create storage account

✓ Validation passed

Basics Networking Advanced Tags Review + create

Basics

Subscription	WVD LAB (WL)
Resource group	wl-wvd-gwc-rg
Location	Germany West Central
Storage account name	wlwwdgcst0
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Locally-redundant storage (LRS)
Performance	Standard
Access tier (default)	Hot

Networking

Connectivity method	Public endpoint (all networks)
---------------------	--------------------------------

Advanced

Secure transfer required	Enabled
Large file shares	Disabled
Blob soft delete	Disabled
Blob change feed	Disabled
Hierarchical namespace	Disabled
NFS v3	Disabled

Home > Microsoft.StorageAccount-20200313085838 | Overview > wlwwdgcst0 | File shares

wlwwdgcst0 | File shares

Storage account

Search (Ctrl+/) << + File share Refresh

Storage account: wlwwdgcst0

Search file shares by prefix

Name	Modified
No results	

Overview
Activity log
Access control (IAM)
Tags

New file share

Name *
wvdprofiles ✓

Quota ⓘ
100 ✓ GiB

Název storage account max 15 znaků (Kerberos limit pro computer account)

Podporované regiony pro integraci s ADDS (stav k 03/2020)

- Všechny regiony, KROMĚ

- West US
- West US 2
- East US
- East US 2
- West Europe
- North Europe

2) Připojení storage do domény

`Import-Module -name AzFilesHybrid`

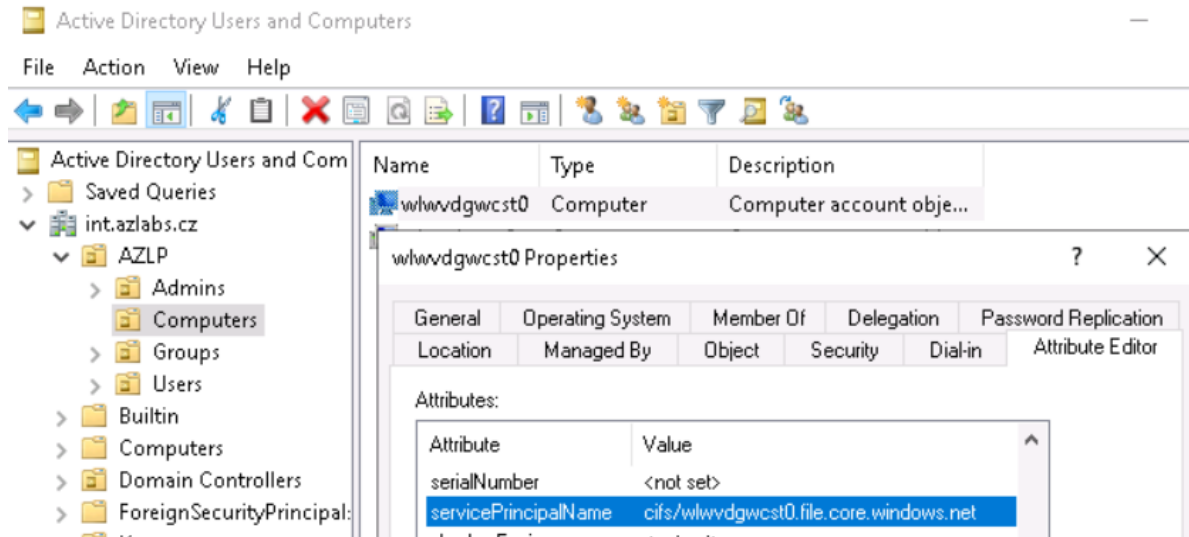
(ke stažení z <https://github.com/Azure-Samples/azure-files-samples/releases>)

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName <název RG> -Name <název storage account>"
```

