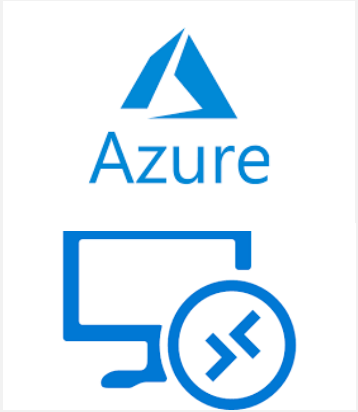
SWS COMPUTERSYSTEME
Member of ACP Group

ACP

MS Windows virtual Desktop (WvD)

Agenda

- Vor- und Nachteile einer WvD-Infrastruktur
- Grundlagen zur Infrastruktur von WvD bzw. Azure
- Grobe Kostenübersicht und Lizensierung
- Grundüberlegungen und benötigte Azure Ressourcen
- Anbindung von OnPremise-Umgebung
- Bereitstellung und Administration von WvD
- Automatische Skalierung



Vor- und Nachteile einer WvD Infrastruktur

Vorteile

- Zentralisierung der Benutzerumgebung
- Kein lokaler Workload, daher ein einfacher schneller Start ohne hohe Investitionskosten
- Anytime – Anywhere – Any Device (App oder Browser)
- Bring-your-own-Device
- Unabhängig von lokaler Infrastruktur und Verfügbarkeit (*)
- Bereitstellung in (fast) allen Azure Regionen
- Monatlich kalkulierbare Kosten pro User
- Automatisierte Skalierung (nach oben und unten)

Nachteile

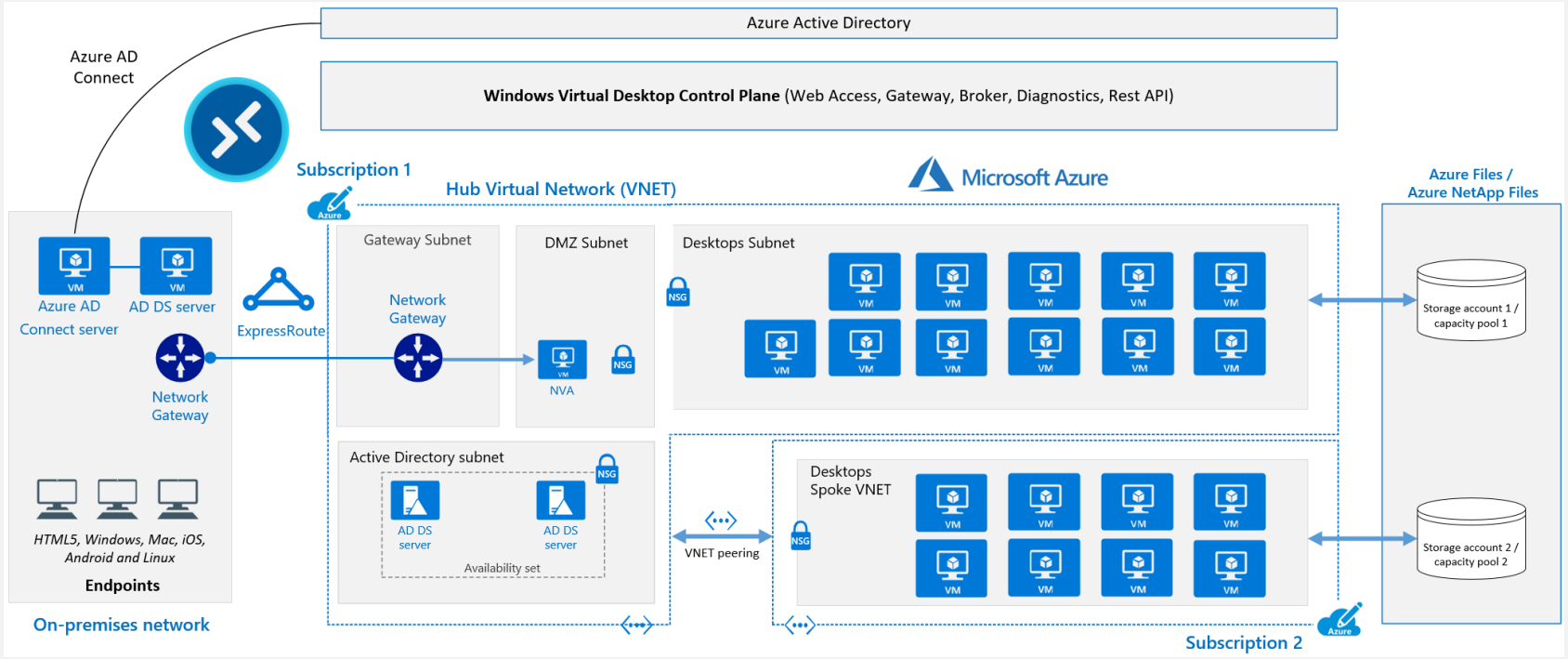
- Internetanbindung (150-300 Kbit/s für Office, bis zu 8 Mbit/s für Video **pro User**!)
- Abhängig von der MS Azure Cloud (Verfügbarkeit, Globale Störungen)
- Teuer bei „lift-and-shift“ im OnPremise Gedanken

