**Min hälsoplan**

**Installationsmanual**

**Revisionshistorik**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Beskrivning** | **Författare** |
| 2015-03-04 | PA1 | Första versionen | PL |

**Innehållsförteckning**

1 Inledning 5

2 Syfte 5

3 Komponenter 5

4 Förutsättningar för installation 5

5 Installation av systemprogramvara 7

5.1 Java SDK 7

5.2 Apache Tomcat 7

5.2.1 Installation 7

5.2.2 Inställningar 8

5.3 NGINX 8

5.4 PostgreSQL 9

6 Installation av applikationen 10

6.1 Hämta applikationen 10

6.2 Inställningar för initial installation 10

6.3 Inställningar för fullständig installation 12

6.3.1 Installera funktionscertifikat 12

6.3.2 Inställningar för MVK SSO 13

6.3.3 Inställningar för mobilnotiser (push) 13

6.3.4 Inställningar för mobilt BankID 14

6.3.5 Inställningar för e-post (SMTP) 14

6.3.6 Inställningar för NGINX och extern Webb-access 14

6.4 Slutför fullständig installation 16

**Definitioner och Referenser**

**Definitioner**

|  |  |
| --- | --- |
| **Term** | **Beskrivning** |
| APNS | Apple Notification Service |
| CA | Certificate Authority. Ställer ut digitala certifikat |
| GCM | Google Cloud Messaging |
| CSR | Certificate Signing Request |
| Java SDK | Öppen och fri att använda applikationsplattform |
| MVK | Mina vårdkontakter där tjänsten Min hälsoplan tillgängliggörs för användare |
| NGINX | Är en fri att använda och öppen källkodsbaserat Webbserver |
| Linux | Är ett fritt att använda och öppen källkodsbaserat operativsystem för datorer |
| PostgreSQL | Är en fri att använda och öppen källkodsbaserat databas |
| SSO | Single Sign On |
| Tomcat | Kortnamn för en fri att använda och öppen Java applikationsserver |

**Referenser**

|  |  |
| --- | --- |
| **Dokument** | **Länk** |
| Min hälsoplan webb | <http://www.minhalsoplan.se> |
| Min hälsoplan programvara | <https://github.com/MinHalsoplan/netcare-healthplan> |
| Min hälsoplan demo | <http://demo.minhalsoplan.se/v2> |
| Min hälsoplan - SAD | <https://github.com/MinHalsoplan/netcare-healthplan> |
| PostgreSQL | <http://www.postgresql.org/docs/9.3/static/admin.html> |
| NGINX | <http://nginx.org/en/docs/install.html> |
| Apache Tomcat | <http://tomcat.apache.org/tomcat-7.0-doc/setup.html> |
| Ubuntu | <http://www.ubuntu.com/server/management> |
| Java SDK on Ubuntu | <https://help.ubuntu.com/community/Java> |

# Inledning

Min hälsoplan är en e-hälsotjänst i Mina vårdkontakter där vårdpersonal och patienter tillsammans skapar en hälsoplan. Hälsoplanen innehåller en eller flera aktiviteter som patienten får påminnelse att göra, samt kan han eller hon rapportera in resultat från aktiviteten direkt till personalen. Syftet med Min hälsoplan är att stötta både patient och personal under en kort eller lång uppföljning genom att öka tillgänglighet och kvalitet på information samt skapa en ökad kontinuitet i vårdprocessen.

Se även: <http://www.minhalsoplan.se>

# Syfte

Detta dokument beskriver hur applikationen Min hälsoplan med nödvändiga tredjeparts systemprogramvaror installeras och konfigureras.

# Komponenter

Min hälsoplan är en Webbapplikation som är byggd för att köras på en plattform bestående av Linux servers med Java plattformen, Apache Tomcat applikationsserver, PostgresSQL databashanterare samt NGINX som webbserver.

Förutsättningar för installation är en Linux server där Ubuntu 11.10 rekommenderas och används även som referens i nedanstående instruktioner.

Följande plattform är verifierad.

* Java 1.7
* Apache Tomcat 7.0
* PostgreSQL 9.3
* NGINX 1.0

Min hälsoplan paketeras som en standard WebARchive (WAR) fil och den senaste versionen är 2.2.