```
join-AzStorageAccount -StorageAccount $storageAccount -DomainAccountType ComputerAccount  
-OrganizationalUnitDistinguishedName <DN organizační jednotky>
```

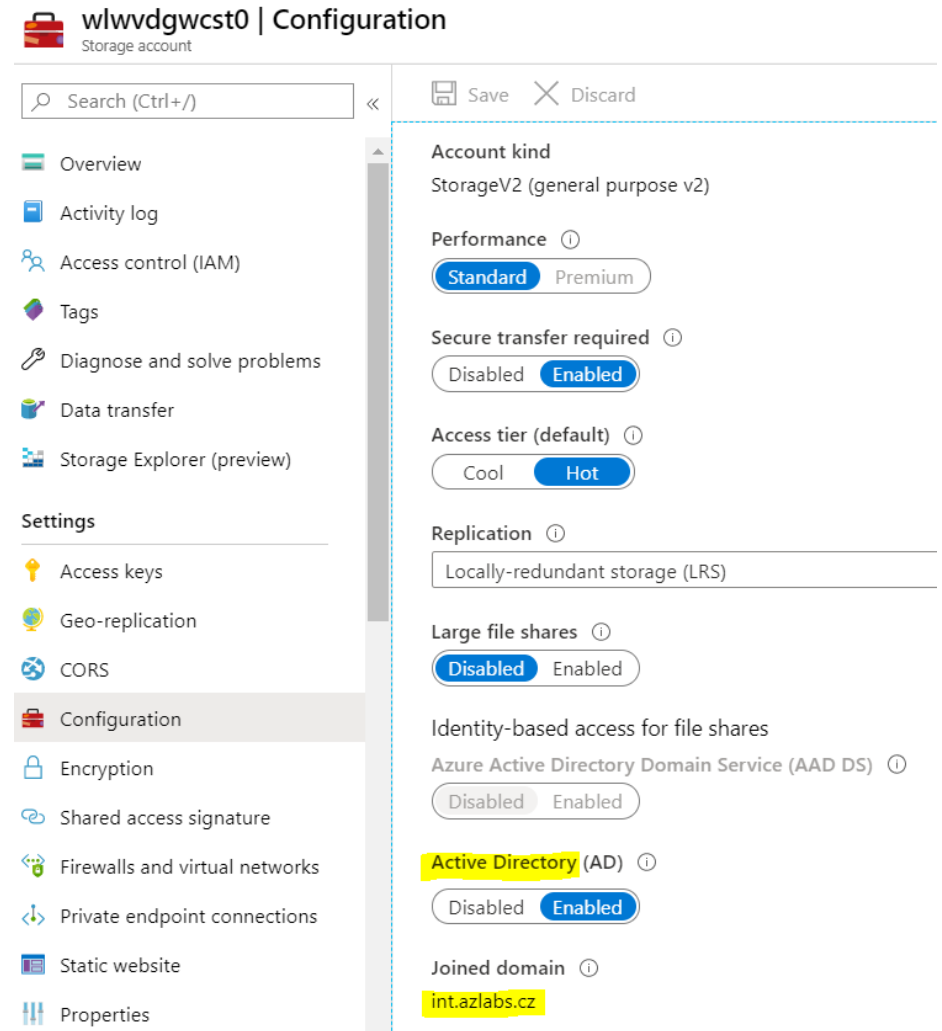
(cmdlet spustit z PC v doméně)

3) Kontrola nastavení



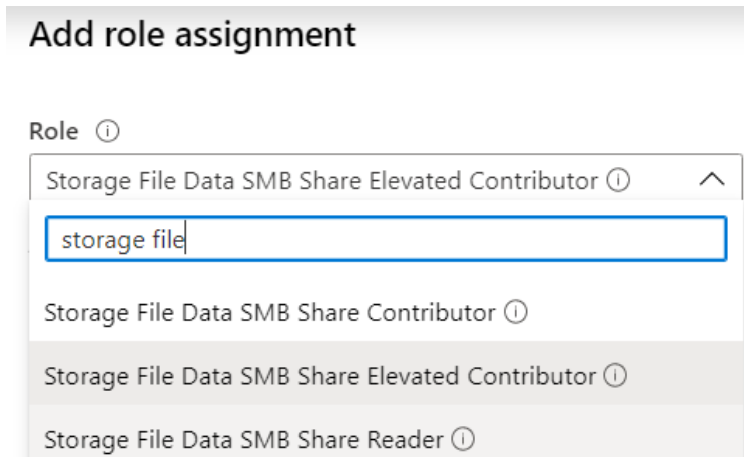
Kontrola

- v AD vytvořen nový computer objekt s SPN „cifs/...file.core.windows.net“
- V Azure povolena integrace s AD



4) Nastavení oprávnění

Azure oprávnění



Oprávnění pro uživatele:

Storage File ..Share Contributor

Admin oprávnění – nastavení NTFS:

Storage File .. Elevated Contributor

NTFS oprávnění

Namapujte Azure Files jako síťový disk po účtem s oprávněním „Storage file .. Elevated Contributor“

