Flytta Lokal Samtyckesadministration till Inera

Tjänst under avveckling

Dessa sidor kommer att tas bort 2023-01-01

Dokumenthistorik

Datum	Version	Namn	Förändring
16 Nov 2021	0.1	Unknown User (lexhagenm)	Dokument upprättat
22 Mar 2022	0.2	Unknown User (lexhagenm)	Procedur omgjord så att den liknar migrering av spärrar.

Innehåll

1. Bakgrund

Alternativet till att ha egen drift av Samtyckestjänsten är att administrera sina samtycken i Ineras nationella installation av Säkerhetstjänster.

Innan man beslutar sig för att flytta något data mellan Lokala Säkerhetstjänster och Ineras nationella installation av nya Samtyckestjänsten så kan man därför undersöka vad som händer ifall man inte flyttar över något data utan endast kopplar över tjänsten till Ineras samtyckestjänst. Kommer det att registreras nya då utan användarpåverkan så kanske det är onödigt att flytta något data?!

2. Förutsättningar

1. Avtal med Inera för att nyttja Samtyckesadministration i nationella installationen. Se https://www.inera.se/tjanster/sakerhetstjanster/Sakerhetstjanster/ under "Beställ Säkerhetstjänster - Spärr, Samtycke, Logg".

2. Avtal med CGI för eventuell hjälp med flytten (vanligtvis ett fåtal timmar men är beroende av hur mycket hjälp regionen behöver på "sin sida").

3. Anslutning till Samtyckeskontrakt version 2 via NTjP för de system som ursprungligen registrerade samtycken i Lokala Säkerhetstjänster. Alternativt ansluta sin Regionala Tjänsteplattform för att själva administrera anslutningarna. Säkerställ att systemen klarar de nya versionerna via tester. Stöd för detta finns även hos NMT

4. Teknisk kontakt alternativt serveraccess åt CGI för att exportera samtyckesdata direkt från databasen samt stänga ner den Lokala Samtyckestjänsten när flytten är gjord.

5. För verifiering av utförandet i testmiljöer krävs en fungerande testmiljö hos regionen samt SITHS-kort för testmiljöer med behörigheter i HSA Test (medarbetaruppdrag med syfte Administration och personlig egenskap *BIF;Samtyckesadministratör*). OBS! Korten skiljer sig från de man använder i produktionsmiljöer och måste dessutom vara av rätt typ (TEST SITHS e-id Person HSA-id 3 CA v1). Access till Ineras testmiljö verifieras innan av administratören på https://samtyckestjanst.ineratest.org/

3. Arbetssätt

Proceduren med att flytta samtyckesdata bör inledas med ett möte mellan Region, Inera och CGI för en samsyn på tillvägagångssättet. Här inventeras förutsättningarna som t.ex att alla anslutna system är kompatibla med rätt version av samtyckeskontrakten.

För att känna en trygghet i att Regionen har förutsättningarna på plats så är det en stor fördel ifall regionen har en fungerande testmiljö med anslutna system att utföra stegen på innan man gör detta i produktionsmiljöer.

Den tekniska personalen på Regionen bör sätta sig in i det tekniska genomförandet och förbereda den administrativa personalen så att de är förberedda på vilka tester som bör genomföras under flytten. Den administrativa personalen kan också vilja läsa igenom användarhandboken för det uppdaterade gränssnittet i Ineras nya tjänst för Samtyckesadministration: Användarhandbok Samtyckestjänsten

Förslag på arbetsordning:

1. Planeringsmöte. Medverkande: Region, Inera och CGI.
2. Flytt av Samtycken i Testmiljö. Medverkande: Region och CGI.
3. Verifiering av flytten i Testmiljö. Medverkande: Region
4. Planering av datum och säkring av resurser för flytt i Produktionsmiljö.
5. Flytt av Samtycken i Produktionsmiljö. Medverkande: Regionoch CGI.
6. Verifiering av flytten i Produktionsmiljö. Medverkande: Region

4. Tekniskt Utförande

När punkterna under förutsättningar är uppfyllda kan man gå vidare till utförandet av dataflytten.