Aber Achtung!

- Audio und Video Traffic sollte/muss lokal ausgeleitet werden (→ MS Teams!)
- Zugriffe in Hybrid-Umgebungen (→ Traffic-Kosten, Latenzen und Bandbreiten!)
- WvD ist nur ein Teil einer Gesamtstrategie

Grundlegendes

Was ist Windows virtual Desktop (WvD)?



Kostenübersicht https://azure.microsoft.com/de-de/pricing/calculator/

Szenario:

Beispiel: 100 User, 90 User zur Hauptnutzungszeit, 10 User Nebennutzungszeit

Sitzung: Multisession (mehrere User pro WvD-SessionHost)

Workload: Anspruchsvoll/Heavy (2 User pro vCPU)

GPU: nicht gefordert, nur Office-Anwendungen und Branchensoftware (keine CAD, etc.)

Anzahl Session-Hosts:

Instanz: DS3 v2 (4 vCPU, 14 GB RAM) → **ACU beachten**!

10h/5d: 12 Instanzen x 220 Stunden Laufzeit (Hauptnutzungszeit)

24h/7d: 2 Instanzen x 510 Stunden Laufzeit (Nebennutzungszeit)

OS-Disk: 12x 128 GB SSD Premium (→ SLA der Verfügbarkeit 99,9 %)

Kostenübersicht (100 User):

VMs: ca. 840,- Euro/Monat

OS-Disk: ca. 220,- Euro/Monat

Summe: ca. 1.060,- Euro/Monat

Azure VM: ACU?

ACU = Azure Compute Unit (https://docs.microsoft.com/de-de/azure/virtual-machines/acu)

SKU-Familie	ACU\vCPU	vCPU: Core
A0	50	1:1
A1–A4	100	1:1
A5–A7	100	1:1
A1_v2–A8_v2	100	1:1
A2m_v2–A8m_v2	100	1:1
A8–A11	225*	1:1
B	Varies	1:1
D1–D14	160–250	1:1
D1_v2–D15_v2	210 - 250*	1:1
DS1–DS14	160–250	1:1
DS1_v2–DS15_v2	210 - 250*	1:1
D_v3	160 - 190*	2:1***
Ds_v3	160 - 190*	2:1***
Dav4	230 - 260**	2:1****

WvD – Take Off

Fehlt da nicht noch was?

Kostenübersicht – was nicht im „Buch“ steht…

Was kommt noch dazu?

Lizenzen:

- Windows 10 Enterprise (M365 >= E3/A3/F3 oder M365 Business Premium) → ca. 15-20,- Euro/User/Monat
- Windows Server >= 2012R2 RDS CAL **mit Software Assurance**

Infrastruktur:

- VPN-Gateway (>= VPNGw1 oder >= VPNGw1AZ) → mind. 130,- Euro/Monat
- Traffic (Azure ausgehend) → pro TB ca. 70,- Euro/Monat

Storage:

- Azure Files für UserProfile (VHDX) und Redirected Folders (LRA, Hot) → pro TB ca. 70,.- Euro/Monat
- Backup (Azure Backup oder 3rd-Party) → zu klären

Security:

- Azure AD Premium P1 (Conditional Access) / Azure AD Premium P2 (Identity Protection) → ca. 5,- bis 7,- Euro/User/Monat
- Firewall (Azure Firewall, 3rd-Party) → zu klären
- Azure Bastion (Bereitstellung, Pflege) → ca. 130,- Euro/Monat

Azure IaaS

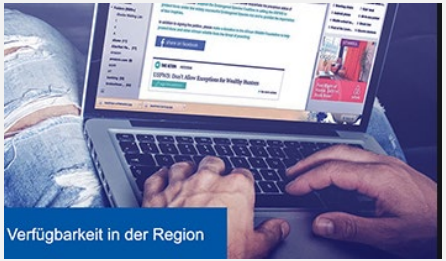
Eine WvD-Umgebung bzw. Azure ist wie ein weiterer Standort der Firma zu betrachten.