```
net use p: \\<storage>.file.core.windows.net\wvdprofiles
```

Nastavte oprávnění na root složky (p:)

<https://docs.microsoft.com/en-us/fslogix/fslogix-storage-config-ht>

Permission entries:

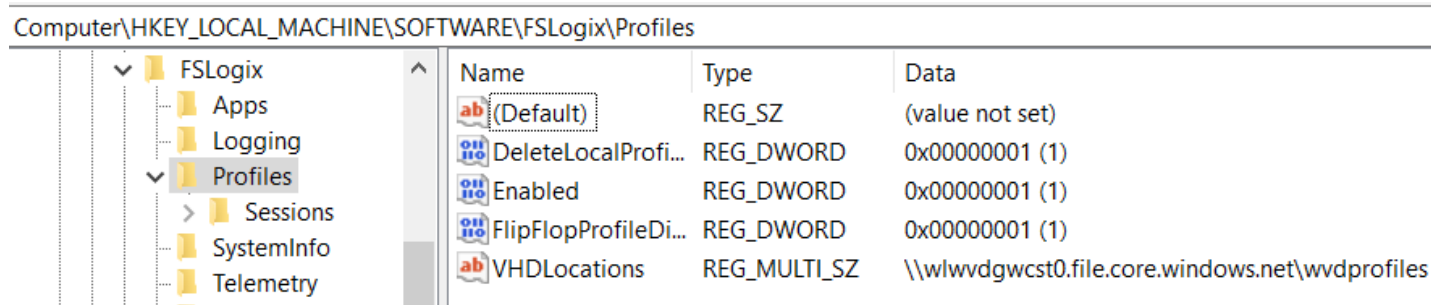
Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (wl...	Full control	None	This folder, subfolders and files
Allow	Users (wlwvdgwcs...	Modify	None	This folder only
Allow	CREATOR OWNER	Modify	None	Subfolders and files only

5) Nastavení klienta

Nainstalujte FSLogix agenta (https://aka.ms/fslogix_download)

Nastavte registry: Computer\HKEY_LOCAL_MACHINE\software\FSLogix

Name	Type	Data/Value
