TDialog – Specifikation och teknisk plattform

Systemkomponenter

TDialog är en lösning för säker meddelandehantering. Grunden i lösningen är att meddelanden lagras i en för kunden central miljö och att den inte kan läsas. Oavsett vilka systemkomponenter som används av en specifik kund så krävs samma plattform.

Meddelandehantering

TDialog hanterar meddelanden skickade från en starkt autentiserad användare till en annan. Användarna kan finnas både innanför och utanför organisationen. Endast en notifiering skickas till mottagarens e-post, meddelandet med den känsliga informationen sparas i lösningen, och användaren måste logga in med stark autentisering i ett webbgränssnitt för att se det.

Uppsättningsalternativ

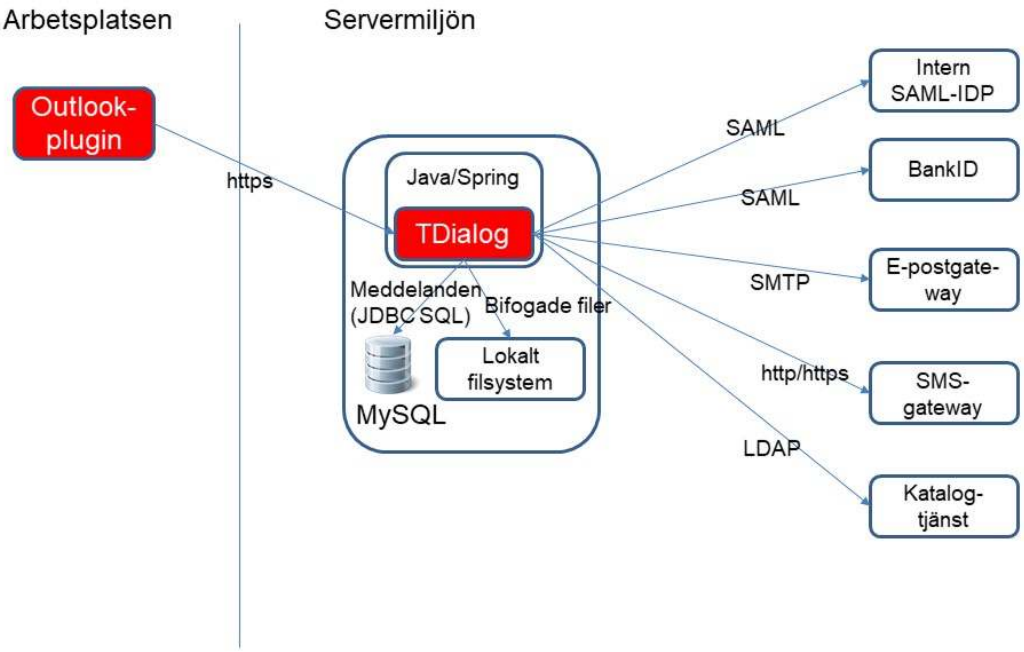
TDialog erbjuds dels som så kallad on-prem-lösning, där Compodium säljer en programvara som kunden själv, ofta med hjälp av support-/driftspartner, installerar och använder i sin miljö och dels som tjänst, dvs att TDialog installeras, konfigureras och driftas i Compodiums datacenter. Nedan delas upp mellan on-prem-alternativet och tjänstealternativet.

