

Azure Advanced

Azure Hands On Lab November 15th 2019

v1.0 door : Gino van Essen
Stephan van de Kruis
Gido Veekens



2tCloud



Inhoud

Introductie.....	3
Stap 1 : Voorbereidingen.....	4
Klantcase	5
Gebruikers.....	5
Applicaties.....	5
Werkplekken	6
Infrastructuur	6
Beheer	6
Wensen	6
Bezwaren	7
Stap 2: Maak een Proof-of-Concept ontwerp	8
Stap 3: Presenteer je oplossing aan de klant.....	9
Bronnen.....	10
Azure Architecture	10
Partner Resources	10
Documentatie	10

Introductie

Estimated time to complete this lab

240 minuten

Doelstellingen

Tijdens dit lab deel je ervaringen en kennis, zodat je gezamenlijk tot een oplossing komt die aansluit bij de wensen en eisen van de klant. Onderwerpen die tijdens dit lab aan bod zullen komen zijn onder meer Windows Virtual Desktop en Microsoft 365. Het gaat daarbij niet om specifieke hands-on kennis, maar we richten ons met name op het ontwerpen van een totaaloplossing met aandacht voor governance en security.

Benodigdheden

Om dit lab te maken heb je een aantal voorzieningen ter beschikking;

- Laptop/notebook met WiFi
- Flipover

Materialen

Alle bronmaterialen voor dit lab worden beschikbaar gesteld via;

<https://github.com/Copaco/handsonlab/>

Stap 1 : Voorbereidingen

Geschatte tijd om deze activiteit te voltooien

30 minuten

Doelstellingen

In deze stap is het belangrijk om;

- Te bepalen uit welke kennis en ervaring je team bestaat
- Je voor te bereiden op het onderwerp door je goed in te lezen in de klantcase
- Te bepalen wie jullie oplossing gaat presenteren aan de klant

Voorbereidingen

De tafel waar je aan zit vertegenwoordigt een Managed Service Provider (MSP). De klant is toe aan een nieuwe oplossing en heeft de vraag hiervoor uitgezet bij meerdere partijen. Jullie concurreren dus met meerdere MSP's. Als MSP hebben jullie een voorkeur voor het ontwikkelen van oplossingen binnen Microsoft Azure.

Stel jezelf kort voor en geef aan waar je kennis en ervaring liggen met de onderwerpen;

- Windows Virtual Desktop
- IaaS
- Microsoft 365
- Security
- Governance
- Management

Op deze manier leer je je team snel kennen. Dat is belangrijk om gezamenlijk tot een zo compleet mogelijke oplossing te komen en je klant te overtuigen.

Zorg voor een pakkende naam voor jullie zojuist gestarte MSP-organisatie!

De klantcase is op hoofdlijnen toegelicht bij de introductie. In de volgende secties wordt de case verder op inhoud gespecificeerd. Neem belangrijke details goed in je op en denk al na over een oplossingsrichting. Later ga je hierover in discussie.

Klantcase

De klant is een relatief kleine zorginstelling die opereert vanuit meerdere locaties. Er is een hoofdkantoor van waaruit de afdelingen als HR, finance, IT en directie opereren. Daarnaast zijn er twee zorglocaties waar patiënten worden behandeld.

De huidige IT-omgeving bestaat al enige jaren en is aan vervanging toe. Daarnaast gaat het hoofdkantoor binnen enkele maanden verhuizen en wil men geen voorzieningen meer treffen voor een serverruimte in eigen beheer. Omdat men zelf de organisatie op gebied van IT niet 24/7 kan ondersteunen, wil men het beheer uitbesteden aan een MSP. Daarvoor worden een aantal partijen benaderd, die de kans krijgen hun oplossing te pitchen.

Gebruikers

Er zijn grofweg 2 persona's te definiëren in de organisatie;

- 40 kantoorwerkers. Deze groep zijn voornamelijk gebonden aan kantoortijden en werken vanuit kantoor. De werkzaamheden van deze groep gebruikers is zeer divers.
- 140 zorgwerkers. Deze verzorgen de patiënten 24x7 in meerdere shifts. Gebruikers maken incidenteel gebruik van een werkplek. Zij hebben een beperkte hoeveelheid taken die zij op hun werkplek uitvoeren.

Applicaties

Binnen de organisatie worden een aantal applicaties gebruikt;

Office 365	Iedere gebruiker heeft de beschikking over een Office 365 E3 licentie met Exchange Online mailbox. Daarnaast is Office ProPlus beschikbaar gesteld op iedere werkplek.
Elektronisch Patiënten Dossier (EPD)	Alle gebruikers hebben toegang tot deze applicatie op basis van Active Directory integratie middels LDAP. Binnen de applicatie is een permissiestructuur van toepassing die bepaalt welke toegang een medewerker heeft. Dit is een client/server toepassing met een SQL 2008R2 database als backend.
HR applicatie	Alleen medewerkers van de afdeling HR krijgen toegang tot de clientinstallatie van deze applicatie. Deze communiceert met een database gebaseerd op SQL 2016. De client-applicatie wordt nu d.m.v. MSI uitgerold naar endpoints.
HR portal	Iedere medewerker krijgt toegang tot de HR portal die via HTTPS beschikbaar wordt gesteld vanaf de applicatieserver. Binnen deze portal kunnen zij eigen gegevens benaderen en organiseren als salarisstroken, verlof, etc. Gebruikers hebben separate credentials voor deze applicatie, die geen meervoudige authenticatie of SSO ondersteund.
Finance	Medewerkers van de afdeling Finance krijgen toegang tot deze applicatie die wordt aangeboden via SaaS. Hiervoor is geen eigen infrastructuur benodigd. Deze applicatie ondersteund SSO, maar dat wordt niet gebruikt.

