**UZ Brussel Installatie Voorwaarden**

**Checklist**

# Doelstelling

Dit document omvat een checklijst opgesteld door de IT-dienst van UZ Brussel.

Indien een of meerdere van vermelde vereisten niet wordt voldaan kan dit resulteren tot een negatief advies voor aankoop.

De bedoeling is om een vlotte doorstart van het project na de aankoopprocedure te kunnen uitvoeren en te plannen (resources etc …). Voor bijkomende vragen of info kan je contact opnemen met de systeem ploeg (security@uzbrussel.be).

Dit document is een vereenvoudigde versie van het complete Installatie Voorwaarden document.  
Bij oplevering wordt de installatie met een system engineer van UZB overlopen om te kijken of alle guidelines zijn gevolgd. Deze kan & zal ook dienen als een basiskennis overdracht.

# Licenties

|  |  |
| --- | --- |
|  | Antwoord |
| Niet afgedwongen door hardware matige oplossingen zoals keys & dongles? |  |
| Fixed MAC adres/VM Hardware ID nodig? |  |
| Enkel nodig voor productie? |  |
| OS/DB/Ondersteunende licentie nodig? |  |
| Indien de betreffende licentie(s) als pakket onder OEM worden voorzien vanuit de aanbieder, gelieve dan hiervoor een document met bewijs eveneens mee te sturen. |  |
| Post mortem data recovery procedure? |  |
| Geldigheidsduur licentie – on line activatie nodig - grace period... |  |