Einige Parameter können nachträglich nur sehr schwer oder gar nicht angepasst werden! Daher:

Azure IaaS: Wo fangen wir an?

Auswahl der richtigen Region nach den Kriterien:

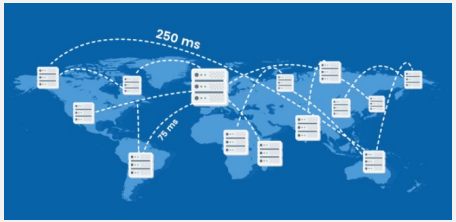
Dienstverfügbarkeit



Compliance

Kosten

Latenz



Azure IaaS: Nächste Schritte

- IP-Konzept (Eindeutig im Unternehmen)
- Namenskonzept für: Ressource-Pools, Netzwerke, Storage-Accounts, VMs, Network Security Groups, etc.
- Berechtigungskonzept (interne Abteilungen, externe Dienstleister)
- Routing und Anbindung (VPN notwendig oder „Insellösung“) → Abhängigkeiten zu Applikationen oder Dienstleistern?
- Security, Security, Security (IaaS, Verschlüsselung, Anbindung, User-Auth, etc.)

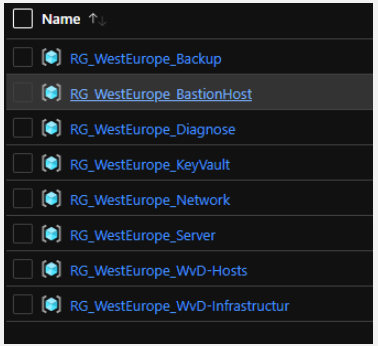
WvD Step 1: Infrastruktur

In welcher Region:

- West/North Europe oder Germany West Central
- Verfügbarkeit, Compliance, Kosten, Latenzen

Erstellung von Ressource-Groups für:

- Diagnose-Konto für VMs
- Netzwerk (vNet, VPN-Gateway, Firewall, etc.)
- BastionHost
- KeyVault (Datenverschlüsselung)
- Server-Umgebung (DC, App-Server, DB-Server, etc.)
- WvD-Ressourcen (GoldenImage, Snapshots, Image Gallery, Automation-Account, etc.)
- WvD-Session-Hosts (tagsächliche Worker)
- Backup



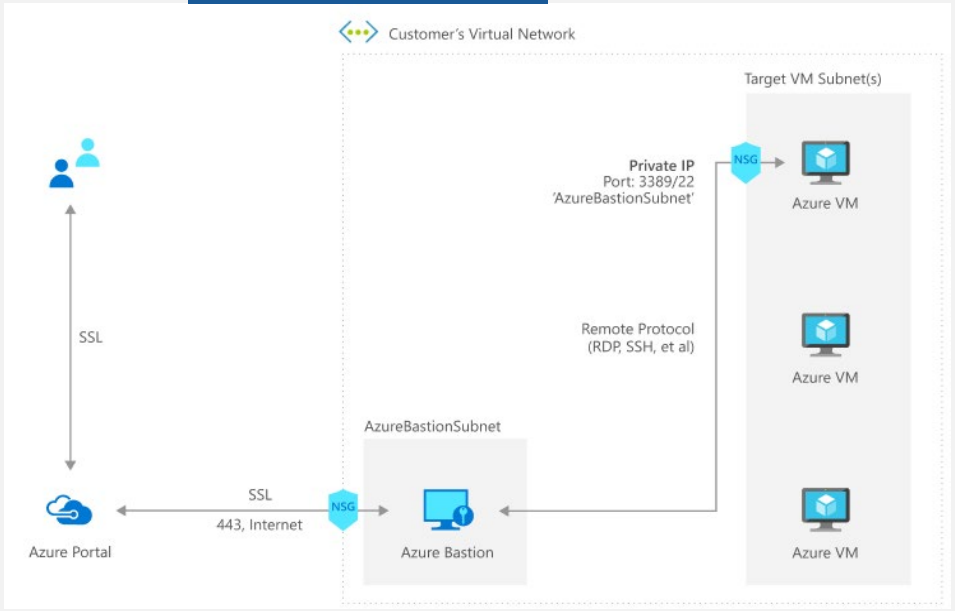
Warum?