# Förutsättningar för installation

För att kunna utföra en initial installation, dvs. att starta upp applikationen utan externa kopplingar krävs följande:

1. Åtkomst till en fysisk eller virtuell server med operativsystemet Ubuntu 11.10 eller senare. Det antas vidare att administration av servern som backup och återställning hanteras i den infrastruktur där servern hanteras.
2. Att servern är uppkopplad mot internet och att portarna 80, 443 och 8890 (Mobilt BankdID) är öppna för utgående trafik. För inkommande trafik i produktion används enbart port 443 (HTTPS).
3. Att installatören är administratör (root) på servern.
4. Att installatören har erfarenhet som administratör och liknande installationer med pakethanteraren apt-get.
5. Att installatören har erfarenhet av verktyg som openssl och Java keytool ör hantering av funktionscertifikat.

För att slutföra en fullständig installation krävs dessutom:

1. Publikt registrerat DNS namn
2. Funktionscertifikat för det publika DNS namnet för att kryptera HTTPS (TLS) Webb trafik
3. Avtal och Steria/CGI funktionscertifikat för att koppla upp sig mot mobilt BankID (CGI)
4. Avtal och Apple funktionscertifikat för att koppla upp sig mot Apples meddelandetjänst (APNS)
5. Avtal och API nyckel för att koppla upp sig mot Google Plays meddelandetjänst (GCM)
6. Avtal och SITHS funktionscertifikat för att koppla upp sig som tjänst till MVK (MVK SSO)
7. Konto till extern mail (SMTP) tjänst för att meddela applikationsfel till en utpekad funktionsbrevlåda

# Installation av systemprogramvara

## Java SDK

Min hälsoplan är verifierad med Oracle Java 1.7. Förmodligen fungerar även Open JDK 1.7 utan några problem. Oracle Java installeras med fördel enligt följande:

$ sudo apt-get install software-properties-common

$ sudo add-apt-repository ppa:webupd8team/java

$ sudo apt-get update

$ sudo apt-get install oracle-java7-installer

Verifiera att Java är korrekt installerat genom att köra kommandot nedan och verifiera att versionen skrivs ut på liknande sätt.

$ java –version

Java(TM) SE Runtime Environment (build 1.7.0\_76-b13)

Java HotSpot(TM) 64-Bit Server VM (build 24.76-b04, mixed mode)

## Apache Tomcat

### Installation

Apache Tomcat 7 är verifierad och installeras med följande kommandon:

$ sudo apt-get install tomcat7

Starta Tomcat applikationsserver:

$ sudo service tomcat7 start

Verifiera Tomcat genom att gå till adressen <http://localhost:8080> som då ska svara med en index sida och HTTP 200.

$ wget –O - <http://localhost:8080>

esolving localhost (localhost)... ::1, 127.0.0.1

Connecting to localhost (localhost)|::1|:8080... connected.

HTTP request sent, awaiting response... 200 OK

Length: 1895 (1.9K) [text/html]

Saving to: 'STDOUT'

...

Alternativt kan man inspektera loggfilen där de sista raderna ska se ut något liknande som nedanstående:

$ tail /var/log/tomcat7/catalina.out

...

INFO: Starting ProtocolHandler ["http-bio-8080"]

Mar 03, 2015 7:52:41 PM org.apache.catalina.startup.Catalina start

INFO: Server startup in 925 ms

### Inställningar

Min hälsoplan applikationen kräver en del inställningar i Java plattformen som minne och profiler. Tomcat rekommenderar att dessa läggs i filen /usr/share/tomcat7/bin/setenv.sh som måste skapas. Använd lämpligen den inbyggda ’vi’ editorn för att skapa filen:

$ sudo vi /usr/share/tomcat7/bin/setenv.sh

Lägg till nedanstående inställning och spara till filen:

**setenv.sh**

export JAVA\_OPTS="-Dspring.profiles.active=prod,mobile-prod -XX:MaxPermSize=512m -Xmx1024m"

Säkerställ dessutom att den aktuella ändpunkten (Connector) som definieras i konfigurationsfilen /etc/tomcat7/server.xml är uppsatt för att hantera UTF-8 tecken, se vidare nedan.

**server.xml**

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

**URIEncoding="UTF-8"**

redirectPort="8443" />

## NGINX

NGINX är en Webbserver som kan användas som reverse proxy men också för att på ett flexibelt sätt hantera HTTP och HTTPS trafik.