Werkplekken

Aansluitend bij de verschillende persona's, zijn er twee groepen endpoints te definiëren;

- Kantoorwerkers hebben een laptop die voorzien is en beheerd wordt door de organisatie. Dit is een Windows 10 Pro apparaat dat aangemeld is op het domein. Thuis kunnen zij gebruik maken van een RDS sessie.
- Zorgverleners maken gebruik van een vast werkplek die op de verschillende afdelingen staat en gedeeld wordt door meerdere gebruikers. Het gaat om ongeveer 20 fysieke werkplekken met Windows 7 die een RDP-sessie opbouwen naar een RDS omgeving. Zij werken niet vanuit huis of andere locaties.

Infrastructuur

Er is sprake van een MPLS netwerk-infrastructuur, waarbij het hoofdkantoor en twee zorglocaties zijn aangesloten. Er is één gezamenlijke internet out-break. Alle servers en primaire infrastructuur staan op het hoofdkantoor. Het gaat daarbij om een VMware-omgeving met daarop de volgende virtuele servers en rollen;

Naam	CPU	Mem	OS	Rol
DC-1	2	8	Windows Server 2016	Domain Controller + AD Connect
DC-2	2	8	Windows Server 2016	Domain Controller
FS	2	8	Windows Server 2016	Fileserver
APP-1	4	32	Windows Server 2008 R2	EPD applicatieserver o.b.v. SQL 2008R2
APP-2	2	16	Windows Server 2012 R2	HR applicatie o.b.v. IIS en SQL 2016
RDS-GW	2	8	Windows Server 2012 R2	RDS Web + Gateway
RDS-CD	2	8	Windows Server 2012 R2	RDS Connection Broker + License Server
RDS-SH-1	4	64	Windows Server 2012 R2	RDS Session Host met client-applicaties
RDS-SH-2	4	64	Windows Server 2012 R2	RDS Session Host met client-applicaties
RDS-SH-3	4	64	Windows Server 2012 R2	RDS Session Host met client-applicaties
BS	2	8	Windows Server 2012 R2	Backup Server

Er is een verscheidenheid aan besturingssystemen. Omdat in de dagelijkse operatie veel aandacht uitgaat naar gebruikersondersteuning en werkplekbeheer, worden zaken als upgrade en migraties op een laag pitje uitgevoerd.

Beheer

Op dit moment zijn er twee beheerders in dienst van de organisatie die zich bezig houden met een combinatie van systeem-, netwerk- en werkplekbeheer. Applicatiebeheer wordt uitbesteedt aan de betreffende applicatieleverancier. Beiden beheerders worden aangestuurd door een IT manager.

Bij onderhoud aan bijvoorbeeld de fileserver, RDS of applicatieservers is er direct invloed op de beschikbaarheid. Voor bijvoorbeeld het EPD en RDS-brokers is dat problematisch, aangezien deze 24x7 beschikbaar moeten zijn voor de zorgwerkers. De afdeling IT merkt daarom dat het lastig is om in een kleine samenstelling te zorgen voor de juiste beschikbaarheid. Daarnaast hopen ze met hulp van een externe dienstverlener meer aandacht te kunnen vestigen op het toevoegen van waarde voor de organisatie.

Er is recent een audit geweest waaruit blijkt dat er veiligheidsrisico's zijn door het achterlopen met security updates. Daarnaast bleek één van de kritieke aandachtspunten het ontbreken van meervoudige authenticatie.

Dagelijks wordt een backup gemaakt van alle VM's gemaakt naar tape. Gegevens op de laptops van gebruikers worden niet meegenomen in het backup-schema. Het wisselen en offsite brengen van de tapes is een taak van de IT-afdeling.