Auf Ressource-Groups können Berechtigungen gesetzt werden für die Administration → Berechtigungskonzept, wer kann/macht was?

WvD Step 1: Infrastruktur

Erstellung der Infrastruktur:

- vNet und Subnetz
- VPN-Gateway und Anbindung an Zentrale
- BastionHost
- KeyVault (Datenverschlüsselung)
- Backup



WvD Step 2: Authentifizierung

Nachdem die Infrastruktur geklärt ist benötigen wir eine Authentifizierungsstelle.

WvD benötigt Kerberos-Authentifizierung, Azure AD ist oAuth/Open ID Connect oder SAML.

- WvD-Sesstion-Host
- Azure-Files

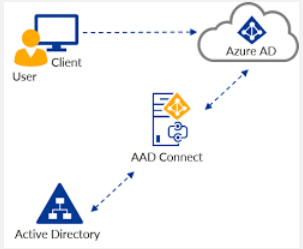
Bereitstellung eines MS AD Domain Controllers in Azure IaaS:

- Installation W2K19 VM als DS2_v2 [smalldisk]
- Verfügbarkeitszonen beachten!
- Zusätzliche Managed Disk für AD-Datenbank (NTDS.dit/SYSVOL) einbinden → Hostcaching deaktivieren!
- Domain-Join ausführen (DC-Promo)
- VM ggf. anpassen auf Burst-VM (→ „Good-Enough“-Strategie → Kosten sparen ☺)

WICHTIG!

Azure AD Connect einrichten damit sich die Remotedesktop-App auch anmelden kann ☺

Passwort-Hash-Synchronisierung aktivieren ☺



WvD Step 2.1: GPOs

Für die WvD SessionHosts sollte im AD eine eigene OU pro Pool (Aufgabenbereich) definiert werden.

GPO Inhalt:

- Default Einstellungen für Profile (Profilspeicherort, Redirected Folders, etc.)
- Einschränkungen am Client (Zugriff Laufwerk C:\, Systemsteuerung ausblenden, Desktop-Symbole, etc.)
- Automatisches Abmelden bei getrennten Sitzungen (Session-Timeout)
- Applikationseinstellungen (z. B. Office für vertrauenswürdige Speicherpfade)
- Zuweisung Netzlaufwerke
- Zuweisung Drucker
- etc.

Es können auch Richtlinien sein, welche im Unternehmen schon vorhanden sind → Absicherung des WvD-Clients/Profile.

WvD Step 3: Speicherkonten

Zur Bereitstellung der Speicherressourcen der Userprofile (VHDX) sowie der Redirected Folder gibt es zwei Möglichkeiten

OLD-School: File-Server

- VM in Azure
- Freigaben im File-System der VM
- Kennen wir von OnPremise

Innovativ: Azure Files

- Azure PaaS-Dienst
- Keine Pflege von Betriebssystem
- Pay-As-You-Go (Abhängig von Premium/Standard)
- 5 TB Standardkapazität pro Speicher-Account
- auf 100 TB erweiterbar durch „Schieberegler
- Nahtlose Integration in ActiveDirectory

WvD Step 3.1: Azure Files

Auch hier gibt es Grenzwerte, Limitierungen und Kosten zu beachten!

Premium = SSD-Speicher, konfigurierte Größe muss bezahlt werden
Standard = HDD-Speicher, tatsächlich belegte Größe muss bezahlt werden
Replikation = LRS, GRS, ZRS, GZRS

Kapazität und Performance Premium:

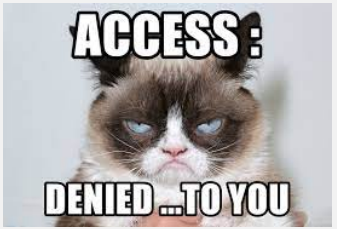
Kapazität: 100 TB — Kosten: ca. 300,- Euro/TB/Monat
Performance: 100.000 IOPs
6,6 GB/sec read / 4,4 GB/sec write → Ist linear Abhängig der Bereitgestellten Kapazität

Kapazität und Performance Standard:

Kapazität: 5 TB (bis 100 TB) — Kosten: ca. 100,- Euro/TB/Monat (Transaction Optimized)
Performance: 1.000 IOPs (ab 5 TB 10.000 IOPs) — Kosten: ca. 70,- Euro/TB/Monat (Hot)
(per Ticket bis zu 50.000 IOPs)
300 MB/sec read/write

Praxis-Tipp: Mehrere Speicherkonten für unterschiedliche Anwendungen erstellen und Speicherkontenname max. 14 Zeichen!