Uppsättningsinformation – TDialog on-prem

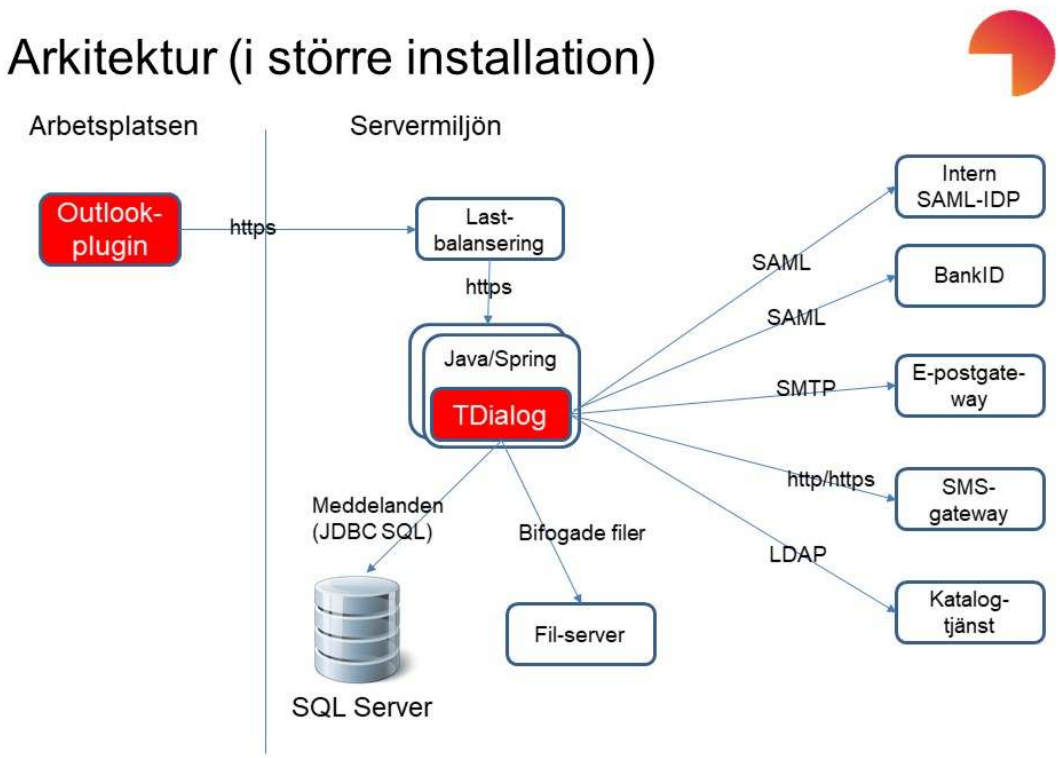
TDialog är en standard Java-lösning som är mycket flexibel vad gäller plattform. Databas med JDBC- och SQL-förmåga samt en miljö som kan köra en Java-lösning är det som krävs. Installations- och uppgraderingsscript är gjorda för MySQL, men motsvarande script för MSSQL är på väg.

Vad gäller rekommenderad plattform så är det mycket beroende på användning. Normalt är inte hastighet ett problem i TDialog, men det beror på antalet meddelanden.

Arkitektur (i normal installation)



www.tdialog.com, info@tdialog.com, 076-711 95 69



Not om filserver

I TDialog lagras meddelandeinformation (rubrik, text etc) i databas medan bilagorna lagras på fil. I en uppsättning med flera applikationsservrar behövs därför ett konsistent sätt att lagra fildata som är åtkomligt från samtliga applikationsservrar för både läsning och skrivning.

Rekommenderad plattform för Linux

På Linux bör 2 CPU:er med 4 GB RAM räcka för en grundinstallation, och 80 GB disk för installation, information och loggar. Med högre krav och mer frekvent användning, monitorera diskanvändning och systemresurser för att veta om det är dags att skala upp.

Rekommenderad plattform för Windows

Medelstor Windows-server. De exakta kraven är inte så viktiga, men nedan finns ett exempel på en sådan miljö.

- 2 x 2,4 GHz processor
- 8 GB RAM
- 80 GB för installation, information och loggar

Med tanke på informationens känslighet så bör inga andra applikationer och tjänster köras på samma maskin. TDialog använder inga specifika Windows-tjänster.

Med högre krav och mer frekvent användning, monitorera diskanvändning och systemresurser för att veta om det är dags att skala upp

Användarens webbläsare

TDialog körs alltid i en webbläsare, även om användaren kommer in via Outlook-plugin eller genom att följa en e-postlänk.

TDialogs webbläsarstödet följer till stor del vilka webbläsare som stöds av JQuery. Följande stöds i princip:

- Internet Explorer: 9+
- Edge: Senaste och näst senaste
- Chrome: Senaste och näst senaste
- Firefox: Senaste och näst senaste
- Safari: Senaste och näst senaste

Vi tar gärna emot feedback om något av detta inte stöds i senare versioner av Windows, iOS eller Android.

Det vi primärt testar är:

- Internet Explorer 11, Windows 10
- Senaste Edge, Windows 10
- Senaste Chrome, Windows 10
- Senaste Firefox, Windows 10

Öppna portar

- Port 443 inkommande trafik (HTTPS).
- Utgående trafik till e-postgateway (SMTP, port 25) (e-postnotifieringar)
- Utgående LDAP/LDAPS (389 eller 636) för koppling till adressregister
- (3.5 och framåt) Utgående 443 för uppkoppling till-SMS gateway (HTTPS) (engångsmeddelanden)

”Utgående” betyder att kommunikationen initieras inifrån TDialog, ”ingående” att kommunikationen initieras utifrån.

Vilka systemkomponenter installeras?

- Java
- TDialog
- MySQL eller SQL Server

Vilka operativsystemkomponenter behöver vara aktiverade?

