Teknisk specifikation

Procapita / Lifecare

2025-01-21	Kap 4.3	Portöppning för RabbitMQ
2025-01-21	Kap 8.2	Tagit bort det vi inte längre stödjer eller behöver
2024-12-05	Kap 10.1.4	Mer förklarande text om IdentityServer
2024-08-22	Kap 8.2	Lagt till RabbitMQ i vår tekniska plattform
2024-05-01	Alla	Omstrukturering för Welfare
2024-01-24	Kap 6.6	Ny text om säkerhetsaspekter för utloggning
2024-01-11	Kap 2.1.3	Ny text om ökade minneskrav för servrar med IIS applikationer

Innehållsförteckning

Teknisk specifikation

1 Om detta dokument

Denna tekniskspecifikation innehåller viktig information för systemägare, systemförvaltare, driftansvariga och tekniker med ansvar för en eller flera installationer av Tietoevrys verksamhetssystem Procapita och Lifecare (nedan kallat verksamhetssystemet). Aktuell version av detta dokument nås på adress: https://doc.service.tieto.com/tekniskspec/

Dokumentet är en viktig vägledning för design och installation av en driftmiljö där verksamhetssystemet ingår. Dokumentet innehåller också viktig information om hur den supportade tekniska plattformen för verksamhetssystemet ser ut.

Tietoevry förbehåller sig rätten att uppdatera innehållet i detta dokument allteftersom verksamhetssystemet utvecklas eller anpassas för ny eller förändrad teknik.

För kunder som använder sig av Tietoevrys SaaS-tjänster (Lifecare Cloud Services) hänvisar vi till de tjänstebeskrivningar som gäller för dessa leveranser

Lifecare: https://doc.service.tieto.com/tjanstebeskrivning/

2 Allmänt

2.1 Procapita On Premise

- är en Klient-/serverlösning där klientprogrammen exekveras på windowsdatorer
- Lokal inloggning sker via säkerhetssystemet TSS, som hanterar användare, lösenord, komponenter, roller och konfiguration. All inloggning och åtkomstkontroll mot komponenter autentiseras mot TSS vid varje access.
- Utvecklas med tjänsteserverarkitektur, vilket möjliggör skapandet av ett öppet system. Systemet driftas på en 64-bitars windowsserverplattform.
- Systemets serverkomponenter tjänar som back-end för alla nya Lifecaremoduler.

2.2 Lifecare On Premise

- Innefattar både Procapita samt de nya Lifecaremodulerna som utvecklas och driftas för webbåtkomst.
- Crystal Reports används som rapportgenerator (32-bitar Crystal Reportsanvänds).
- Vår rekommendation är att Procapitas serverprogramvara driftas i en eller flera för ändamålet dedikerade serverar. Det går dela installationer genom att ha flera domäner i samma miljö för samma delsystem.
- Godkända versioner av tredjepartsprogramvaror avsedda för Procapitas driftsmiljö, v.g. se information om godkända tredjepartsprogramvaror nedan.

2.3 Ökat minneskrav för IIS-tjänster på våra servrar

Som en del i den tekniska moderniseringen, utvecklar vi Lifecare för att vara mer modulariserat samt att i framtiden kunna stödja Containers som hosting-lösning. Modulariseringen medför en ökad tillgänglighet hos enskilda moduler samt ökad stabilitet i systemet över lag.

Ett led i den här utvecklingen är övergången från .NET Framework till .NET Core som plattform. Övergången till .NET Core sker succesivt och per webbapplikation. Här ställer vi också om till att exekvera i 64-bitarsläge för att möjliggöra utnyttjandet av mer minne i samband med höga laster.

I och med nyttjandet av .NET Core plattformen, är det inte längre möjligt för webbapplikationer att dela samma applikationspool. Detta är en begränsning i .NET Core plattformen, med syfte att öka prestanda och stabilitet hos de enskilda webbapplikationerna. En konsekvens är att varje webbapplikation exekverar i en egen applikationspool.

Under 2023 har vi ökat takten på övergången till .NET Core och vi har nu sett indikationer på att minnesförbrukningen för IIS-tjänster på våra servrar har ökat.

I praktiken betyder det att en server som kör Lifecare, också kommer att få många IIS-arbetsprocesser (w3wp.exe). Varje process i sig tar har en låg minnesförbrukning men med många webbapplikationer, ökar den totala minnesförbrukningen.

Detta har medfört att vi nu utökat minimirekommendationerna för minne för servrar installerade med IIS-applikationer. Läs mer under sektion 3 nedan.

Referenser:
https://learn.microsoft.com/sv-SE/aspnet/core/host-and-deploy/aspnet-core-module
https://learn.microsoft.com/sv-SE/aspnet/core/host-and-deploy/iis/in-process-hosting

3 Hårdvarurekommendation - On Premise

3.1 Referenskonfigurationer

Vid uppsättning av servermiljön On Premise, bör nedanstående referenskonfigurationer och riktvärden övervägas för att erhålla en väl fungerande driftmiljö. I samråd med Tietoevrys tekniker bör varje kund överväga vilken typ av installation som krävs. En installation kan skalas på olika sätt beroende på hur många samtidiga användare som beräknas samt hur många moduler som skall installeras.

Vi rekommenderas att hårdvaran är utbyggbar (2 → 4 → 8 cpu) ifall prestandakraven ökar, vid fler användare, fler komponenter i Lifecare etc. För virtuell miljö påverkar även hostarnas hårdvara och dess belastning och ev överallokering i systemet. Detta måste beaktas av er som kund.

Vid design av en första installation är det viktigt att ta en dialog med systemägare och systemförvaltare om följande punkter eftersom dessa ligger till grund för design av systemet

- Åtkomst för användare, enbart intranätet el via internet
- Antal användare vilket hjälper till med initial bestyckning av servrar
- Recovery time objective (RTO) vilket ger en uppfattning om hur lång tid en återställning av systemet tar vid en större incident
- Tillgänglighet

- Säkerthet vid åtkomst

Beskrivning av servertyper	
Core Server	Traditionell TSS-server inklusive Agenten, IDP-service samt övriga tjänster för gemensamma komponenter, metatjänst och syslog.
Applikationsserver	Innehåller delsystemens brokerfunktionalitet för Procapitas serverdelar samt web services för delsystemens moduler.
Intranetserver	Innehåller webbmoduler som exponerat till användare på intranätet.
Web Server	Innehåller webbmoduler som exponeras ut till användaren, antingen placerad på Intranätet och/eller på DMZ.
Databasserver	Server inklusive databashanterare.

Servertyperna kan kombineras på en maskin eller delas upp. Denna dialog tas med Tietoevrys tekniker inför första installation.

3.1.1 Klientdator – för classic Navigator

Nedan finner ni Tietoevrys rekommendationer för uppsättning av en klientdator. Rekommendationen ska ses som ett minimivärde för att erhålla en väl fungerande miljö.

Rekommendation för klient	
Processor	2 CPU
Minne	8 GB
Lokal hårddisk (exkl. OS)	256 GB SSD
Operativsystem	V.g. se information om Tredjepartsprogramvaror nedan.
Bildskärm/Grafik	- Skärmupplösning - 1920x1080, minst 65535 färger. - DPI - 100% - 24-tum

3.1.2 Procapita och tunna klienter

Procapitas klient (tcm.exe) är testad och verifierad för installation och användning i s.k. tunn klient-miljö där användarna har separata konton till miljön.

Följande tekniker är supportade:

- Citrix XenApp (vissa funktioner fungerar ej som t ex dockning av Navigatorn)
- Microsoft Remote Desktop Services

3.1.2.1 Dimensionering av Terminal Server

Tietoevry hänvisar till Microsoft och Citrix för mer information om exempelvis övervägande vid design, installation och dimensionering av en tunn-klientmiljö.

3.1.3 Core Server/Applikationsserver

Rollerna Core samt Applikation kan installeras på samma server. Nedanstående information gäller för bägge typer av applikationsserver, (Core samt Applikation), vare sig installerade separat eller tillsammans.