# Infrastructuur

|  |  |
| --- | --- |
|  | Antwoord |
| Rollbackscenario updates? (incl mogelijke DB scripted rollback) |  |
| Update zonder downtime? (indien niet, wat is de downtime?) |  |
| Totaalconcept nog 5 jaar in verkoop,  10 jaar onder support? |  |
| Toegangsbeheer & RBAC minstens gekoppeld aan UZB MS AD via Azure AD ? |  |
| Toepassen MFA mogelijk? |  |
| MS Exchange Online (o365) compatible? (zie installatie voorwaarden voor beperkingen) |  |
| Client | Desktop/Laptop/Tablet/… |
| Client & licentie aangekocht door UZB? |  |
| Verbonden apparatuur voorzien door UZB? |  |
| Windows versie (voorkeur = 10 LTSB of later)? |  |
| Kan oplossing overweg met VDI (vmware Horizon)? |  |
| Clients zijn lid van uzbrussel.be AD-domein, beheerd via GPO’s. Aanpassingen nodig? (indien niet AD joined vereist, argumenteer) |  |
| Client software in SCCM formaat? (liefst MSI) incl handleiding tot deploy? |  |
| Andere browser dan Microsoft Edge of Google Chrome ? |  |
| Bezwaar tot laatste versie van Adobe Acrobat Reader ? |  |
| Bezwaar tot gebruik standaard UZB  anti-virus client ? (TrendMicro ApexOne) |  |
| Exclusions nodig voor anti-virus client ? |  |
| Wordt er gebruik gemaakt van socket-based communicatie? (waarop full scan van anti-virus een negatief effect kan hebben)? |  |
| Kan oplossing overweg met UAC op de client ? |  |
| Kan de oplossing draaien zonder local admin rechten ? (harde eis vanuit UZB) |  |
| TeamViewer/WebEx/VNC/etc nodig ? (enkel na overleg met UZB ICT) |  |
| Andere versie dan MS Office 2016 32bit nodig ? |  |
| Java nodig ?  Zoja, naast geïnstalleerde versie draaien. |  |
| Microsoft .NET nodig ? Zoja, aligneren met huidige UZB versie of zorgen dat deze niet interfereert met UZB versie. |  |
| Internet toegang vereist ? Motiveer. |  |
| Installatiepad, bestandstructuur en schijfindeling gekend ? (zoja, leg uit) |  |
| Bezwaar tegen gebruik UZB CA ? Of is er publiek certificaat vereist ? |  |
| Bezwaar tegen Windows security patching ? |  |
| Server |  |
| Bezwaar tegen virtuele server ? |  |
| OVA/OVF, of server aangeleverd door UZB ? |  |
| Onderliggende CPU is AMD Epyc. Intel emulatie vereist ? |  |
| MS Windows 2019 (1809), 2022, CentOS 8.x of RHEL8? |  |
| Draait oplossing op Operating Systeem dat nog minstens 3 jaar gesupporteerd is ? |  |
| Is server binnen geleverde oplossing aangesproken met zijn FQDN ? (domainname uzbrussel.be, FQDN die op internet beschikbaar moet zijn zal split DNS gebruiken) |  |
| Ondersteunt de oplossing HA/vMotion op vSphere 7.x ? (indien niet, argumentatie vereist) |  |
| Is Fault Tolerance nodig ? |  |
| Servers zijn lid van uzbrussel.be AD-domein, beheerd via GPO’s (zie installatie voorwaarden voor opsomming). Aanpassingen nodig? (indien niet AD joined vereist, argumenteer) |  |
| Software installatie nodig ? (zoja, MSI-formaat, vergezeld van installatiehandleiding) |  |
| Bezwaar tegen (bepaalde?) MS Windows security patches ? Binnen de 2 weken na vrijgave door Microsoft aan te geven. |  |
| Bezwaar tot gebruik standaard UZB  anti-virus client ? |  |
| Exclusions nodig voor anti-virus client ? |  |
| Wordt er gebruik gemaakt van socket-based communicatie ? (waarop full scan van anti-virus een negatief effect kan hebben) ? |  |
| Geen remote overname van servers zonder overleg met UZB IT dienst. Remote toegang kan worden verkregen via VPN VPN mbv Pulse Secure Client & onze PAM oplossing, is dit nodig ? |  |
| Wordt er een ander remote control systeem (bvb Axeda) gebruikt ? |  |
| Bezwaar dat installatie account disabled wordt na de installatie van de oplossing ? |  |
| Service account(s) nodig ?\* Zoja, welke specifieke rechten ?  \* UZB standaarden : Niet OS-gerelateerde services MOETEN met een service account draaien. Liefst een Managed Service Account zonder admin rechten (bvb Windows APIs, services, IIS Pools ed), als alternatief kan een "klassieke” SA zonder admin rechten voorzien worden. |  |
| Is het passwoord van de service account(s) zichtbaar in clear text in config bestanden? |  |
| Kan de oplossing/applicatie overweg met Group Managed Service Accounts (passwoord beheer door AD) ?  Indien niet, is argumentatie vereist. |  |
| Draait de oplossing/applicatie als een service ? |  |
| Internet toegang vereist ? Zoja, details (incoming, outgoing, URL’s, IP’s, poorten, protocollen) ? |  |
| Welke services & URL’s zijn van belang om met welke thresholds (met welke onderlinge relatie tss de services en de user experience) te monitoren via MonitorNow ? |  |
| Bezwaar tegen gebruik UZB CA? Of is er publiek certificaat vereist ? |  |
| Gebruik van Kerberos authenticatie of NTLMv2 ? |  |
| Schema van server componenten, informatiestromen en dependencies ? |  |
| Operationele procedure aangeleverd voor systeem check na patchen/rebooten server ? |  |
| Kan oplossing/applicatie overweg met quiesce voor snapshot/backups ? |  |
| Gebruikt de oplossing/applicatie een webserver ?  Zoja, gebruikt deze HTTPS? En wat zijn de subject & SAN namen waarvoor het certificaat (dat door UZB aangeleverd is) wordt gebruikt ? |  |
| Gebruikt de oplossing/applicatie HTTP/FTP/Telnet of andere onveilige protocollen ? |  |
| Kan de applicatie data buiten de VM op een NAS locatie (NetApp MetroCluster) opgeslagen worden ? |  |
| Zijn er local shares nodig ? |  |
| Is een Active Directory connectie nodig ?  Zoja, kan deze overweg met LDAPS ? |  |
| Nood aan nVidia GPU-kaarten ?  Zoja, type licentie voor nVidia Grid & gewenst profiel ? |  |
| Communicatieserver | (HL7 gebaseerde berichten) |
| Is er socket-based communicatie met Mirth voorzien ? Zoniet, wordt een share voorzien op het centrale storage platform of op (een van) de servercomponent(en) van de toepassing één of twee shares gedefinieerd voor in-en uitgaande file gebaseerde communicatie ? |  |
| Database server |  |
| SAP ASE, MS SQL2016(AlwaysOn, Availability Group)? |  |
| Indien geen SAP ASE of MS SQL, welke DB? Door leverancier onderhouden? Ook de licentie voorzien door leverancier ? |  |
| Report services of andere db activiteiten (SSIS, SSAS, SSRS, ETL,…) nodig? |  |
| Geen sysadmin rechten nodig? |  |
| Communicatie tussen applicatie en DB servers geëncrypteerd met minstens TLS 1.2 of hoger? |  |
| Load balancer |  |
| NGINX-software/HA Proxy load balancer of Reverse Proxy nodig? |  |
| File server |  |
| Fileserver of lange termijn file opslag op archief (tot 1 jaar op tier2 disk array of tape indien langer) nodig ? |  |
| Back up / Restore |  |
| Elke virtuele server in beheer van UZB krijgt dagelijks standaard 3 snapshots, is dit voldoende ? |  |
| Kan de applicatie overweg met quiesce of niet ? (resulteert in application - of crash consistent backups) |  |
| Indien fysieke server, moet Commvault agent geïnstalleerd worden. Lijst van folders die meegenomen moeten worden in de backup ? |  |
| Is de DB supported (zie hoger) ? Dan voorziet UZB volledige back-up & restore. Indien andere DB, voorziet de leverancier dit zelf & zal UZB zorgen voor een file-based backup van DB export die voorzien is. |  |

