ilionx
experts in eenvoud

Noodomgeving voor HiX in Microsoft Azure - Wat u moet weten

Inleiding

De beschikbaarheid van ChipSoft HiX is door het steeds intensiever en breder gebruik van het EPD zeer belangrijk. Bij het onverhoopt uitvallen van de ChipSoft HiX configuratie dient een adequate oplossing beschikbaar te zijn. Dit document geeft u een duidelijk overzicht van wat de ilionx Noodomgeving voor Chipsoft HiX inhoudt.

Wat is de ilionx Noodomgeving voor HiX?

Een noodomgeving voor het EPD is een slim plan om ervoor te zorgen dat het EPD altijd beschikbaar en bruikbaar is, zelfs in noodsituaties als uw rekencentrum of netwerk getroffen wordt door een virusaanval of andere calamiteit.

De ilionx Noodomgeving in Microsoft Azure is een schaalbare omgeving die bestaat uit alle componenten om uw kritieke applicaties, waaronder HiX, beschikbaar te kunnen stellen aan een selectieve groep gebruikers in het geval van een calamiteit binnen de productieomgeving. De ilionx Noodomgeving is op een veilige manier met twee-factor authenticatie vanaf het internet te benaderen zodat met een werkstation of laptop met 4G-verbinding vervolgens de applicaties kunnen worden opgestart. De ilionx Noodomgeving wordt gehost in de Azure regio 'West Europe'. In de praktijk betekent dit dat er gebruik wordt gemaakt van Microsoft-datacentra in Nederland.

De ilionx Noodomgeving in Azure is een doorontwikkeling van de ilionx Noodomgeving in de private cloud van ilionx, waar ilionx al vele jaren voor verschillende zorginstellingen een dergelijke omgeving klaar heeft staan voor gebruik in noodscenario's.

Hoe Werkt het?

Binnen de ilionx tenant binnen Microsoft Azure wordt voor uw zorginstelling een set aan componenten ingericht om uiteindelijk de applicaties aan uw eindgebruikers beschikbaar te stellen. Hiervoor wordt gebruik gemaakt van Azure DevOps Pipelines in combinatie met Terraform om te zorgen dat uw Noodomgeving schaalbaar en beheersbaar is. Ook wordt via dezelfde principes een image voor het ziekenhuis klaargezet voor iedere ChipSoft HiX Hotfix zodat altijd de juiste applicatieversie beschikbaar is.

De ilionx Noodomgeving maakt gebruik van enkele shared componenten om de omgeving zo kostenefficiënt mogelijk voor zorginstellingen beschikbaar te stellen. Denk hierbij aan domeincontrollers, Citrix componenten en netwerkbenodigdheden. De data van uw applicaties wordt altijd op zorginstelling specifieke Azure infrastructuur geplaatst om toegang tot uw data enkel voor uw eindgebruikers mogelijk te maken.