- Viktigt att följa Windows instruktioner genom att inte namnge servrar med mer än max 15 tecken i servernamnet då NetBIOS-namnet används i TSS, samt i namnuppslagning mellan TSS och applikationsservern. Att inleda ett servernamn med en siffra är ej möjligt.

Nedanstående information anger **minimivärden** för applikationsserver för ett delsystem:

Rekommendation för Applikationsserver (Core och/eller applikation)	
Processor	2x2 (2 vCPU w 2 vCore)
Minne	16 GB
Lokal hårddisk (exkl. OS)	100 GB
Operativsystem	V.g. se information om tredjepartsprogramvaror nedan.

3.1.4 Databasserver

Viktigt! Kommunikation mellan verksamhetssystem och databas klarar lösenord med max 15 tecken.

Nedanstående information anger **minimivärden** för en databasserver. Utifrån kundens behov, dvs antalet Lifecaresystem som installerats samt antal användare, kan dessa måsta utökas.

En rekommendation är att ha lika mycket minne som databasernas storlek.

Rekommendation för Databasserver	
Processor	2x2 (2 vCPU w 2 vCore)
Minne	16 GB
Lokal hårddisk (exkl. OS)	500 GB
Operativssytem	V.g. se information om tredjepartsprogramvaror nedan.
Databashanterare	V.g. se information om tredjepartsprogramvaror nedan.
Disksystem	Tietoevry hänvisar till respektive databasleverantörs rekommendationer.

Nedanstående uppgifter är beräknade riktvärden angående utrymmesbehov för registerdata.

KIR	
KIR	6 MB per 1 000 invånare
Procapita IFO	
Familjeomsorg	10 MB per 100 ärenden
Familjeomsorg historik	9 MB per 100 ärenden
Tidbok	50 MB per 10 handläggare
Dokument	4,5 GB per 1000 insats eller 30 KB per dokument. Dokument med logotyp, bilder, fet stil etc. kräver väsentligt mer utrymme.
Procapita VoO	
Vård och Omsorg	80 MB per 100 vårdtagare

Dokument	150 KB per dokument

Extra utrymmeskrävande funktioner

Loggtabeller – i takt med att användningen ökar och åren går växer behovet av utrymme för de databaser som hanterar loggning.

Dokumentlagring - VoO o IFO introducerar ytterligare funktioner 2022 för att spara pdf-dokument i databasen istället för på disk. Vi räknar då med ett markant utökat utrymmesbehov. För IFO utökas utrymmesbehovet beroende på användningen av funktionerna och storleken på bifogade filer. Medborgartjänster har också denna funktionalitet. Avvikelse har också en möjlighet att infoga filer både från webbrapporter och i utredningsdelen vilket gör att utrymmesbehovet kan växa även här.

Rekommendation - se över övervakning av datafiler och diskutrymme på er databasserver. Rebuild index kräver dubbel diskstorlek för största tabellen.

3.1.5 Webbserver/Intranätwebbserver

Nedan angivna rekommendation gäller för varje separat webbserver oberoende om denna är placerad på Intranätet eller på DMZ. Möjligheter måste finnas för utbyggnad av både CPU och minne, då belastningen varierar beroende på antal moduler som installerats och av antal användarsessioner.

Ifall intranätwebbserverrollen är installerad på applikationsservern, bör minnet anpassas med krav för **både** applikationsserver och webbserver.

Om webbapplikationer skall exponeras ut mot Internet skall denna webbserver vara separerad från övriga delar av installationen via en brandvägg.

Numera krävs att säker kommunikation (https) används både på webb och intranätwebbservrar.

Rekommendation för Webbserver	
Processor	2x2 (2 vCPU w 2 vCore)
Minne	12 GB
Hårddisk (exklusive OS)	50 GB

3.1.6 Teknikdelar för LMO (Lifecare Mobil Omsorg)

3.1.6.1 Mobila applikationer

Tekniska krav för de mobla enheterna för LMO finns beskrivna i ett separat dokument och nås via denna länk https://prod-lcsse.service.tieto.com/teknikkravlmo/

OBS! Om kundern använder ett sk offlineläge på sin mobila enhet är det på kundens ansvar att se till att uppkoppling görs innan appen slås av så att data inte går förlorat.

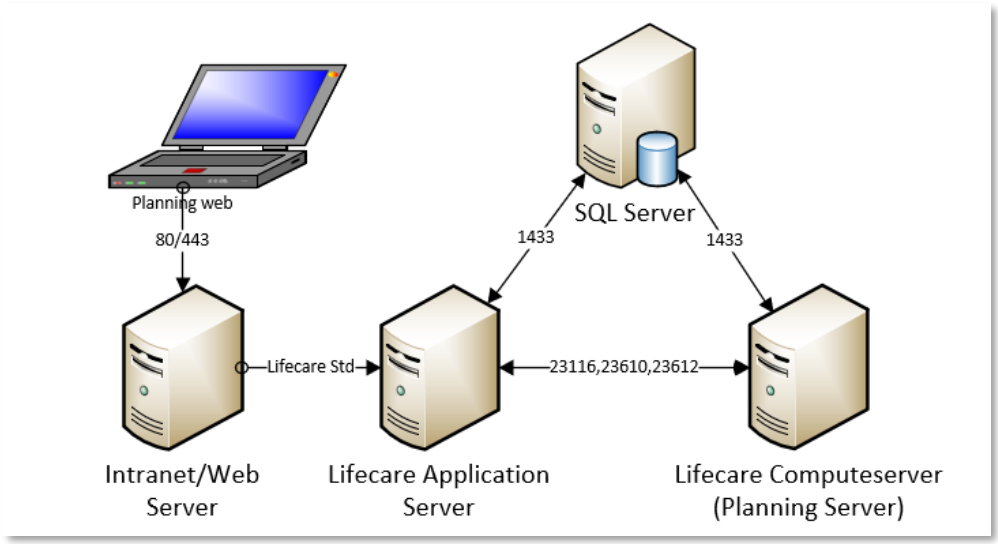
3.1.7 Computeserver för Lifecare Planning

Beräkningsdelen för Lifecare Planning bör installeras på en separat beräkningsserver, här kallat computeserver. Denna server ersätter den LapsCare-server som fanns förut.

Första installation av computeservern görs av Tietoevrys tekniker, sedan uppdateras den på samma sätt som övriga servrar i Lifecarefamiljen. Nedan angivna rekommendation gäller per computeserver och måste kunna utökas vid behov.

Rekommendation för Analysserver	
Processor	2 (2 vCPU)
Minne	16 GB
Lokal hårddisk (exkl. OS)	40 GB
Operativssytem	V.g. se information om tredjepartsprogramvaror nedan.
Databashanterare	V.g. se information om tredjepartsprogramvaror nedan.
Disksystem	Tietoevry hänvisar till respektive databasleverantörs rekommendationer.

För kommunikation och portöppningar se nedanstående ritning.



4 Nätverk och portöppningar

4.1 Nätverk

Installation av verksamhetssystemet On Premise rekommenderas att göras i ett eget isolerat nätverk för att minimera risken för obehörig åtkomst av känslig information.

4.2 Kommunikation

För daglig användning av Procapita, rekommenderas en förbindelse med kapacitet motsvarande 10 Mbit (eller bättre) mellan klient och server. Svarstid (latency) i nätförbindelse mellan klientdator och server får ej överstiga 10 ms. Om nätinfrastrukturen mellan klientdator och server är av WAN-typ rekommenderas att Procapita-klienten exekveras i en tunn klientmiljö (Citrix eller Remote Desktop Services).