Enabled	DWORD	1 (povolí FSLogix)
VHDLocations	Multi-String Value	"\\<storage>.file.core.windows.net\vvdprofiles"
DeleteLocalProfileWhenVHDSshouldApply	DWORD	1 (místo lokálního profilu vytvoří FSLogix)
FlipFlopProfileDirectoryName	DWORD	1 (název vhd = username-SID a ne obráceně)



Name	Type	Data
(Default)	REG_SZ	(value not set)
DeleteLocalProfi...	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000001 (1)
FlipFlopProfileDi...	REG_DWORD	0x00000001 (1)
VHDLocations	REG_MULTI_SZ	\\wlvwdgwcst0.file.core.windows.net\vvdprofiles

<https://docs.microsoft.com/en-us/azure/virtual-desktop/create-host-pools-user-profile>

IV) Připojení

Web Client:



Windows



macOS



Linux



Chrome OS



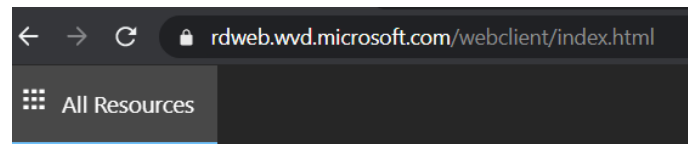
Desktop Client:



iOS

1) Test připojení - Web

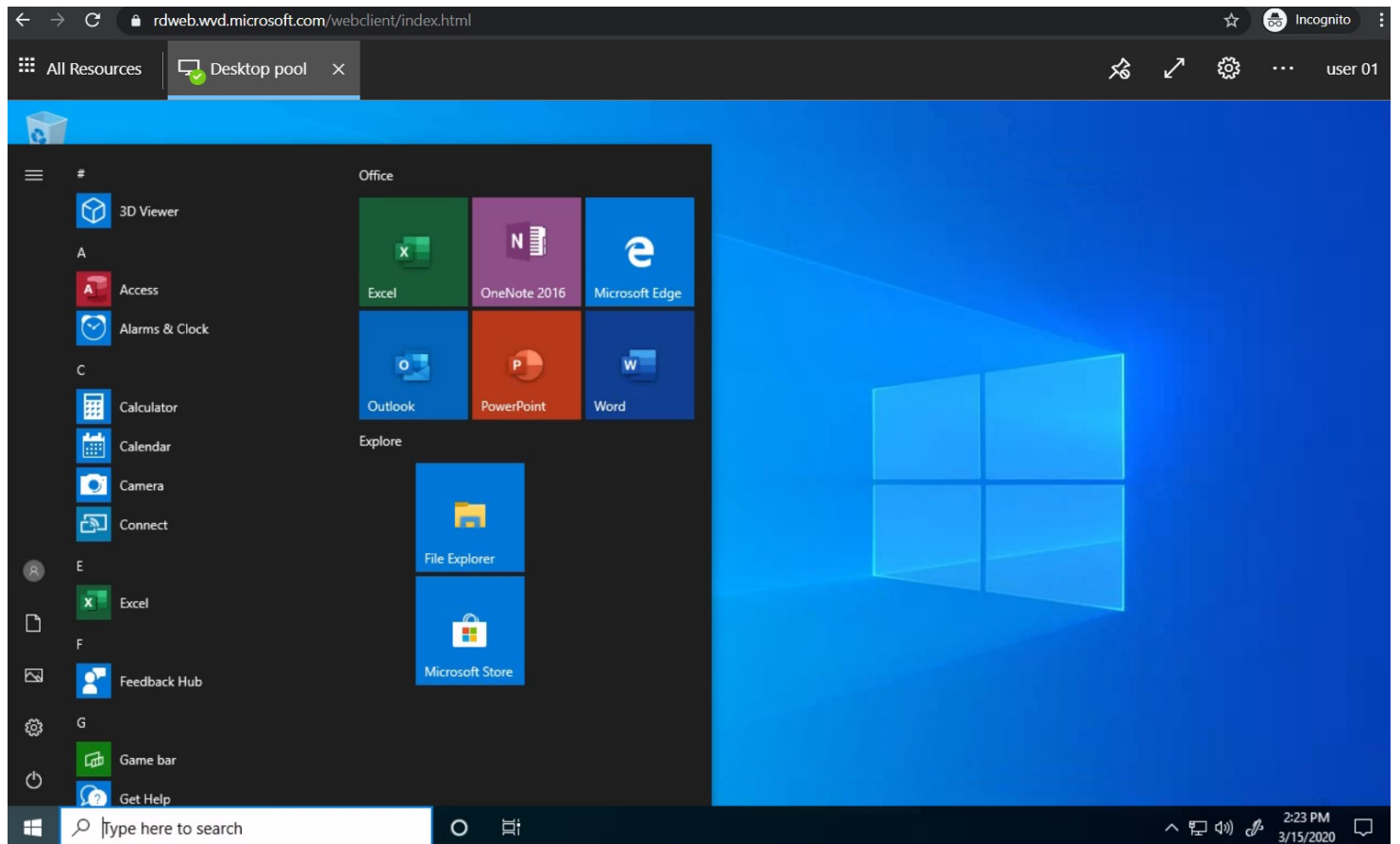
<https://rdweb.wvd.microsoft.com/webclient>



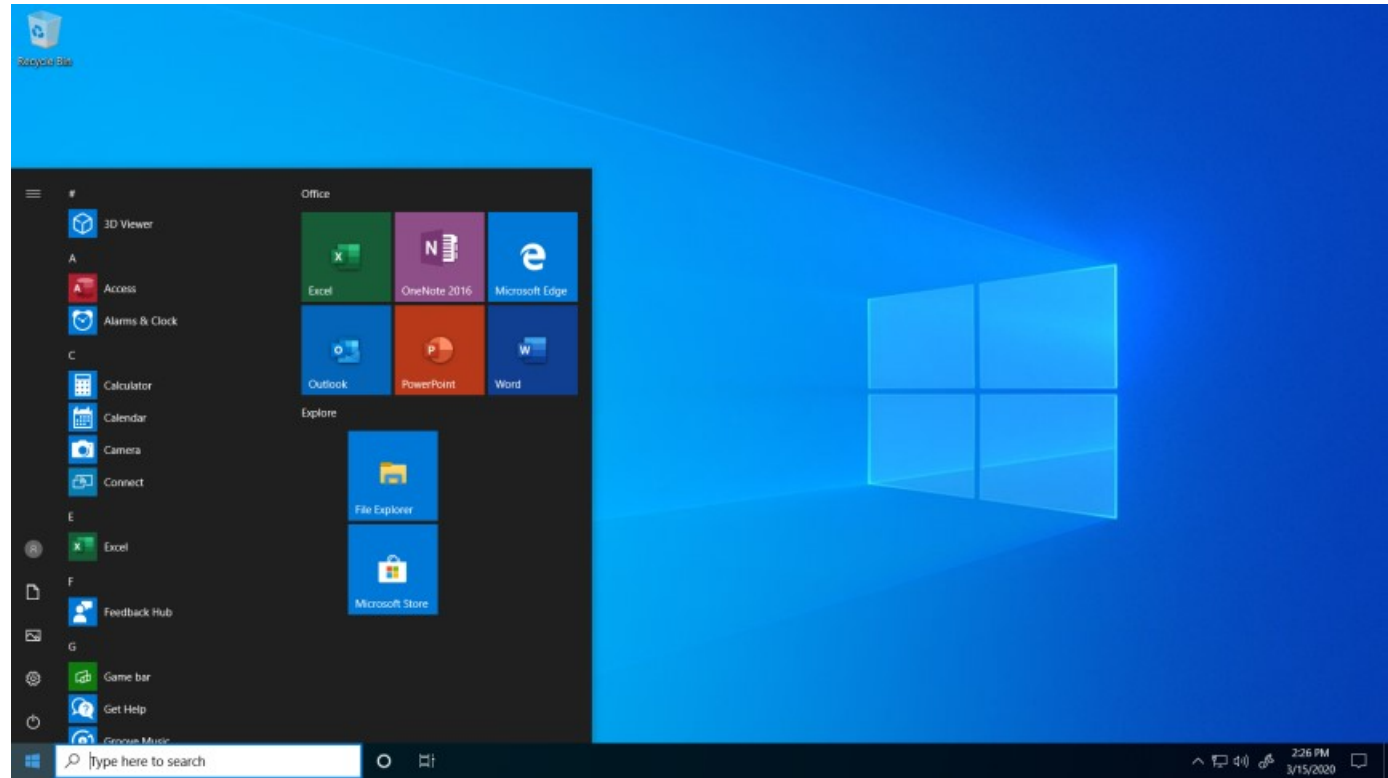
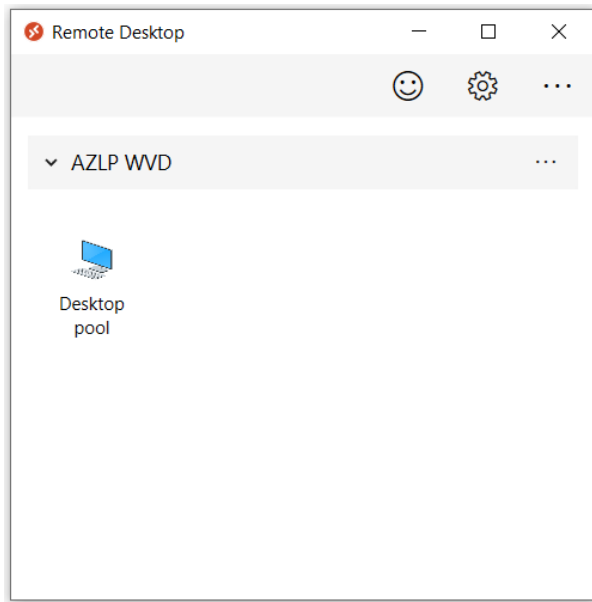
▼ AZLP WVD



Desktop pool

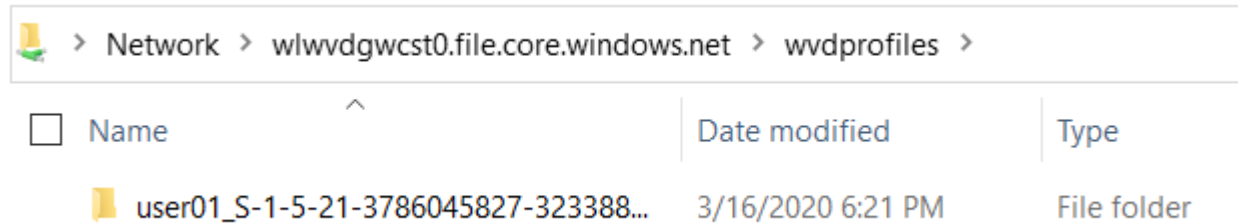


2) Test připojení – RD Client



<https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10>

3) Kontrola vytvoření uživatelského profilu



<input type="checkbox"/> Name	Date modified	Type
user01_S-1-5-21-3786045827-323388...	3/16/2020 6:21 PM	File folder

4) Přidání dalších uživatelů