Wensen

Naast de aangestipte aandachtspunten in het klantcase, zijn er een aantal standpunten die de klant heeft gedeeld;

- Men loopt nu achter de feiten aan, maar wil in algemene zin met deze stap klaar zijn voor de toekomst. Overziet niet waar te beginnen en wat er allemaal bij komt kijken.
- De organisatie wil kantoorwerkers beter faciliteren in thuiswerken. Microsoft Teams moet daar een bijdrage aan leveren, zodat er eenvoudig digitale meetings plaats kunnen vinden met audio & video en worden samengewerkt aan documenten.
- Bij verlies of defect van een laptop gaat gebruikersdata die lokaal staat nu verloren. Dat heeft tot problemen geleid, een gebruiker zou zich daar geen zorgen over moeten maken.
- Beveiliging moet in lijn zijn met moderne best practices en aansluiten bij conclusies uit de recente audit.
- De oplossing moet passend zijn, echter speelt het budget uiteraard een belangrijke rol. Er zou daarom een goede balans moeten zijn tussen beiden.
- Men wil niet meer investeren in een eigen datacenter, operationele kosten passen beter in de financiële huishouding van de organisatie.
- De druk op beheerders zou moeten afnemen, zodat zij zich bezig kunnen houden met het toevoegen van waarde in plaats van het blussen van brandjes op dagelijkse basis.

Als MSP hebben jullie zelf natuurlijk ook een aantal belangen en/of uitdagingen;

- Hoe ga je om met beheer van meerdere klantomgevingen?
- Welke zaken kun je reproduceerbaar maken, zodat je ze niet voor iedere klant opnieuw bij elkaar hoeft te klikken in de Azure Portal?

Waarschijnlijk kunnen jullie gezamenlijk vanuit jullie ervaringen tot meerdere aandachtspunten komen die positief bijdragen aan de oplossing voor de klant.

Bezwaren

De klant heeft een aantal bezwaren uitgesproken;

- Men is bang dat de publieke cloud zal leiden tot een verhoging van de kosten.
- Biedt de publieke cloud wel voldoende aandacht voor security en compliancy?
- We hebben in het verleden al licenties aangeschaft voor Windows Server en SQL server, is er sprake van kapitaalvernietiging of kunnen we deze meenemen?
- Onze IT beheerders hebben nu alle rechten, maar omdat in de nieuwe omgeving een deel van hun werkzaamheden wordt uitbesteed zouden die rechten moeten worden beperkt.
- Biedt de publieke cloud wel voldoende performance?
- Is de oplossing technisch haalbaar en gebruikersvriendelijk? We zouden de oplossing daarom graag toetsen voor we hem in gebruik nemen.

Stap 2: Ontwerp een Proof-of-Concept

Geschatte tijd om deze activiteit te voltooien

150 minuten

Doelstellingen

In deze stap is het belangrijk om een ontwerp te maken dat aansluit bij de uitdagingen uit de klantcase. Ga in discussie met je teamleden en zorg dat je een aantal zaken kunt opleveren;

1. Schematische tekening van de omgeving
2. Bill of Materials
3. Oplossingen voor de probleem van de klant

Ontwerpfase

Gebruik de flipover om je oplossing te schetsen en ontwerpkeuzes vast te leggen. Maak daarnaast gebruik van je laptop om research te doen indien dat nodig is. Mocht je vragen hebben, vergeet dan niet de klant (trainers) te vragen om aanvullende input.

Aandachtspunten die tijdens de review aan bod kunnen gaan komen zijn bijvoorbeeld;

- Welke Azure componenten gebruik je?
- Van welke licenties maak je gebruik en waarom?
- Welke maatregelen treffen jullie om security te verbeteren?
- Waar houden jullie rekening met governance?
- Hoe bereik je een beheersbare en reproduceerbare omgeving voor jullie als MSP?

Stap 3: Presenteer je oplossing aan de klant

Geschatte tijd om deze activiteit te voltooien

60 minuten

Doelstellingen

In deze stap is het belangrijk dat je alle informatie van het team voorhanden hebt, zodat de presentator van jullie oplossing deze goed kan overbrengen op de klant en andere teams. Je krijgt vragen en feedback uit de groep. Probeer antwoord te geven op de uitdagingen van de klant. Maar richt je vooral ook op de unieke voordelen die de door jullie gekozen oplossing met zich meebrengt.

Vervolgens is het ook de bedoeling dat je actief meedoet bij de presentatie van de andere oplossingen. Accepteer dat er overeenkomsten en verschillen zitten in de uitwerking van de oplossing. Geef feedback of stel vragen als dat nodig is. Uiteindelijk krijgt iedere MSP de gelegenheid om zijn oplossing te pitchen.

Bronnen

Ter research en onderbouwing van je ontwerpkeuzes is het vaak verstandig om gebruik te maken van een aantal bronnen. Om je op weg te helpen zijn een aantal relevante bronnen hieronder opgenomen.

Azure Architecture

<https://docs.microsoft.com/nl-nl/azure/architecture/>

https://github.com/microsoft/WVD_Network_Reference_Architecture

Partner Resources

<https://www.microsoft.com/azure/partners/windows-virtual-desktop>

<https://www.microsoft.com/microsoft-365/partners/resources>

<https://www.microsoft.com/azure/partners/resources/download/windows-virtual-desktop-lighthouse-partner-guide>

Documentatie

<https://docs.microsoft.com/nl-nl/azure/virtual-desktop/>

<https://docs.microsoft.com/nl-nl/azure/lighthouse/>

<https://docs.microsoft.com/nl-nl/azure/governance/>

<https://docs.microsoft.com/nl-nl/azure/security/>