4.3 Övergripande förteckning av portar

Server

Nedanstående portar krävs för samtliga typer av installationer. Om separat applikationsserver eller webbserver saknas, kan dessa portar uteslutas. Övriga portar behöver vara öppna för kommunikation mellan de servertyper som beskrivs enligt nedan:

Från	Till	Port	Namn
Internet/Intranet	WebServer	443	HTTPS
Intranet	IntranetServer	80	HTTP
		443	HTTPS
WebServer/ IntranetServer	ApplicationServer	23110	HCW.Welfare.KIR.ServiceModel.IISHost
		23114	HCW.Welfare.FC.ServiceModel.IISHost
		23116	HCW.Welfare.EC.ServiceModel.IISHost
		23612	Lifecaretjänster
WebServer/ IntranetServer	CoreServer	23610	Coretjänster (Metaservice, IP tjänst m fl)
ApplicationServer	CoreServer	2100	TSS
		30710	Tieto Name Server
		23610	Coretjänster
		9091	Event System
		23611	Resursagent (Web.Agent)
		23612	Lifecaretjänster
ComputeServer	ApplicationServer	23612	Lifecaretjänster
		9091	Event System
ComputeServer	CoreServer	23610	Coretjänster
CoreServer/ ApplicationServer/ ComputeServer	Databasserver	1433	Defaultport SQL Server (el. den ni använder)
ApplicationServer	WebServer/ IntranetServer	808	Event System Notifiering till webbar (Net.tcp)
		80/443	För att kunna recycla Applikationspooler

Från	Till	Port	Namn
CoreServer	WebServer/ IntranetServer	80/443	För att kunna recycla Applikationspooler
Lastbalanserad server	Lastbalanserad server	11211	Memory Cache
		11212	Memory Cache Sync
WebServer/ IntranetServer	ApplicationServer	5672	RabbitMQ via http
		5671	RabbitMQ via https

Klient

För kommunikation mellan Procapita-klient (Navigatorn) och server behöver portar enligt Appendix E1 öppnas. För att förenkla att sätta brandväggsregler kan följande portspann öppnas:

2100-2140,23110-23120,30600-30620, 30710, 30722, 30751

Tietoevry rekommenderar **inte** längre att ha dessa portar öppna 30700-30709, 30711-30721, 30723-30750 samt 30752-30760. Dessa portar behövs endast för access till administrations-GUI för brokrar osv. Ur ett säkerhetsperspektiv rekommenderar Tietoevry att dessa accessas endast från core/applikationsserver.

4.4 VOO och Windows Firewall

Om databasen ligger på en separat server och Windows Firewall är påslagen, måste brandväggen öppnas för nedanstående program (från M3SERVER) mellan applikationsserver och databasserver:

Inkomstöverföring LEFI Online

- Kq1fkController.exe
- Kq1ConvertFkxml.exe

Byte Organisation Handläggare

- HCW.Welfare.ec.byteorgverkstallighet.exe
- HCW.Welfare.ec.controllerbyteorg.exe
- HCW.CustomSolutions.KQ0GALXML.exe

Databas-providers för OLEDB behöver finnas i samma version på både applikationsservern och databasservern. För SQL Server installeras nödvändiga providers om SQLManager uppdateras.

Obs! Det krävs att port 7020 är öppen ut från applikationsservern för anrop till FK.

4.5 Nedladdning av installationspaket/licensfil

För att kunna ladda ner installationspaket eller licensfil till Lifecare Installer måste port 22 (sftp) samt 443 (https) vara öppen (inifrån och ut) på respektive Procapitaserver. Det är även möjligt att ladda ner installationsfiler från teknikerns egna dator (om dessa kan överföra filerna till servrarna). Även licensfilen går att ladda ner från annan dator. Smidigast är dock att låta Lifecare installer ladda ner denna fil i realtid då installationen körs för att säkerställa att installationen görs med en aktuell licensfil.

4.6 Ipv6 och Direct Access

Stöd för Ipv6 finns implementerat i Procapita, både på server- och klientsidan.

Det finns olika parametrar (environment variables) som kan användas för att styra vilket protokoll som respektive klienter skall använda., Enbart Ipv4 är påslagen default.

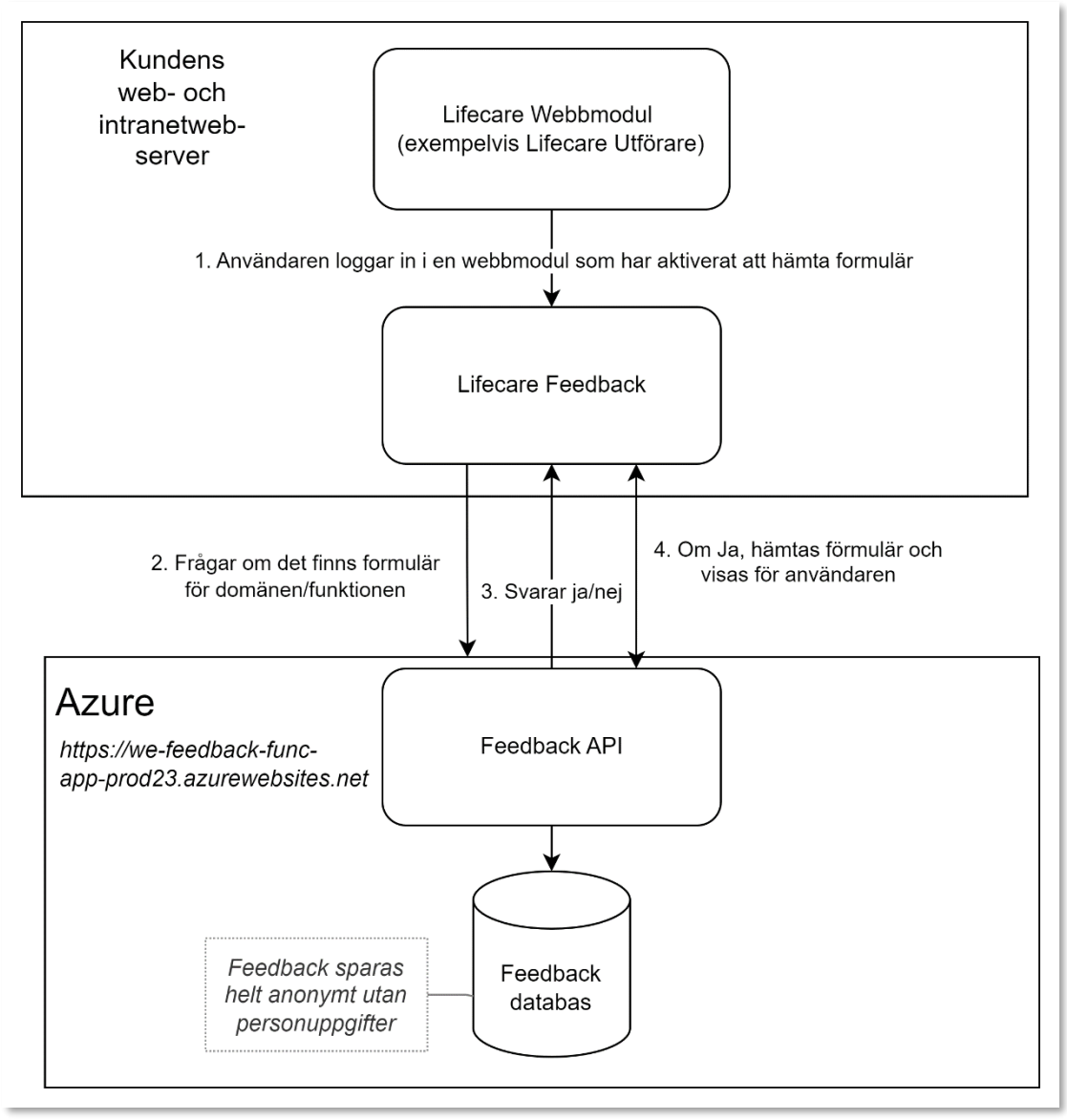
Miljövariabel på klient	Parameter	Förklaring
TITAN_LOOKUP_IPV6_ENABLE	Y	Sätt denna till Y på klienterna för att möjliggöra kommunikation med Ipv6
TITAN_LOOKUP_IPV4_DISABLE	Y	Sätt denna till Y på klienterna för att spärra kommunikation med Ipv4

Att aktivera Ipv6 har varit en förutsättning för att få Direct Access (DA) att fungera. Vill ni efter 9.6w04 prova att köra på Ipv6 samt DA måste både TITAN_LOOKUP_IPV6_ENABLE samt TITAN_LOOKUP_IPV4_DISABLE aktiveras på den klient ni vill testa med. Se till att ert AD har Ipv6 aktiverat samt att det inte är spärrat i er brandvägg. Kör ni enbart med Ipv4 internt, måste miljövariablerna slås av när samma klientdator kopplas upp på det interna nätet igen.