```
Add-RdsAccount -DeploymentUrl "https://rdbroker.wvd.microsoft.com"
```

```
Add-RdsAppGroupUser <tenantname> <hostpoolname> "Desktop Application Group" -UserPrincipalName <upn>
```

Co dál..

WVD máme zprovozněné, čím ho dále můžeme obohatit

- GPO a RDP nastavení
- Instalace aplikací pomocí MSIX app attach
- Publikace RemoteApp aplikací
- Zálohování
- Nástroje pro správu
- Nástroje pro monitoring

Nastavení klientského prostředí

GPO

- Na desktop pool můžete aplikovat libovolné politiky, včetně RDSH politik (např. Time Zone Redirection, Session Time Limits)

RDP parametry

- Na WVD můžete přednastavit libovolné RDP parametry (např. Drive redirection, Multi-monitor, Remote audio)

<https://docs.microsoft.com/en-us/azure/virtual-desktop/customize-rdp-properties>

Instalace aplikací

Aplikace instalujte pomocí MSIX app attach

- Aktuálně (03/2020) v public preview
- Aplikace jsou připojeny k OS jako virtuální disk (vhd per aplikace)

Postup: <https://docs.microsoft.com/en-us/azure/virtual-desktop/app-attach>

Další informace: <https://myignite.techcommunity.microsoft.com/sessions/THR3074>

Jak vypublikovat RemoteApp

```
Add-RdsAccount -DeploymentUrl "https://rdbroker.wvd.microsoft.com"
```

```
New-RdsAppGroup <tenantname> <hostpoolname> <appgroupname> -ResourceType "RemoteApp"
```

```
Get-RdsStartMenuApp <tenantname> <hostpoolname> <appgroupname>
```

```
New-RdsRemoteApp <tenantname> <hostpoolname> <appgroupname> -Name <remoteappname> -AppAlias <appalias>
```