- Inga, förutom det som behövs för att köra Java och eventuell databas.

Åtkomst vid installation och support

Vid installationstillfället behöver programvara kunna kopieras till maskinen och installeras på maskinen.

För snabb support kommer remoteåkomst behövas (se supportavtal). Man behöver dock tillse att åtkomst till miljön föregås av korrekt stark autentisering, eftersom den innehåller känsliga personuppgifter. Det ställer krav på vilken typ av åtkomst som används, så fort TDialog ska fyllas med "riktig" information.

Backup och återställning

För att komma igång med minimal nedtid rekommenderas att regelbundna snapshots tas av TDialog-applikationen. Om databas, fillager och loggar inte ligger på applikationen kommer applikationen endast förändras vid omkonfiguration, så i det fallet viktigare att snabbt kunna återställa än att ha en färsk backup.

Konfiguration (config-katalogen), databasen, fillagret och loggarna bör backas upp, var och en enligt organisationens vanliga backuprutiner.

Vid återläsning läggs konfiguration, databas och fillager på konfigurerad plats och applikationen startas.

Uppsättningsinformation - TDialog som tjänst

Teknik

TDialog som tjänst körs i Compodiums datacenter. Varje kund har en egen TDialog-installation i en Docker-container och en separat databas i ett databaskluster (Galera). Det finns en hög nivå av automatisering i uppsättning och förändringar av dessa installationer.

Rent fysiskt befinner sig dessa installationer i co-location med lås och kameraövervakning som endast Compodium har tillgång till.

GDPR mfl lagrum

Compodium driftar dessa TDialog-installationer själva, dvs är personuppgiftsbiträde. Compodium är ett helsvenskt företag.

Information inför installation och konfiguration

Autentisering

TDialog har ingen egen autentisering, utan det krävs en s.k. SAML-IDP, dvs en mjukvara som kan utföra autentisering och skicka ett SAML-intyg för utförd autentisering. Fördelen med det är att TDialog är mycket flexibelt vad gäller vilken autentisering som utförs. I normalfallet finns en sådan programvara tillgänglig hos kommun, landsting eller myndighet (ofta är den kopplad till Skolfederation i en kommun, vårdtjänster som Pascal i ett landsting respektive interna tjänster på en myndighet). Produkter som hanterar denna typ av autentisering är exempelvis ADFS, Nexus Access Gateway, Phenix ID eller Shibboleth. E-legitimationstjänster eller Ineras Säkerhetstjänster 2.0 kan användas för autentisering.

Användaråtkomst

I samband med autentisering med SAML så skickas ett intyg när autentisering är utförd. Det intyget kan också innehålla attribut som ger ytterligare information om användaren, exempelvis grupptillhörighet. Sådana attribut styr åtkomsten till TDialog, vilket oftast innebär att dels behöver sådana attribut ofta läggas till i katalogtjänsten (AD:t), och dels behöver SAML-IDP:n konfigureras för

att skicka med dessa attribut. Detta är standardfunktionalitet i SAML-IDP:er men det är ett konfigurationsarbete som behöver göras.

De behörigheter som styrs på detta sätt i TDialog är dels att alls ha åtkomst till systemet, och dels att ha åtkomst till en eller flera funktionsbrevlådor.

Vid installation av TDialog konfigureras vilka attribut och värden som ska krävas för åtkomst (om några) men ett exempel skulle kunna vara:

TDialog=allow

Tillgång till funktionsbrevlådor bestäms genom att adressen till funktionsbrevlådan specificeras med ett attribut, exempelvis:

TDialogMailboxes=ungdomsmottagning@grevlinge.se

Spårbarhet

Användares skapande, borttagande och meddelandehantering loggas med spårbarhet till inloggad användare.

E-postgateway

Åtkomst och eventuell kontoinloggning till e-postgateway krävs för att kunna skicka e-postnotifieringar när nya meddelanden/chatstarter inkommit.

Kryptering

Före produktionsanvändning av TDialog, se till att kryptering är påslaget genom att sätta server.encryption.enabled=true i application.properties, gå in som administratör under ”inställningar” och sätta krypteringslösenord. Se till att lösenordet sparas och skyddas enligt gängse rutiner.

TDialog använder AES256 som krypteringsalgoritm i vila och PKCS5 PBKDF2 för nyckelgenerering.

Data i rörelse krypteras med TLS, precis som all annan https-trafik. Man kan styra vilka ciphers och TLS-versioner som ska accepteras, server.ssl.ciphers, respektive server.ssl.protocols (observera att trots namnen har dessa properties inte längre något med SSL att göra).