4.7 Lifecare återkoppling

Från version 12w47 har Lifecaremodulerna möjlighet att koppla på ett feedback-formulär till sin applikationsmeny. Det ger Tietoevry möjlighet att samla feedback från användare i Lifecare. Alla svar sparas i en databas i Azure. Svaren är helt anonyma och inga personuppgifter skickas med.

En öppning ut från applikationsservern till följande adress krävs https://we-feedback-func-app-prod23.azurewebsites.net, se lösningsritning nedan.



5 Integrationer

För integration med myndigheter, externa produkter, andra Tietoevry-produkter t ex inkomsthämtning eller hämtning av aviseringar till KIR, rekommenderas TEIS från Tietoevry. Med den säkerhet som finns inbyggd i TEIS är det möjligt att använda Internet för externa integrationer om så önskas.

6 Säkerhet/Underhåll

6.1 Autentisering

Grunden i all autentisering för våra webbapplikationer ligger i verksamhetssystemets Identity Portal (IdP). IdP styr vilken metod för autentisering som ska användas. Används metoden SAMLv2 är det utbudet från kundens IdP-leverantör som styr vilken inloggninsmetod som kan användas.

OBS! Beakta ALLTID de krav på s.k. stark autentisering (2-faktors etc.) som ställs av Integritetsskyddsmyndigheten – IMY när webbapplikationer görs tillgängliga över Internet.

Kunden kan i stor utsträckning själv välja vilken metod som ska användas via en konfigurering.

Följande autentiseringsmöjligheter finns för olika delar av Procapita/Lifecare:

- Procapitas behörighetssystem TSS
- SAML

SAML kan hanteras via:

- Microsoft Active Directory Federation Services (ADFS)
- Extern IdP-leverantör

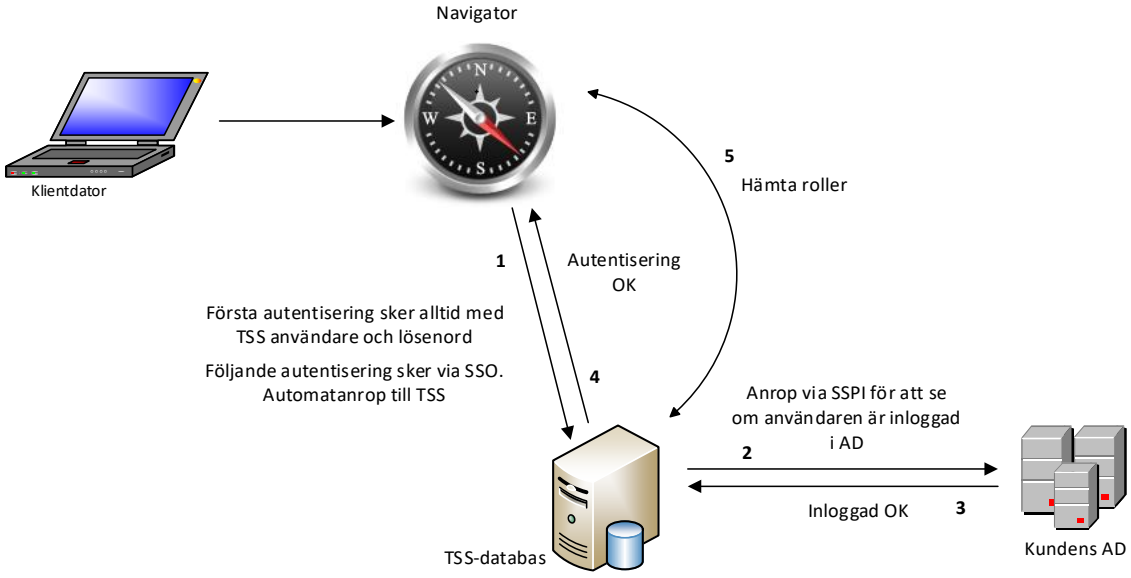
Exempel på IdP-leverantörer

- Tietoevry Lifecare IAM Services (LIAM)
- MobilityGuard
- Nexus HAG
- Visma Ticket Server
- PhenixID Authentication Services (PAS)
- Svensk e-identitet

Se mer detaljerad information i dokumentet som finns via denna länk https://doc.service.tieto.com/SAML/.

6.1.1 Procapita Single Sign-On (SSO)

Vid inloggning till Procapita kan integration till extern katalogtjänst av typen Microsoft Active Directory, AD, aktiveras (tillvalsmodul).



6.1.2 Inloggning och Signering med eTjänstekort

Inloggning och signering via eTjänstekort är ett tillval i Procapita som ger stark autentisering (av 2-faktors-typ) med hjälp av s.k. smarta kort. Tillvalet är endast implementerat och supportat i Procapita Vård och Omsorg (VoO) och i Procapita Familjeomsorg (IFO).

Supportade korttyper

- SITHS-kort

6.2 Backup och återläsning

Kunden ansvarar för att säkerställa att backup och återläsning av server/data kan göras (inklusive installationskatalog). Detta är viktigt så att en återläsning kan göras, både vid systemhaveri eller problem vid uppdatering.

Systembackup bör ske av samtliga servrar (OS-nivå) som ingår i den installerade miljön. Backupfrekvens och retention-policy bestämmer kunden själv utifrån de krav som förvaltningen ställer på verksamhetssystemet och ansvarig enhet för driftverksamheten.

Utöver systembackup av servrar är det också viktigt att databasbackup (SQL Server, inkl transaktionslogg) konfigureras för systemet så att återläsning av hela eller delar av databasens innehåll kan ombesörjas vid behov. Mer information om detta finns i dokumentet ”SQL Server Maintenance plan”.

Vi rekommenderar alltid våra kunder att ta hjälp och råd av våra teknikkonsulter när det kommer till att fastställa en mer detaljerad design för backup av vårt system.

6.3 Övervakning/Larm

Vid drift i egen regi ger Tietoevry några exempel på rekommenderade övervakningar/larm som bör sättas upp:

- OS-övervakning
- CPU-belastning
- Diskutrymme
- Minneshantering
- Tieto och Welfare Windowstjänster, t ex Tieto Server Manager Service
- Bevakning av enskilda TSB-processer
- Max filstorlek på TSS-databasen
- IIS Tjänsten, applikationspooler samt web siter
- Ping, så att den idp-portal ni använder är uppe och svarar, t ex ger metadata tillbaka
- Kontroll att SQL Server samt SQL Agent tjänsterna är igång
- Kontroll att någon svarar på 1433 på databasservern

Miljön kan t ex övervakas med hjälp av Microsoft System Center Operational Manager, SCOM.
Genom att använda Templates från Microsofts Management Packs kan man skapa övervakningen/larm på de tjänster och funktioner som önskas.
OBS! App Performance Monitoring (APM) bör EJ vara aktiv på applikationsservern ifall SCOM används.

Ifall övervakningsverktyget medger förordar vi att vid uppdatering av miljön sätta servrarna i s k Maintenace Mode tills uppdateringen med Lifecare installer är klar. *En felkälla vid installation är då tjänster osv som skall vara av slås på under uppdateringstillfället.*

6.4 Uppstartsordning

När miljön för verksamhetssystemet startas om skall servrarna startas upp i följande ordning; TSS (Core) Server först, därefter applikationsservrar och sist webservrar.

6.5 SLA – tillgänglighet för systemet

Vid införande av Procapita/Lifecare bör tillgängligheten beaktas. Kunden måste ta i beaktning att servicefönster för uppdateringar kan behöva planeras in i takt med att LCS har servicefönster.

6.6 Webb

Kakor (cookies)

Verksamhetssystemet använder **inga** ”kakor” som kan användas av tredje part för att kunna se användarens nyttjande av webbplatsen.

Verksamhetssystemet använder sk. temporära sessionskakor. Dessa används som huvudsak för att veta att användaren är auktoriserad och försvinner när användaren loggar ut, stänger webbläsaren eller stänger datorn. Sessionskakor används för att användaren skall kunna byta sidor på webbplatsen utan att behöva mata in namn och lösenord på nytt.