```
New-RdsRemoteApp <tenantname> <hostpoolname> <appgroupname> -Name <remoteappname>  
-FilePath <filepath> -IconPath <iconpath> -IconIndex <iconindex>
```

```
Add-RdsAppGroupUser <tenantname> <hostpoolname> <appgroupname> -UserPrincipalName <userupn>
```

Zálohování

Zálohujte všechny komponenty WVD

- ADDC

- Pokud máte více než jeden doménový řadič, zálohujte ho pomocí system state.

- <https://docs.microsoft.com/en-us/azure/backup/backup-azure-system-state>

- <https://docs.microsoft.com/en-us/windows/win32/ad/backing-up-and-restoring-an-active-directory-server>

- Zdrojový image

- Pokud jste použili vlastní image pro nasazení WVD, zálohujte ho např. v rámci Blob Storage

- FSLogix profily (+ MSIX aplikace)

- Zálohujte Azure Files úložiště pomocí Azure Backup

- <https://docs.microsoft.com/en-us/azure/backup/backup-afs>

Nástroje pro správu

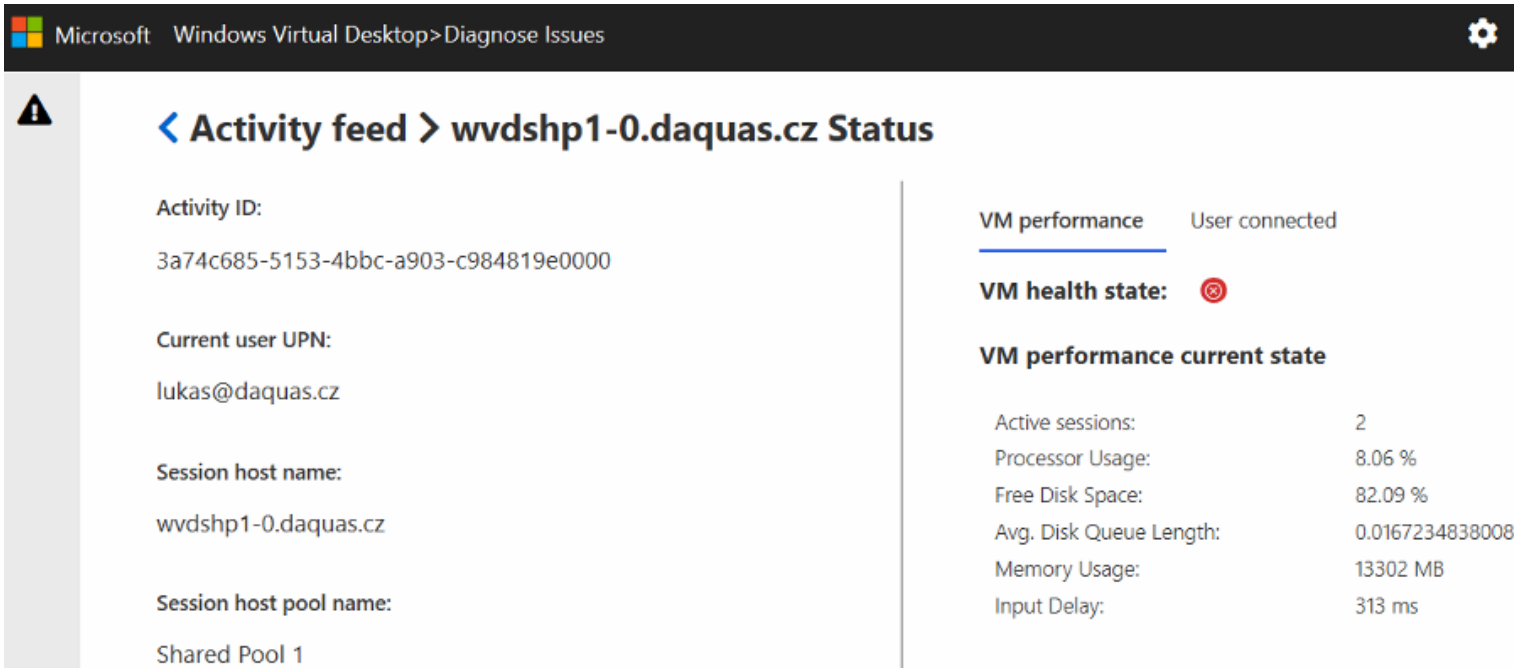
- PowerShell / CLI
- Management UI od Microsoftu (níže)
- Nástroje třetích stran

The screenshot displays the Microsoft Windows Virtual Desktop Management interface. The breadcrumb path is: Microsoft > Windows Virtual Desktop > Tenants > Daquas-WVD-Prod > Shared Pool 1. The left-hand navigation pane shows a tree view with 'WVD Tenants' at the top, followed by 'Tenants', 'Daquas-WVD-Prod', and 'Shared Pool 1'. A tooltip indicates that clicking the arrow icon expands or collapses the menu. The main content area is titled '"Shared Pool 1" Hostpool' and has three tabs: 'General', 'Hosts', and 'App Groups'. The 'Hosts' tab is active. Below the tabs, there are several action buttons: '+ Add a SessionHost', 'Edit', 'Delete', 'Restart', 'Drain Mode', and 'Refresh'. At the bottom, a table lists the session hosts in the pool.

<input type="checkbox"/>	SessionHost(FQDN)	Allow New Sessions	Agent Version
<input type="checkbox"/>	wvdshp1-0.daquas.cz	Yes	1.0.1632.1200