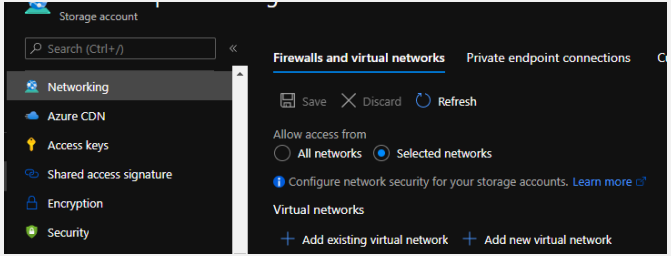
WvD Step 3.2: Azure Files Security



Speicherkonten müssen geschützt werden!

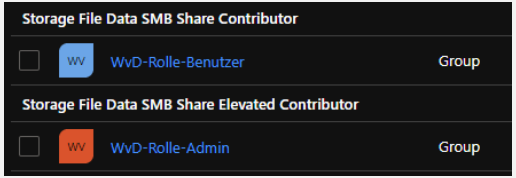
Infrastruktur Zugriff:

- Begrenzung auf einzelnes vNET oder IP-Ranges (auch VPN berücksichtigen!)
- Zugriff der Public-IPs beschränken → überhaupt notwendig (Backup?)
- Private-Endpoint erstellen für internen Zugriff
- Public DNS-Eintrag löschen



Benutzer Zugriff:

- AD-Implementierung
- Freigabeberechtigungen über RBAC bzw. IAM-Zugriffssteuerung
- File-Berechtigung über „NTFS“-Rechte



Datensicherheit:

- (Eigenen) Verschlüsselungs-Key über KeyVault zuweisen
- Backup einrichten

Können wir jetzt endlich anfangen mit WvD?

WvD Step 4: Erstellung Session-Hosts

Drei Schritte zum Glück…

1. Golden Image bzw. Master Image erstellen
2. Shared Image Gallery erstellen zum Verwalten der Images
3. WvD-SessionHost bereitstellen incl. Workspace

WvD Step 4.1: Golden Image bzw. Master Image

Golden Image/Master Image:

Aufgabe: Grundinstallation als Template für die SessionHosts

ToDo: Wird mit lokalen User (ohne AD-Join, etc.) installiert

WvD Optimierungs-Script ausführen (Grundanpassung Windows 10)

Applikationen und Branchensoftware installieren

Ggf. Applikationstuning konfigurieren! → MS Teams Optimierung für WvD bezüglich Audio/Video

Vor dem Sysprep wird ein Snapshot erstellt, damit am Image nachträgliche Anpassungen durchgeführt werden können (sysprep geht max. 8x in Windows 10 Enterprise! → Löschen, neu erstellen)

VM wird beim wandeln in ein „VM Image“ gelöscht, Ressourcen bleiben aber erhalten → Kosten!

Aufwand: Abhängig von Applikationen, mind. 1-2 Stunden für Grundsetup

WvD Step 4.2: Shared Image Gallery

Shared Image Gallery:

Aufgabe: Verwaltung und Versionspflege von Images

ToDo: Erstellung der Shared Image Gallery

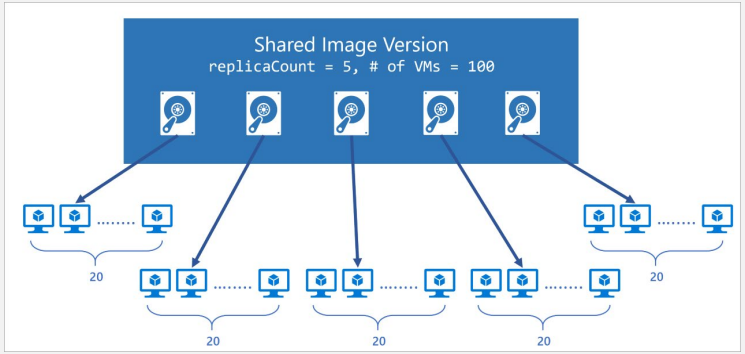
Neue Image-Definition hinzufügen

Achtung bei der Versionsnummer!