Tietoevry rekommenderar våra kunder att informera sina användare, (på de webbsajter – kommunens hemsida, e-tjänsteportal, skolportal el dyl.) varifrån våra webbapplikationer kan nås. Följande

beskrivning rekommenderas: ”Genom att logga in så samtycker man till att webbplatsen får använda sessionskakor.

Utloggning

Ur ett säkerhetsperspektiv är det viktigt att tillse att en användare blir utloggad när denne lämnar applikationen, gäller både ifall en applikation körs på dator eller telefon. Vi rekommenderar att ni använder er IdP’s funktionalitet för *single log out*. Ifall en webbsida stängs utan att användaren har tryckt på logga-ut-knappen finns en risk att sessionen ligger kvar och nästa användare kommer in på föregåendes uppgifter.

6.7 Virusprogramvara

Tietoevry hänvisar ill Microsofts egna rekommendationer avseende IIS och SQL Server. Se exempelvis följande länk

https ://support.microsoft.com/en-us/help/309422/how-to-choose-antivirus-software-to-run-on-computers-that-are-running

6.8 Åtkomst till disk för applikationen

För att verksamhetssystemet skall fungera behöver applikationens användare ha read/execute behörighet till de kataloger som används för exekvering, samt även för kataloger där in/ut-filer skall sparas. När applikationen installeras hjälper er Tietoevry tekniker till att sätta upp detta. Kontakta alltid denna tekniker igen ifall ni planerar någon förändring av användarkonton eller behörighet för applikationen.

6.9 Åtkomst till data via API-anrop

För att bidra till kundens digitala ekosystem på bästa sätt, tillhandahåller Tietoevrys verksamhetssystem API:er som kan nyttjas av externa aktörer. Externa aktörer kan t.ex. vara andra system i kundens miljö eller tjänster som tillhandahålls av andra leverantörer. För att inte påverkas av eventuella system- eller databasförändringar, ska dessa API:er användas vid integration med verksamhetssystemet.

Kunden ansvarar för alla integrationer med verksamhetssystemet. T.ex. att data som lämnar verksamhetssystemet behandlas på ett sätt korrekt sätt, med lämplig säkerhet och enligt rådande lagstiftningar.

Vid kommunikation med API:er som exponeras via er externa webbserver skall den externa aktören identifiera sig med ett klientcertifikat (s.k. dubbelsidig SSL). Av säkerhetsskäl (GDPR mm.) är det vår starka rekommendation att detta krav tillämpas både på Internet och på interna nät. Vid lokal drift är det kundens ansvar att förse den externa aktören med ett lämpligt klientcertifikat. Klientcertifikat kan utfärdas av kommersiella certifikatutfärdare eller av kundens eventuella egna certifikatutfärdare. Tietoevry rekommenderar inte att kunden delar med sig av sitt wildcard-certifikat (*.domain.se) till en extern aktör. Dock kan en extern aktör använda sitt klientcertifikat (ifall detta stödjer klientautentisering och om kunden och den andra leverantören tycker att detta är lämplig lösning). För mer information om klientcertifikat läs på Wikipedia eller kontakta Tietoevrys teknikkonsulter.

Om kunden väljer att använda lastdelare eller SSL-terminering framför systemets servrar så måste instruktionerna i dokumentet ”Setup lastbalanserare eller proxy” följas.

Ifall stora datamängder skall läsas ut ur verksamhetssystemet, är det kundens ansvar att säkerställa att systemresurser och resurser i infrastrukturen används på ett vettigt sätt (t.ex. inte tunga bearbetningar under dagtid). Detta för att inte t.ex. svarstider i övriga delar i verksamhetssystemet ska påverkas negativt.

OBS! För kunder som använder våra API’er sker en större mängd loggning i HCWSYSLOG databasen än för andra kunder. Så se till att max size och growth ökas på.

7 Fjärrsupport

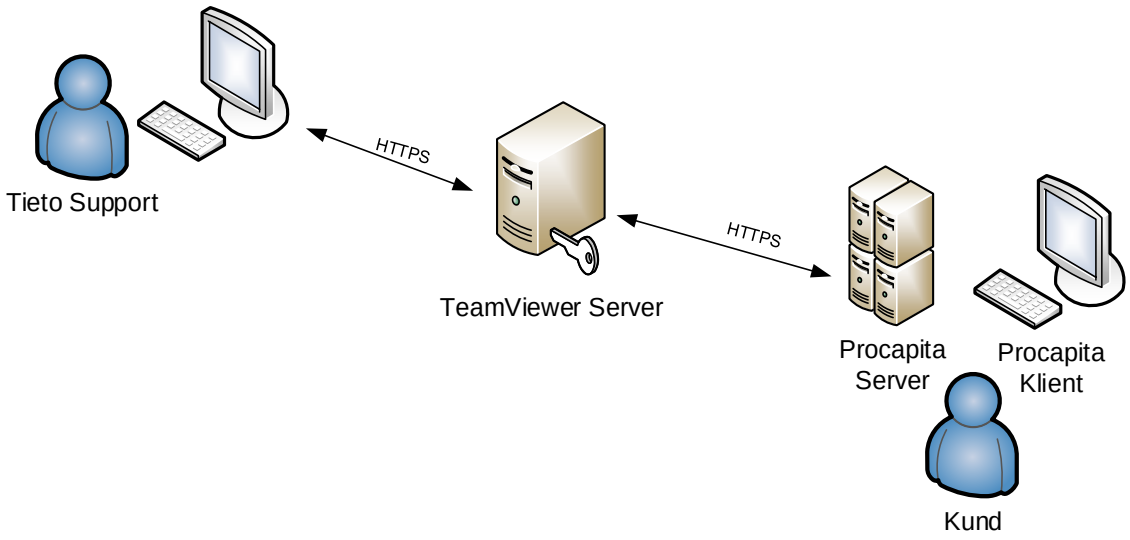
Tietoevry erbjuder (och har i avtal kravet på oss) att kunna utföra tjänster på distans. Ett exempel är olika typer av kundstöd kring tillämpning och drift. För detta ändamål krävs att kunden etablerar möjlighet för Tietoevry att nå driftsmiljön via fjärrförbindelse.

En viktig faktor vid fjärrförbindelser är säkerhetsaspekten. Vid användandet av öppna TCP/IP-nät som bärare av data ökar exponeringen för olika former av yttre påverkan. Risk finns att data avlyssnas av obehöriga, förändras eller på annat sätt förvanskas. Integritetsskyddsmyndigheten (IMY) kräver att känsligt data, t ex personuppgifter, skall krypteras vid transport. IMY anger dock inte hur data skall krypteras. Det är upp till respektive ansvarig part att bedöma om styrkan i krypteringen är tillräcklig.

7.1 Rekommenderad lösning

För att få en säker lösning med hänsyn till ovanstående säkerhetsaspekter, rekommenderar Tietoevry programvaran TeamViewer.

Principen för denna lösning är att trafik sker via Internet med en central server som länk mellan Tietoevrys interna nät och kundens. All kommunikation är krypterad (RSA private/public key exchange (2048-bit) and AES (256-bit) session encryption), och använder internt port 443 (HTTPs) och loggas på servern.



Vid behov av fjärrsupport laddas TeamViewer-programvaran ner från TeamViewers hemsida och startas på den dator, server eller klient som behöver nås av Tietoevrys support och/eller konsultpersonal. Efter avslutad session stänger kunden ner TeamViewer.

8 Teknik

8.1 Tredjepartsprogramvaror och nya versioner

Beträffande tredjepartsprogramvaror och nya versioner (högre versioner inklusive Service Pack eller motsvarande) gäller generellt att verksamhetssystemet måste verifieras och godkännas av Tietoevry för att tredjepartsprogramvaran skall stödjas för drift. Det innebär att nya versioner av tredjepartsprogramvaror ej ingår i Procapita/Lifecares tekniska plattform förrän information om detta lämnats skriftligt av Tietoevry.

V.g. se appendix C1 nedan för en förteckning över tredjepartsleverantörer vars komponenter ingår i verksamhetssystemet.