# Beveiliging

|  |  |
| --- | --- |
|  | Antwoord |
| Worden mutaties van data in het systeem en/of op de apparatuur gelogd ? |  |
| Is de apparatuur beschermd tegen door UZB ongewenst installeren van apparaat-vreemde software door onbevoegden ? |  |
| Verbindt de opdrachtnemer zich ertoe om beveiligingslekken zo snel mogelijk kenbaar te maken aan UZB ? |  |
| Verbindt de opdrachtgever zich ertoe eventuele bounties door kwetsbaarheden gevonden door ethische hackers op publiek toegankelijke websites/applicaties te betalen indien deze vermeden hadden kunnen worden? |  |
| Worden er enkel geëncrypteerde verbindingen gebruikt? (HTTPS, LDAPS, …) |  |
| Zijn alle aangeleverde software & runtime environments (java, .net, python, …) vrij van gekende security issues ? |  |
| Is van ieder software component een beschrijving van versie & lopende garantie/support aangeleverd ? |  |
| Bevat de oplossing middelen voor de detectie en correctie van fouten in de invoer, de verwerking, de uitvoer en de verspreiding van gegevens? |  |
| Voldoet de oplossing aan de geldende richtlijnen op moment van gebruik vanuit overheid voor onder andere het beveiligen van de informatiegegevens ? |  |
| Is de hoger vermelde logging van activiteiten bewaard en is UZB in staat om deze logging te consulteren zonder interactie met de opdrachtnemer ? |  |
| Zijn de wachtwoorden, indien binnen applicatie bewaard, gesalt en gehasht ? |  |
| Gebruikt de authenticatie binnen de applicatie de integratie met de MS AD omgeving van UZB ? Indien niet, geef de autorisatie mogelijkheden binnen het product aan, alsook de wachtwoorden doorgeven. |  |
| Wordt er enkel gebruik gemaakt van individuele login/passwoord combinaties en dus geen generieke accounts ? |  |
| Is de oplossing multi-user ? Zoja: - Is er een minimaal onderscheid qua rechten van gebruikers (lezen/toevoegen/wijzigen/…) ? - Zijn de rechten van de types gebruikers eenvoudig voor te leggen via rapport ? |  |
| Kan de applicatie overweg met Imprivata als Single-Sign-On? |  |

# Invullen en ondertekenen leveranciers informatieverwerking (GDPR) contract

Indien internetverbinding vereist - telemetrie actief? - welke data ?

# Contactinfo

Gelieve dit document ondertekend door te sturen via e-mail naar security@uzbrussel.be

Naam firma:

Commercieel:

Naam & Voornaam: …………………………………………………………………

Datum: …………………………

Handtekening voor akkoord: …………………………………………………….

IT Technisch:

Naam & Voornaam: …………………………………………………………………

Datum: …………………………

Handtekening voor akkoord: …………………………………………………….