Nástroje pro monitoring a troubleshooting

- Log Analytics
- Diagnostics UI od Microsoftu (níže)
- Nástroje třetích stran



Microsoft Windows Virtual Desktop > Diagnose Issues

< Activity feed > wvdshp1-0.daquas.cz Status


Activity ID:
3a74c685-5153-4bbc-a903-c984819e0000

Current user UPN:
lukas@daquas.cz

Session host name:
wvdshp1-0.daquas.cz

Session host pool name:
Shared Pool 1

VM performance User connected

VM health state: 

VM performance current state

Active sessions:	2
Processor Usage:	8.06 %
Free Disk Space:	82.09 %
Avg. Disk Queue Length:	0.016723483800881
Memory Usage:	13302 MB
Input Delay:	313 ms

Sizing a cena

Sizing pro 8 kancelářských pracovníků (Office, custom aplikace)

Role	Azure zdroje	Cena PAYG	Cena Reserved Instance 1Y	Cena Reserved Instance 3Y
AD DC	B2s (2vCPU, 4GB RAM), 128GB OS + 32GB data HDD	41	29	22
Sdílený desktop	B4ms (4vCPU, 16GB RAM), 128GB SSD	146	97	73
FSLogix profily	Azure Files 80GB (10GB/uživ)	4	4	4
Záloha	DC system state + FSLogix profily (90GB)	15	15	15
Monitoring	Log Analytics (5GB data ingestion zdarma)	0	0	0
Traffic	Bandwidth 20GB	1	1	1

Volitelně:

- VPN pro připojení onprem zdrojů (Basic GW): 22 EUR
- Management UI (App Service D1 plan): 8 EUR
- Diagnostics UI (App Service D1 plan): 8 EUR

Ceny jsou Microsoft doporučené koncové, v datovém centru West Europe, měsíční, v EUR. Poslední update 03/2020.

Licenční řešení

Pro řešení postavené na desktopovém OS **Windows 10 multi-session / single-session nebo Windows 7** potřebujete některou z těchto licencí:

- Microsoft 365 E3, E5, A3, A5, **Business**, F1
- Windows E3, E5, A3, A5

Pro řešení postavené na **Windows Server 2012 R2, 2016, 2019** potřebujete

- RDS CAL s aktivní SA
- nebo RDS jako Software Subscription v CSP (pouze pro Windows Server 2019)

FSLogix je dostupný v licencích:

- Windows E3, E5
- Microsoft 365 E3, E5
- RDS CAL