8.2 Teknisk plattform

Nedanstående programvaror från tredjepartsleverantör utgör verksamhetssystemets tekniska plattform. Informationen nedan gäller tills annat anges, v.g. se speciella förutsättningar i fotnötterna. Viss installationsmedia finns att ladda ner under Tieto Service på vår leverans-FTP.

Produkt & version	Leverantör	Kommentar (detaljkrav)
Operativsystem (Klient)		
Windows 10	Microsoft	Service Option Semi-Annual Channel (förr kallad CBB). Semi-Annual Channel (Targeted) (förr CB) och Long-Term Servicing Channel (förr LTSB) är ej supportade alternativ.
Windows 11	Microsoft	Support från 2022v4
Operativsystem (Server)		
Windows Server 2019	Microsoft	Engelsk version
Windows Server 2022	Microsoft	support från 2022v4
Databashanterare		
SQL Server 2019	Microsoft	support från 2020v20
SQL Server 2022	Microsoft	support från 2023v7
Databaskommunikation från applikationsserver		
Microsoft OLE DB Driver	Microsoft	Senaste version
Webbserver		
Internet Information Server (IIS)	Microsoft	Aktuell version för supportat os
Applikationsramverk		
.NET Framework 3.5, 4.0, 4.7 och 4.8	Microsoft	4.8 är ett krav på samtliga servrar och klienter från 2023v38.
.Net 8.0	Microsoft	.Net bundle från 2024v04

Produkt & version	Leverantör	Kommentar (detaljkrav)
Webbläsare[1]		
Firefox	Mozilla	Senaste version
Chrome	Google	Senaste version
EDGE Chromium 80+	Microsoft	support från 2020v37 – senaste version
Rapporthantering (Procapita)		
Crystal Reports 2013	SAP	Version 13.0.22 (32-bitar)
Meddelandehantering		
RabbitMQ	Open Source	Senaste full version
Dokumenthantering		
Acrobat Reader	Adobe	BBIC (IFO)
E-post		
Outlook	Microsoft	Office 2007 eller senare (32-bit)

8.3 Webbapplikationer i mobiltelefon

Vissa Lifecaremoduler avsedda för en webbrowser på laptop kan fungera att köra i en webbrowser på mobiltelefonen. Då krävs dock att mobiltelefonen är från 2020 eller nyare.

Kunder som kör Lifecaremoduler i sin mobil behöver säkerställa att mobilen har bra täckning överallt där den kommer att användas.

Sker åtkomst till Lifecaremodulen från intranätet krävs ett stabilt wifi som har täckning överallt där personalen arbetar. Är det så att personalen kör via internet och stabilt wifi saknas krävs då 4G.

Lista av Lifecaremoduler som är verifierade för mobil	
Lifecare Utförare	Senaste 2 versionerna av: Chromium-baserade webbläsare på Android (tex Chome) samt Safari-baserade webbläsare på IOS

[1] Det sker en ständig utveckling av olika Internetstandarder (t.ex. HTML, HTML 5 och Javascript) och därför också olika webbläsarversioner. Tietoevry arbetar ständigt för att kvalitetssäkra och utöka våra tjänster så att de kan användas av så många som möjligt av de på marknaden förekommende klienter och webbläsare. För att tillgodose våra kunders och dess användares önskemål bevakar Tietoevry vilka olika webbläsare och operativsystem kunden använder och anpassar stödet därefter. Tietoevry reviderar webbläsar- och operativsystemstöd i slutet av varje kvartal. Detta kan innebära att Tietoevry officiellt slutar att stödja en viss version av webbläsare eller operativsystem på grund av för liten användning medan nya versioner tillkommer.

9 Scanning

Scanning är en tillvalsmodul.

Scanningsmodulen använder sig av standardgränssnittet TWAIN (www.twain.org) som stöds av de flesta scannerleverantörerna.

Beskrivning	
Hårddisk	V.g. se avsnittet ”Databasserver – Hårddisk” för uppgifter om utrymmesbehov i databasen.
Gränssnitt	TWAIN lägst version 1.7

Kunden ansvarar själv för driftsättning av den scannerutrustning som kunden själv köper in.

10 Procapita/Lifecare webb

10.1 Allmänt

10.1.1 Serverarkitektur

Verksamhetssystemets webbapplikationer är i samtliga fall byggda kring Microsoft Internet Information Server (IIS).

Tietoevry rekommenderar att en separat webbserver sätts upp för webbapplikationer, v.g. se serverrekommendationer ovan. Vid beräkning av serverkapacitet beakta att webbapplikationerna kan vända sig till både medborgarna (Internet), samt internt till personal (Intranät). Samråd gärna med Tietoevry för att göra en mer exakt bedömning i varje enskilt fall. Det faktiska behovet av serverkapacitet för varje webbapplikation varierar med hur kunden väljer att använda applikationen med avseende mot antal användare, nyttjandegrad osv.

För mer information om konfigureringsalternativ v.g. se bilaga A4.

Beskrivning	
Webbserverprogramvara	V.g. se information om tredjepartsprogramvaror ovan beträffande versioner.
Kryptering	Använd alltid HTTPS/SSL på Webbservrar (IIS)
Operativsystem	V.g. se information om tredjepartsprogramvaror ovan beträffande versioner.
Exekveringsmiljö	.NET. V.g. se information om tredjepartsprogramvaror ovan beträffande versioner.

10.1.2 Klientarkitektur

Beskrivning	
Webbläsare	V.g. se information om tredjepartsprogramvaror ovan beträffande versioner.

Brandvägg mellan webbserver (IIS) och applikationsserver/ behörighetsserver måste konfigureras så att datatrafik på berörda portar släpps igenom.

10.1.3 Säkerhet

Kunden ansvarar själv för att erforderlig installation, konfiguration och test av brandväggar och databasreplikering utförs, om inte annat överenskommits med Tietoevry.

Kunden ansvarar också för installation av operativsystem, webbserverprogramvara, brandväggar, certifikat, databaser, FTP-programvara och andra programvaror från annan leverantör än Tietoevry.

Kommunikation

För att kunna kommunicera med Procapita måste Tietoevrys applikationer anropa kundens webbserver enligt givna specifikationer som beskrivs i detta dokument eller i detaljdokument för varje applikation.

Nyttjas en lastbalanserare eller proxy, vänligen se dokumentet ”Setup lastbalanserare eller proxy” för att se vilka krav Tietoevry har samt vilken typ av uppsättning som stödjs.

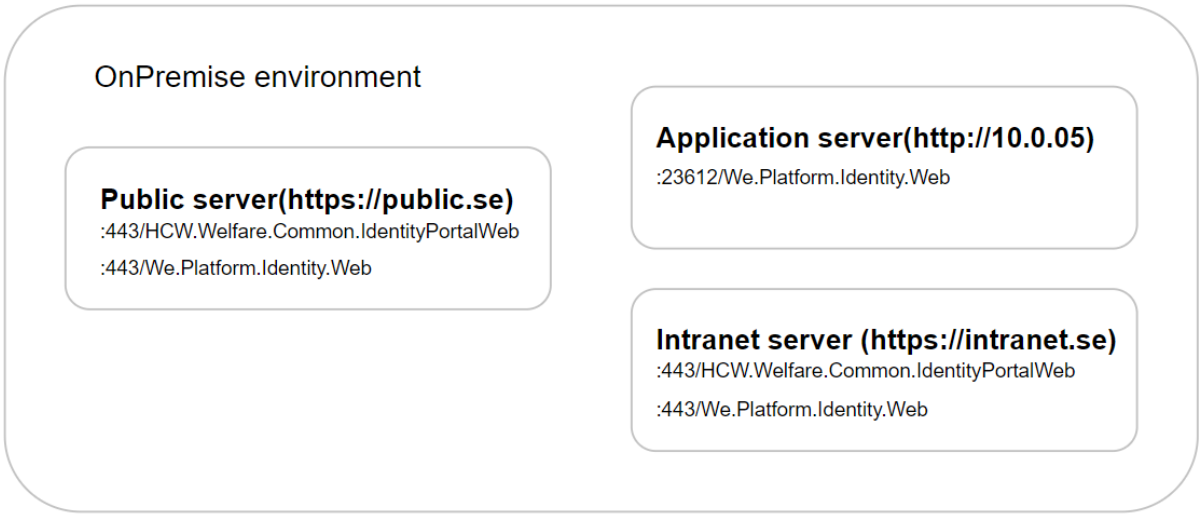
10.1.4 Identityserver

Vi kommer från och med 2025 introducera Identityserver som en del av vår inloggninsprocess.