3-Stellig mit Punkt getrennt, es empfiehlt sich das aktuelle Datum in umgekehrter Schreibweise (2021.05.11)

Immer die Versionsnummer mit der höchsten Zahl wird beim erstellen der SessionHosts verwendet!

Aufwand: ca. 20-30 Minuten (Bereitstellung)



WvD Step 4.3: SessionHosts

WvD SessionHost:

Aufgabe: Erstellung der SessionHosts

ToDo: Erstellung eines HostPools

Definition ob User

- Horizontal (gleichmäßig über alle verfügbaren SessionHost) oder
- Vertikal (einen SessionHost nach den anderen füllen)

verteilt werden.

Richtiges Image auswählen!

Domain-Join konfigurieren (macht die Plattform für uns)

Aufwand: ca. 5-15 Minuten (Bereitstellung incl. Domain-Join)

WvD Step 4.3: Was passiert jetzt?

Bei der Bereitstellung der SessionHost werden folgende Ressourcen angelegt:

Web-Access-Service

HTML5-Service für den Zugriff des Clients auf die Ressourcen. Absicherung über MFA möglich (Azure AD)

Gateway

Verbindungsglied zwischen dem Client/RemotedesktopApp und dem Session-Host nach der erfolgreichen Authentifizierung

Verbindungsbroker/LoadBalancer

Regelt die Verteilung der User-Sessions über Verfügbarkeitsgruppen auf die einzelnen Session-Hosts

Diagnose

Monitoring und Logging

Add-Ons

REST-API Schnitstellen für 3rd-Party Hersteller zur Verwaltung der Umgebung

WvD Step 4.4: Workspace und Zugriff

So, Umgebung läuft, warum kann ich mich noch nicht verbinden?

Application Group

Per Default wird eine [HostPoolName]-DAG App-Group erstellt. Darin versteckt sich der „RDP-Link“ für den Client

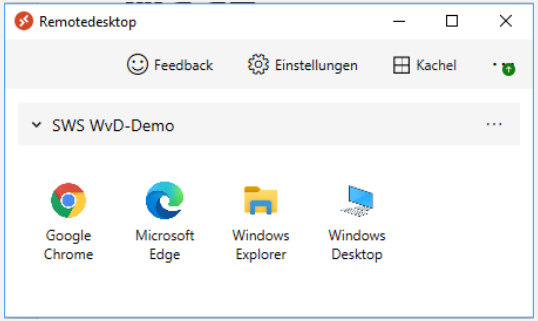
Je nach Zugriffsvariante sollten auch Applikationen freigegeben werden, welche dem User direkt angezeigt werden.

→ Erstellung mehrerer Application Groups für verschiedene Fachanwendungen

→ Pro App-Group können User berechtigt werden (evtl. interessant bei Softwarelizensierung?)

Workspace

Aus den App-Groups wird dann der Workspace definiert (Sammlung aus Applikationen) welche der User dann im Client sieht.



WvD Step 4.4.1: RDP-Einstellungen

Pro SessionHost-Pool können die Einstellungen für die RDP-Sitzung konfiguriert werden:

Sitzungsverhalten (Auszug)

→ Client reconnect

→ Bandbreitenerkennung (Netzwerkerkennung)

→ Komprimierung

Lokale Ressourcen (Auszug)

→ Mikrofonumleitung

→ Audio- und Videoumleitung

→ Kameraumleitung

→ USB, lokale Laufwerke und Drucker

→ Zwischenablage

→ Smart Card

Anzeige-Einstellungen (Auszug)

→ Multi-Display-Support

→ Vollbild oder Fenster

→ Desktop-Größe (Auflösung)

WvD Step 4.4.2: MSIX

Bereitstellung von Applikationen über Container (VHDX-File)

Vorteile von MSIX gegenüber der klassischen App-Installation

→ Benutzer, OS und Apps werden voneinander getrennt

→ Bei dynamischer Bereitstellung müssen keine neuen Pakete erstellt werden

→ Die Anmeldezeit für Benutzer wird verkürzt

→ Infrastrukturanforderungen und –kosten sinken

Doing:

Applikationen werden in Containern (also VHDX-Dateien) bereitgestellt → Applikation muss MSIX-File sein!