Dessa steg görs i testmiljön först innan det görs i produktionsmiljön:

1. Ifall Regionen skall registrera/hämta samtycken till t.ex ett journalsystem via NTjP och/eller en regional tjänsteplattform så verifieras denna anslutning först av allt (allmän resp teknisk anslutning).
2. Regionen utför stopp för hantering av samtycken i den egna samtyckestjänsten.
3. Befintliga aktiva samtycken exporteras direkt från regionens MySQL-databas mha ett skript som CGI tillhandahåller.
4. Resultatet zippas i ett lösenordsskyddat arkiv och läggs överförs på ett säkert sätt till CGI.
5. CGI registrerar samtyckena i Ineras installation av Samtyckestjänsten så att de kan administreras där.
6. Regionen verifierar med ett par stickprov att de nu kan administrera sina samtycken i Ineras installation.
7. Regionen stänger ner sin egen Samtyckestjänst.

4.1. Exportera samtyckesdata från MySQL-databasen

CGI förser organisationen med ett SQL-skript och instruktioner om hur detta kan exekveras mot databasen för att få ut aktiva samtycken. Den resulterande filen förs på ett säkert sätt över till CGI som registrerar samtyckena så att de kan administreras i Ineras installation av Samtyckestjänsten:

Test
https://samtyckestjanst.ineratest.org
Produktion
https://samtyckestjanst.inera.se

SQL-skriptet för extrahering har INTO OUTFILE i frågan som säger åt MySQL att skriva resultatet till en tecken-separerad fil.

OBS!
INTO OUTFILE kräver att användaren som exekverar skriptet har behörighet (GRANTs) till *file*. T.ex för användaren sak genom kommandot *grant file on *.* to 'sak'@'127.0.0.1';*
INTO OUTFILE kräver även att variabeln *secure_file_priv* är satt under *[mysqld]*-sektionen i MySQL-serverns konfigurationsfil till en för servern skrivbar sökväg.

```
[mysqld]
secure-file-priv=/var/lib/mysql-files
```

Vid en eventuell förändring av värden i konfigurationsfilen måste MySQL-servern startas om för att förändringen ska få effekt.

Man kan kontrollera värdet på denna i MySQL-variabel med kommandot:

```
mysql> SHOW VARIABLES LIKE "secure_file_priv";
+------------------+----------------------+
| Variable_name    | Value                |
+------------------+----------------------+
| secure_file_priv | /var/lib/mysql-files |
+------------------+----------------------+
1 row in set (0.00 sec)
```

Möjligen kan SQL-skriptet för extrahering nu behöva modifieras så att sökvägen till katalogen för filskrivningen stämmer med variablen ovan.

```
INTO OUTFILE '/var/lib/mysql-files/blocks_db.txt'
FIELDS TERMINATED BY '\t' OPTIONALLY ENCLOSED BY '"' ESCAPED BY ''
LINES TERMINATED BY '\n'
```

Exekvera skriptet för att extrahera samtycken på MySQL-servern:

mysql -h 127.0.0.1 -uroot -p consent < extract_consents_into_file.sql

Ladda ner skriptfil som extraherar de samtycken som skall migreras...

- sql_consents.zip

5. Övriga tjänster i Lokala Säkerhetstjänster

5.1. Autentisering - IdP

IdP-funktionalitet erbjuds både som nationell tjänst och lokal installation (se Lokal IdP). Läs mer om detta på sidorna för Autentisering via SITHS eID

5.2. Spärrtjänsten

Se Flytta Lokal Spärradministration till Inera

5.3. Loggtjänsten

Inget fullständigt övertagande av en regions loggarkiv erbjuds. Kontakta Inera för strategi ifall regionen har konsumenter kopplade till StoreLog-kontraktet och därmed en större mängd loggar att arkivera. Endast loggar från Säkerhetstjänster själv, som ett resultat av arbete i Spärradministration, brukar anses nog att regionen lagrar i sina loggarkiv på någon lagringsyta i fem år i enlighet med patientdatalagen.