Syftet med IdentityServer är att erbjuda en bättre sessionshantering i verksamhetssystemet. Sessionshanteringen bygger på standarden Oauth 2. Denna standard kräver att kommunikationen mellan användare och systemet är krypterad med TLS.

OBS! Det betyder att både publika webbservern och Intranet-webbservern **måste vara konfigurerade för att använda TLS (https)**.

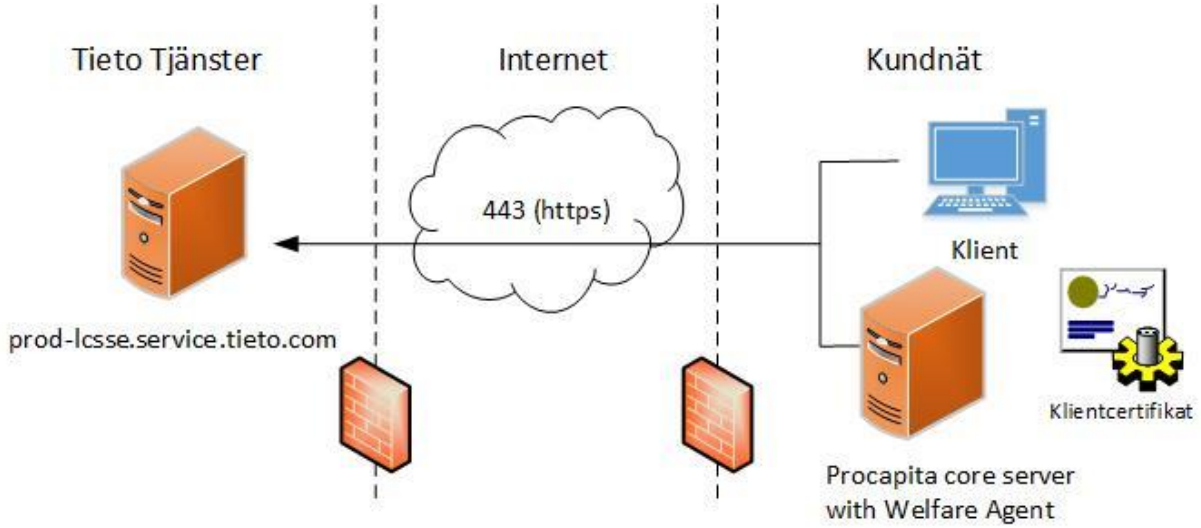
Används en reverse-proxy (lastbalanserare, webbpublicerare etc) framför webb-/intranet-servern som TLS-terminerar, måste reverse-proxy skicka med headrarna X-Forwarded-Host och X-Forwarded-Proto till bakomliggande webbservrar.



11 Övriga produkter

11.1 Lifecare Cloud Agent (LCA, “Welfare Agent”)

Lifecare använder Procapita som back-end system och därför krävs en integration mot kundens verksamhetssystem. För detta används en kommunikationslösning (Lifecare Service Bus, LSB) i kombination med Lifecare Cloud Agent (LCA). Tjänsten för LCA heter Welfare Agent. LSB och Welfare Agent skapar tillsammans en säker förbindelse mellan kundens servermiljö och Tietoevrys motsvarande servermiljö i molnet, där våra webblösningar driftas. Tietoevry kan även tillhandahålla viss fjärrsupport via denna tjänst.



Det certifikat som används vid kommunikationen utfärdas av Tietoevry som CA och med en löptid på 3 år och tillhandahålls av Tietoevry utan extra kostnad, dock tillkommer kostnad då certifikatet måste förnyas och bytas ut av vår Tietoevrytekniker.

Alla anrop sker från den lokala agenten via säker förbindelse till Tietoevrys molntjänster.

Det finns även en lokal agent som driftas i IIS, Welfare.Agent.Web. Denna används enbart för intern kommunikation mellan applikationens installerade servrar.

12 Generellt om säkerhet

Tips och rekommendationer från Tietoevry angående säkerhet on premise.

12.1 Bakgrund

I linje med det vi tidigare dokumenterat ovan vill vi här komplettera med ytterligare tips vad gäller den interna säkerheten i er kommun. Denna sektion är inte en komplett guide till vad ni behöver identifiera, hantera, skydda och logga, utan rekommendationer från Tietoevrys sida.

12.2 Riskbedömningar

En viktig del i ert säkerhetsarbete är att ta fram riskbedömningar för de olika delarna av er tekniska plattform. Både server- och klientsidan, samt den personliga aspekten. Risker är också föränderliga och behöver ses över kontinuerligt. Lite försöker vi ge tips om nedan. Mer info finns att läsa här Integritetsskyddsmyndigheten – IMY - https://www.imy.se/

12.3 Interna nät

Se över åtkomst till interna nät och brandväggar. Om möjligt kör produkter i eget internt nät skiljt från administrativa nät som t ex för elever.

Skapa rutiner för inloggning för att säkerställa dokumentation av vem som loggar på. Personliga AD-konton används till fördel istället för lokala konton. Detta för att kunna följa inloggningar via Audit loggen i Event Viewer.

För att slippa hantering av service-lösenord är det möjligt att använda Group Managed Accounts. I de fall ni redan har detta på plats så kan sådana konton med fördel användas för Tietoevrys tjänster som t ex Tieto Server Manager.

Datakommunikation (Data in motion) avser all data som skickas över ert interna nät. All kommunikation mellan olika nät och olika maskiner skall krypteras och detta kan göras på flera sätt, vanligast med certifikat. Här kan även IPsec användas.

12.4 Publikt nät

Kommunikation från DMZ och in till ert interna nät via brandvägg/lastbalanserare skall göras via de portar som är specificerade av Tietoevry. Kommunikation till IIS skall sättas upp med TLS och certifikat.

Vi rekommenderar alltid stark autentisering (s k 2-faktorsinloggning), för säker inloggning till våra webbmoduler/appar.Vissa av våra moduler har också krav på 2-faktorsinloggning.

12.5 Applikationsservrar och utdelade kataloger

Se över åtkomst till era servrar. Både via direktinloggning och även behörighet till utdelade kataloger. Är en katalog utdelad och synlig för samtliga användare så är detta extra viktigt.

12.6 Databas

Åtkomst till databas bör ske med AD-konton för att få en loggning på vilka som varit inloggade via t ex SQL Server Management Studio (SSMS) och tilldelning av administratörskonton bör hanteras enligt dokumenterad process. Procapita/Lifecare/Education använder lokala SQL Server konton. Tietoevrys installationskonto behöver endast vara aktivt vid installationstillfällen. Lösenord till lokala SQL Server konton bör hanteras via något verktyg för säker hantering av lösenord och inte ligga i läsbar textfil.

Vi rekommenderar starkt att kommunikation till/från SQL Server krypteras. Att sätta upp TLS (Transport Layer Security) kräver certifikat. Använder kommunen IPsec kan detta gälla som säker kommunikation.

Datafiler (Data at rest) kan krypteras och för detta krävs certifikat. Detta kan göras både för backup- och datafiler (för datafiler krävs dock SQL Server Enterprise Edition). Denna teknik kallas TDE (Transparent Data Encryption).

Viktigt är att kommunen bestämmer hantering av certifikat och nycklar innan införande av detta planeras.

Kontakta er Tietoevry-tekniker om ni vill ha hjälp att få något av detta uppsatt.

12.7 Certifikat

Kommunen måste skapa en säker rutin dels för var aktuella certifikat och dess nycklar finns sparade, samt en rutin för förnyelse innan ett certifikat förfaller, så att ett nytt hinner beställas i tid.