$ sudo add-apt-repository ppa:nginx/stable

$ sudo apt-get update

$ sudo apt-get install nginx

$ sudo service nginx start

Verifiera NGINX genom att gå till adressen http://localhost som då ska svara med en index sida och HTTP 200.

$ wget –O - <http://localhost>

Resolving localhost (localhost)... ::1, 127.0.0.1

Connecting to localhost (localhost)|::1|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 867 [text/html]

Saving to: 'STDOUT'

...

## PostgreSQL

PostgreSQL är en relationsdatabas där all information om hälsoplaner lagras.

$ sudo apt-get install postgresql-9.3

$ sudo service postgresql start

Verifiera att PostgreSQL databasen fungerar genom att ansluta med det medföljande klientprogrammet psql. Kommandot ’\q’ alternativt ’Ctrl-d’ avslutar psql.

$ sudo -u postgres psql postgres

psql (9.3.6)

Type "help" for help.

postgres=# **\q**

$

Skapa en databasanvändare med namn mhp-admin och ange dessutom lösenord som hädanefter refereras som <db-password>.

**$** sudo -u postgres createuser mhp-admin

$ sudo -u postgres psql

$ postgres=# \password mhp-admin

Enter new password: <db-password>

Enter it again: <db-password>

Skapa en databas med namnet mhpdb och starta sedan psql för att tilldela mhp-admin rättigheter att administrera databasen.

**$** sudo -u postgres createdb mhpdb

$ sudo -u postgres psql

postgres=# grant all on database mhpdb to "mhp-admin";

GRANT

# Installation av applikationen

## Hämta applikationen

Applikationen är en WAR fil som lämpligen hämtas direkt från källkodsarkivet för att installeras i Tomcat.

Hämta applikationen i detta fall version 2.2.2:

**$** wget <https://github.com/MinHalsoplan/netcare-healthplan/releases/download/netcare-2.2.2/netcare-web-2.2-2.war>

...

Saving to: 'netcare-web-2.2-2.war'

100%[=====================================>] 26,453,352 340KB/s in 85s

2015-03-05 03:22:06 (303 KB/s) - 'netcare-web-2.2-2.war' saved [...]

## Inställningar för initial installation

Innan det går att starta applikationen krävs det ett antal initiala inställningar och återfinnas i hemmabiblioteket för den användare som exekverar applikationsservern. Det är således användaren tomcat7 som kör processen och därmed ska inställningarna placeras i tomcat7 hemkatalogen. Observera att man mycket väl kan länka biblioteket för inställningar till en annan plats under förutsättning att tomcat7 har behörighet att läsa konfigurationsfiler och skriva till loggfiler som ligger i samma katalogstruktur.

Efter de initiala inställningarna som säkerställer att applikation kan startas och köras i lokal miljö så återstår fullständiga inställningar som säkerställer att integrationerna med externa tjänster fungerar.

Skapa katalogstruktur och filer för inställningar:

$cd /usr/share/tomcat7

$ sudo –u tomcat7 bash

$ mkdir –p netcare-healthplan-prod/logs netcare-healthplan-prod/cert

$ cd netcare-healthplan-prod

$ touch application.properties bankid.properties database.properties email.properties mvk.properties push.properties

Ställ in initiala inställningar för applikationen genom att editera följande filer:

**application.properties**

# email för att erhålla applikationsfel, se email.properties för

# själva kontoinställningarna

support.email = nc-support@callistaenterprise.se

# avgränsare för Excel exporter (CSV)

csv.delimiter = ,

# hur ofta ska jobb för påminnelser köras (i minuter)

reminder.time = 15

**database.properties**

# inställningar för den lokala PostgreSQL databasen

database.vendor = POSTGRESQL

database.dialect = org.hibernate.dialect.PostgreSQLDialect

database.driver = org.postgresql.Driver

database.url = jdbc:postgresql://localhost/mhpdb

database.username = mhp-admin

# det lösen som angavs när användaren skapades ovan

database.password = <db-password>

database.show-sql = false

database.format-sql = false

database.updateStrategy = update

**push.properties**

# initialt är notifieringar till Apple iOS (APNS) avstängt

apns.production = false

Med dessa inställningar kan man starta upp Min hälsoplan applikationen. Stegen är att stänga ned Tomcat och sedan installera den hämtade WAR filen för att starta upp Tomcat igen.