VHDX-Dateien sind wiederum auf Azure Files abgelegt.

Verhalten:

Der Endanwender kennt in der Applikation keinen Unterschied und das MasterImage wird noch einfacher zu pflegen.

WIN-WIN-Stiuation für Admin und User ☺

WvD Step 5: Auto-Scale

AlwaysOn OK, aber muss das sein bzw. muss die gesamte Umgebung 24/7 laufen?

Anzahl Session-Hosts:

Instanz:	DS3 v2 (4 vCPU, 14 GB RAM) → **ACU beachten**!
10h/5d:	12 Instanzen x 220 Stunden Laufzeit (Hauptnutzungszeit)
24h/7d:	2 Instanzen x 510 Stunden Laufzeit (Nebennutzungszeit)
OS-Disk:	12x 128 GB SSD Premium (→ SLA der Verfügbarkeit 99,9 %)

Implementierung von Auto-Scale:

→ Azure Automation-Account	→ Berechtigung zur Ausführung (wie oft läuft der Vorgang)
→ Azure LogicApps	→ Startet den Webhook (Scheduler)
→ Azure Webhook	→ Startet das Runbook (was soll gemacht werden)
→ PowerShell Runbook	→ Das Script was letztendlich was tut

Parameter (Auszug):

`LimitSecondsToForceLogOffUSer`	→ Sekunden, bis User automatisch abgemeldet werden
`LogOffMessageBody`	→ Nachricht an den User („[…] in 5 Minuten ist Feierabend, bitte speichern […])
`MaintenanceTagName`	→ Tag, wenn bestimmte VMs nicht vom Script behandelt werden sollen
`SessionThresholdPerCPU`	→ Anzahl User pro CPU für die Automatisierung
`BeginPeakTime`	→ Beginn Business-Hour
`EndPeakTime`	→ Ende Business-Hour

WvD – Endlich fertig?

WvD Step 6: Und was fehlt noch?

Punkte die man nicht vergessen sollte, OnPremise machen wir das doch auch ☺

Virenschutz:

Azure Defender Endpoint AV ist (z. B. bei M365 Business Premium) mit lizensiert.

Konfiguration über AD GPO zur Registrierung → Dynamische Azure AD Gruppe → Intune Policy

HDD-Verschüsselung mit Bitlocker:

Key-Verwaltung über KeyVault oder internen bestehenden Ressourcen.

Monitoring der SessionHosts:

Diagnose-Konto erstellen (VM Identity), Boot-Diagnose aktivieren (CPU/RAM)

Azure Security-Center:

Überwachung der VM notwendig (Kosten ca. 15,- Euro pro VM/Monat)

Windows Updates:

Von WSUS OnPremise?? → Besser über Guest-Update-Policies in Azure ☺

Softwareverteilung:

via M365 Intune-Policies?

Und, und , und…

→ Alles was ein lokaler Client/TS auch braucht!

SWS Managed Service für Windows virtual Desktop

SWS Managed Service für Windows virtual Desktop

Service Operation	Inkludierte administrative Tätigkeiten • Zuweisen von Apps und Desktops • Freigabe von Zugriffsberechtigungen • Beheben von globalen Authentifizierungsstörungen • Profilmanagement (zurücksetzen, Profilspeicher anpassen) • Sitzungsmanagement (Session abmelden, neu starten) • Hinzufügen von Session Hosts in einem Host-Pool Typ Pool • Pflege der Dokumentation
Health Check	• Session Host Zeiten • Bewertung der WVD Ressourcen • Belegung/Auslastung Profilspeicher • Windows Update Status • Auswertung Imageversionen • Auswertung Ereignisprotokoll • Auswertung aus Monitoring
Wartung & Pflege	• Windows & Office Updates • Versionsbereinigung der Images • Profilpflege • Anpassen der Betriebszeiten • VM Session Host Ressourcen anpassen
Monitoring	Monitoring folgender Parameter • CPU • RAM • Festplattenauslastung • Verfügbare Sitzungen im Multiuserbetrieb

Die monatliche Gebühr je Service-Baustein ist abhängig der gesamt Userzahl.

Bei Interesse gehen Sie bitte auf Ihren Vertriebskontakt der SWS/ACP zu bzw. über info@sws.de

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?