12.8 Hantering av loggar/filer

Gemensamt för exporterade filer och loggar (TSS-logg, gallring, produktlogg osv) är att de bör ligga på en säker plats. Antingen sparas undan på annan media eller ligga på en katalog (som ej är utdelad) som bara behöriga har access till.

Loggar som inte längre behövs/måste sparas skall rensas. En rutin för detta behöver sättas upp.

12.9 Säkerhetsuppdateringar

Viktigt att kommunen har en rutin för att kontinuerligt (en gång per månad) ta in de senaste säkerhetsuppdateringarna från Windows samt vara vaksamma ifall extra uppdateringar släpps

12.10 Klientenhet

Dator

Utöver inloggningsskyddet i Procapita/Lifecare bör man ha en policy att alltid låsa sin skärm när man lämnar datorn och gärna en policy som låser skärmen efter en kortare inaktivitet. Där möjlighet finns i applikationen bör även automatutloggning aktiveras

Smart telefon/surfplatta

Där möjlighet finns bör app-lås aktiveras alternativt använda telefonens inbyggda skärmlås.

13 Bilagor/Appendix

13.1 A1) Portöppningar webb

IIS sätts upp på webbserver i DMZ-nätet eller webbserver på intranätet. Data läses/skrivs via tjänster i den befintliga applikationsservern i det administrativa nätet. Nedanstående gäller för våra äldre webbapplikationer, för övrigt se portöppningar under sektion 4.3

Brandvägg mellan DMZ och administrativa nätet			
Port	*TCP/UDP*	*Syfte*	*Kommentar*
2100	TCP	Behörighetssystemet TSS	Kan bindas till dedikerade servrar
30710	TCP	Tieto Name Server (TNS)	För COM och .Net webbar
2116	TCP	Procapita applikationsserver (VoO)	Kan bindas till dedikerade servrar

13.2 C1) Ingående komponenter från tredjepartsleverantör

Nedanstående komponenter från tredjepartsleverantör ingår i Procapita. Informationen nedan gäller tills annat anges.

Produkt och version	Leverantör	Leverantör
Visual C++ runtime 2013	Microsoft	Preinstall94.msi
Visual C++ runtime 2017	Microsoft	Microsoft redist
Visual C++ runtime 2019	Microsoft	MS redist (fr 99v46)
Fujitsu NetCOBOL v8.0	Fujitsu	Runtime för VOO servermoduler
CodeBase 6.3	Sequiter Software	Databashanterare för behörighetssystemet TSS
WinWrap Basic	Polar Engineering and Consulting	Visual Basic-tolk
OLETools 5.0	MicroHelp	Kalender
SLCalend 8.0.0.5	SamLogic	Kalender
Formula One 4.1.2.2	Visual Components	Kalkylark
Graphical Server 4.52	Bits Per Second	Grafikpresentation
Visual Writer 1.02.502	Visual Components	Texthantering
AccuSoft ImageGear 8.1.37.c	AccuSoft	Scanning (IFO)
Spellchecker	Oribi	Rättstavning
Spellchecker	Lingsoft	Rättstavning Finland
FlexGrid Control 5.00.3714	Microsoft	Tidbokning (IFO)
ZipArchive	Artpol Software	TCU m.fl. komponenter
RabbitMQ	Open source	Meddelandehantering på applikationsserver. Admin lokalt via http://localhost:15672

13.3 D1) Installerade databaser

Nedan beskrivs de databaser som installeras med Lifecare installer. Vissa databaser är delsystemsberoende och återfinns bara då aktuellt delsystem finns installerat. Vissa databaser installeras enbart då en viss feature har köpts av kommunen och vissa behöver aktiveras via LCC för att dyka upp. Så nedan är summan av samtliga möjliga databaser och skiljer sig alltså från kund till kund.

De delsystem som är gemensamma för kund, har kundnamnet som suffix. De delsystem som är gemensamma för en och samma TSS-domän, har detta domännamn som prefix.

Databas	Delsystem	Beskrivning
HCWMETA1	Samtliga installationer	Metadata för alla delsystem
HCWMYMESSAGES_Kundnamn	Samtliga installationer (används av IFO/VoO)	Meddelandedata
HCWREPORT	Samtliga installationer (används av VoO)	Rapportdata för lastbalansering
HWE_WEBatch	KIR/IFO/VOO	Batchmotor nya bakgrundsjobb
HWE_SYSLOG	Samtliga installationer	Applikationsloggar
HWE_SignService	Samtliga installationer	Temporärlagring av signeringsdok samt loggning
HWE_Identity	Samtliga installationer	Identifieringsdb för inloggningar hanterade av IdentityServer
HWE_Domän_ActivityLog	VoO (EC)	Applikationsaktivitetsloggar
HWE_Domän_Checklist	IFO/VoO (FC/EC)	Checklista avvikelse
HWE_Domän_CitizenInternal	VoO (EC) - medborgartjänst VoO	Loggning och länkinfo
HWE_Domän_Compensation	VoO (EC)	Ersättning Utförare
HWE_Domän_Deviation	IFO/VoO (FC/EC)	Avvikelser, IFO/VoO
HWE_Domän_EconomyConfiguration	VoO's ersättare för FtB	Ekonomidata
HWE_Domän_ECPlanning	VoO (EC)	Planering (fd Lapscare)
HWE_Domän_ECProvider	VoO (EC)	Utförare
HWE_Domän_ECReportedVisit	VoO (EC)	Besöksrapportering
HWE_Domän_ECSEReport	VoO (EC)	Rapporter medborgartjänster
HWE_Domän_FCSEReport	IFO (FC)	Rapporter medborgartjänster
HWE_Domän_Housing	VoO (EC)	Vård- och omsorgsdata
HWE_Domän_ResourceModule	VoO (EC)	VoOs Resursregister
HWE_Domän_Tida	VoO (EC)	Tidrapportering
HWE_Domän_TimeBook	VoO/IFO (EC/FC)	Bokningssystem - Tidbok
HWE_Domän_TSS	Gemensam**	Ersätter TSS på disk
HWE_Domän_WorkSchedules	VoO (EC)	Schemaintegration Planering
Domän_CSI	VoO (EC)	Schemaintegrationsdata

Databas	Delsystem	Beskrivning
Domän_EKO	FtB (används av IFO/VoO)	Ekonomidata
Domän_KI0	KIR	Befolkningsregister
Domän_KQ0	VoO (EC)	Vård- och omsorgsdata
Domän_LD0	IFO (FC)	Familjeomsorgsdata

HWE_xxx -> namnstandard för nya Lifecaredatabaser på systemnivå
HWE_Domän_xxx -> namnstandard för nya Lifecaredatabaser per domän
Domän_ -> Följande databaser kan förekomma med denna äldre namnstandard; Activity, Deviation, Housing. Dessa kommer med tiden att migreras över till ny db med ny namnstandard enligt ovan.

** Efter aktivering

13.4 E1) Portförteckning - kommunikation mellan Procapita-klient och server

Port	Typ	Namn	Beskrivning
2100	tss	TSS	Behörighetssystem
2110	broker	KIR	Befolkningsregister
2114	broker	IFO	Individ och familjeomsorg
2116	broker	VoO	Vård och omsorg
2119	broker	IFO - Mina meddelanden	Meddelanetjänst - IFO
2120	broker	FtB	Konteringsdel för IFO, VoO
23110	Webservice	HCW.Welfare.KIR.ServiceModel.IISHost	KIR
23114	Webservice	HCW.Welfare.FC.ServiceModel.IISHost	IFO
23116	Webservice	HCW.Welfare.EC.ServiceModel.IISHost	VoO
30600	broker	CDS	Centralt Dokument System
30601	broker	Extrakt	Extraktserver
30610	broker	PCC	Gemensamma tjänster mellan delsystemen
30611	broker	Integration KIR	Integrationer KIR
30612	broker	Integration IFO	Integrationer IFO
30613	broker	Integration VoO	Integrationer VoO
30710	tns	Tieto Name Server	Namnservice
30722*	tev	Tieto Event Service	Händelseserver
30751	tes	Tieto Error Service	Hanterar loggning

*denna port var tidigare dynamisk och kan därför variera från kund till kund. Nyinstallerade miljöer kommer dock från 11v03 alltid att ha port 30722.