$ sudo service tomcat7 stop

\* Stopping Tomcat servlet engine tomcat7 [ OK ]

$ rm –rf var/lib/tomcat7/webapps/ROOT\*

$ cp netcare-web-2.2-2.war /var/lib/tomcat7/webapps/ROOT.war

$ sudo service tomcat7 start

Nu kan man kontrollera att Min hälsoplan har startat genom att inspektera loggfilerna där Tomcat loggfilen ska innehålla något liknande nedanstående (och inga fel dessförinnan)

$ tail -f /var/log/tomcat7/catalina.out

...

INFO: Starting ProtocolHandler ["http-bio-8080"]

Mar 05, 2015 4:16:16 AM org.apache.catalina.startup.Catalina start

INFO: Server startup in 20114 ms

Loggfilen för Min hälsoplan ska set ut liknande nedanstående:

$ tail -f /usr/share/tomcat7/netcare-healthplan-prod/logs/healthplan.log

...

015-03-05 04:52:57,965 DEBUG o.c.netcare.web.util.WebUtil - Check whether to setup initial data...

2015-03-05 04:52:58,021 INFO o.c.netcare.core.job.SystemAlarmJob - ======== ALARM JOB STARTED =========

2015-03-05 04:52:58,083 DEBUG o.c.netcare.web.util.WebUtil - System currently have 21 county councils, 5 roles and 1 care units.

2015-03-05 04:52:58,087 DEBUG o.c.netcare.web.util.WebUtil - Initial data already setup. Returning...

2015-03-05 04:52:58,087 INFO o.c.n.w.l.ApplicationListener - ======== NETCARE STARTED ========

...

Dessutom ska det gå att köra lokala HTTP anrop med tex wget:

$ wget -O - http://localhost:8080

...

HTTP request sent, awaiting response... 200 OK

Length: 223 [text/html]

Saving to: 'STDOUT'

...

<!DOCTYPE html>

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<title>Min hälsoplan</title>

...

Det bör vidare poängteras att databasen och en del referensdata automatiskt skapas när Min hälsoplan applikationen startar för första gången. Därför är det viktigt att man alltid startar med en tom databas.

## Inställningar för fullständig installation

### Installera funktionscertifikat

Funktionscertifikaten placeras i underkatalogen ~/tomcat7/netcare-healthplan-prod/cert och följande certifikat måste inhämtas från respektive part med gängse CSR.

Certifikat och nycklar som ska finnas i katalogen för inställningar:

~/tomcat7/netcare-healthplan-prod/cert

|  |  |  |
| --- | --- | --- |
| **Filnamn** | **Typ** | **Kommentar** |
| mvk-prod.p12 | Klient SITHS CA v3 | Från Inera SITHS  Med privat nyckel |
| apns-prod.p12 | Klient Apple | Från Apple  Med privat nyckel |
| chain-server.pem | Server, hela kedjan med CA evetuellt intermediate samt server cert. | Tillhör Min hälsoplantjänsten och kan köpas av valfri leverantör. |
| server-key.pem | Nyckel | Den privata nyckeln för server certifikatet. |
| truststore-eidp.jks | Truststore | Ska innehålla Sterias CA certifikat och Bank Id tjänstens server certifikat |
| truststore-siths.jks | Truststore | Ska innehålla aktuellt SITHS CA som v3 |

### Inställningar för MVK SSO

Öppna filen ~/tomcat7/netcare-healthplan-prod/mvk.properties och ställ in följande parametrar. Parametrar markerade med fetstil måste tilldelas riktiga värden.

#

mvk.validatetoken.address = https://asbc.minavardkontakter.se/MvkAsb\_ValidateIDWeb/sca/ValidateToken

#

# Set this to true if the we should verify

# the server's dns name against the certificate's

# common name

#

mvk.commonNameCheck = true

#

# The name of the URL-parameter that

# contain the guid from mvk

#

mvk.guidParamName = guid

mvk.truststore.file = ${user.home}/netcare-healthplan-prod/cert/truststore-siths.jks

mvk.truststore.type = jks

**mvk.truststore.password = <password>**

mvk.keystore.file = ${user.home}/netcare-healthplan-prod/cert/mvk-prod.p12

**mvk.keystore.password = <password>**

mvk.keystore.type = pkcs12

**mvk.keystore.keyPassword = <key-password>**

mvk.create-missing-users = true

### Inställningar för mobilnotiser (push)

Öppna filen ~/tomcat7/netcare-healthplan-prod/push.properties och ställ in följande parametrar. Parametrar markerade med fetstil måste tilldelas riktiga värden.