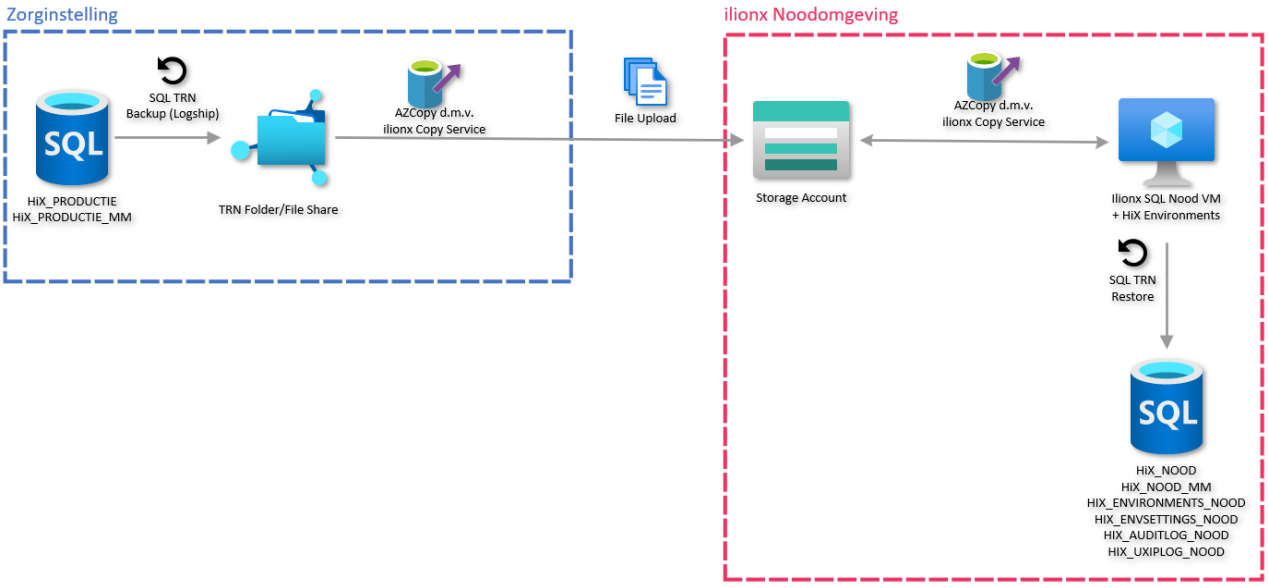
Citrix front-end
De HiX cliënt software, of andere applicatie, werkt vanaf een Shared Citrix farm en een front-end server per eindgebruiker. Randapparatuur wordt softwarematig geïntegreerd in HiX, om hier direct vanuit HiX gebruik van te maken. De automatisch actueel gehouden CS-HiX Noodomgeving wordt, in het geval sprake is van een calamiteit, beschikbaar gesteld aan een overeen te komen aantal medewerkers.

De kosten hiervoor worden per gebruik (pay per use) aan het ziekenhuis doorbelast. Zo betaalt u enkel voor de front-end server(s) wanneer deze gebruikt worden.

SQL back-end
De SQL back-end staat standaard in de zogenoemde 'restoring mode' en is daarmee niet actief benaderbaar. Deze gegevens worden alleen geactiveerd wanneer geautoriseerde medewerkers dat nodig achten. De geactiveerde omgeving is alleen-lezen en wordt regelmatig bijgewerkt met kopieën van nieuwe gegevens van de originele bron. Er kan ook worden gekozen om de kopie enige tijd achter te laten lopen voor extra veiligheid. De

details van wanneer en hoe dit gebeurt, staan in een document genaamd DAP (Disaster Activation Plan).

Synchronisatie proces
Om de data van het ziekenhuis naar de ilionx Noodomgeving over te brengen wordt er gebruik gemaakt van backup routines met software door ilionx ontwikkeld. Indien de Noodomgeving wordt geactiveerd kan deze gemiddeld genomen binnen 10 tot 30 minuten volledig actief zijn. In onderstaande weergave is in kaart gebracht hoe de datastroom voor de ilionx Noodomgeving eruit ziet.



Veilig en betrouwbaar

De Noodomgeving is opgezet met beveiliging als prioriteit, volgens internationaal erkende CIS-beveiligingsrichtlijnen. We zorgen er voor dat de omgeving blijft voldoen aan actuele beveiligingsstandaarden bieden continuïteit door actieve bewaking vanuit onze dienstverlening met daarin o.a. de volgende componenten:

Managed Response
ilionx Managed Response detecteert en reageert op bedreigingen, zelfs als ze nieuw en onbekend zijn voor conventionele virusscanners. Hierdoor wordt het risico voor uw organisatie aanzienlijk verminderd. Managed Response maakt gebruik van SentinelOne-software en het ilionx SOC om uw servers in de Noodomgeving te beschermen tegen geavanceerde aanvallen.

Proactive bewaking
ilionx bewaakt 7x24 uur de status van uw servers en de SQL database en bewaakt de synchronisatiestatus van de Noodomgeving.

Test service
Het blijft uiteraard van belang om regelmatig gezamenlijke testmomenten in te plannen om de technische werking en het kennisniveau van de noodprocedure te testen. Hier maken we samen afspraken over.