# GOOGLE GCM SERVICES

**gcm.authKey = <api-auth-key>**

# Apple APNS SERVICES

apns.cert-file=${user.home}/netcare-healthplan-prod/cert/apns-prod.p12

**apns.cert-password = <cert-password>**

apns.production = true

### Inställningar för mobilt BankID

Öppna filen ~/tomcat7/netcare-healthplan-prod/bankid.properties och ställ in följande parametrar. Parametrar markerade med fetstil måste tilldelas riktiga värden.

# Nuvarande avtal och serviceId

bankid.serviceId = jonkoplan4729

bankid.displayName = Mina vårdkontakter

bankid.truststore.file=${user.home}/netcare-healthplan-prod/cert/truststore-eidp.jks

**bankid.truststore.password=<password>**

bankid.truststore.type=JKS

bankid.url=https://grp.funktionstjanster.se:8890/mbi/service

bankid.disableCNCheck = false

### Inställningar för e-post (SMTP)

Öppna filen ~/tomcat7/netcare-healthplan-prod/email.properties och ställ in följande parametrar. Parametrar markerade med fetstil måste tilldelas riktiga värden.

#

**email.host = <ex-smtp.gmail.com>**

**email.username = <email-username>**

**email.password = <email-password>**

### Inställningar för NGINX och extern Webb-access

Förutom att terminera HTTPS trafik så används NGINX till att hantera access loggning för all extern åtkomst. Det är enbart port 443 (HTTPS) som är öppen för extern åtkomst.

Konfigurationsfilerna för NGINX återfinns under katalogen /etc/nginx/sites-available. De aktiva återfinns under /etc/nginx/sites-enabled och normalt länkar man därifrån till de so, är tillgängliga för att aktivera och tar bort länkar för att de-aktivera.

Skapa en konfigurationsfil under /etc/nginx/sites-available som heter mhp och med följande innehåll. Parametrar markerade med fetstil måste tilldelas riktiga värden.

ssl\_certificate /usr/share/tomcat7/netcare-healthplan-prod/cert/chain-server.pem;

ssl\_certificate\_key /usr/share/tomcat7/netcare-healthplan-prod/cert/server-key.pem;

ssl\_session\_cache shared:SSL:10m;

ssl\_session\_timeout 10m;

server {

# enbart HTTPS porten

listen 443 ssl;

# serverns namn i enlighet med certifikat

**server\_name <dns-names>;**

# exponera inte information som eventuella angripare kan nyttja

server\_tokens off;

location / {

proxy\_pass http://127.0.0.1:8080;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-Proto $scheme;

proxy\_set\_header X-Forwarded-Host $host;

proxy\_set\_header X-Forwarded-Server $host;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

proxy\_redirect http:// $scheme://;

}

}

När detta är klart så ta bort default konfiguration, länka till den nya konifguration och starta om NGINX:

$ sudo rm /etc/nginx/sites-enabled/default

$ sudo ln –s /etc/nginx/sites-available/mhp /etc/nginx/sites-enabled/mhp

$ sudo service nginx restart

Förutsatt att servern är publikt åtkomlig från internet så kan man nu koppla upp sig med en bläddrare mot den aktuella servern: https://<server-name>

## Slutför fullständig installation

När samtliga ovanstående steg har utförts så återstår detaljer för backuphantering med mera som förutsätts finnas på plats i det datacenter som servern hanteras i.

För att slutföra krävs slutligen att man startar om Tomcat applikationsserver:

$ sudo service tomcat7 restart

Precis som under den initiala installationen så kan loggfilerna vara lämpliga att inspektera, dvs. /var/log/tomcat7/catalina.out för att säkerställa om applikationen startat korrekt, och

/usr/share/tomcat7/netcare-healthplan-prod/logs/healthplan.log för att säkerställa att applikationen med integrationer fungerar korrekt.

Att skapa script som regelbundet tar en kopia av databasen för backup på externt media beskrivs utförligt i manualen för PostgreSQL. Även hur en redundant databaslösning kan skapas och användas beskrivs utförligt i manualerna.

Exempel på hur en databas kan exporteras och komprimeras till filen mhpdp.dump.gz är:

$ pg\_dump -U mhp-admin –w mhpdb | gzip > mhpdb.dump.gz