# SIM DHS paigaldusjuhend

|  |  |  |  |
| --- | --- | --- | --- |
| **Versioon** | **Muutja** | **Muutmise kuupäev** | **Muudatus** |
| 1.0 | Erko Hansar | 16.12.2009 | Dokumendi algversioon |
| 1.1 | Erko Hansar | 04.01.2009 | Pisiparandused seoses alfresco-global.properties faili kopeerimisega GlassFish domeeni alla. |
| 1.2 | Erko Hansar | 18.01.2010 | Lisatud repositiooriumi tühjendamise osa. |
| 1.3 | Erko Hansar | 01.03.2010 | Lisatud uusi seadistusparameetreid. |
| 1.4 | Alar Kvell | 26.03.2010 | Lisatud ja kustutatud seadistusparameetreid. |
| 1.5 | Erko Hansar | 22.04.2010 | Sõnastik, kontaktandmed, tooteversioonide täpsustused, seadistuse täpsustused. |
| 1.6 | Alar Kvell | 25.03.2011 | Täiendatud varundamise ja taastamise juhendit |
| 1.7 | Alar Kvell | 08.04.2011 | Täiendatud rakenduse versioonivahetuse juhendit |

## Sissejuhatus

SIM DHS on Java EE tehnoloogial põhinev ja Alfresco (Community Edition 3.2 final) põhjal ehitatud dokumendihaldustarkvara.

Käesolev dokument kirjeldab SIM DHS tarkvara paigaldamist kliendi testkeskkonda ja on mõeldud kasutamiseks SMIT administraatoritele.

## Sõnastik

*SIM* Siseministeerium

*SMIT* Siseministeeriumi infotehnoloogia- ja arenduskeskus

*DHS* Dokumendihaldussüsteem

*SVN* Subversion koodirepositoorium

*WAR* Java web archive failiformaat

*Java EE* Java Enterprise Edition platvorm

*SMTP* Simple Mail Transfer Protocol

*IMAP* Internet Message Access Protocol

*NTLM* Microsoft authentication protocol

## Kirjeldus

Webmedia laeb projekti koodi ülesse SMIT-i SVN repositooriumisse. SMIT-i administraatorid valmistavad ette infrastruktuuri, paigaldavad ja seadistavad vajaliku kolmandate osapoolte tarkvara (andmebaas, rakendusserver, ehitusvahendid, single sign-on jne.), ehitavad SIM DHS projektist WAR arhiivi ja paigaldavad selle rakendusserverisse.

Hiljem uue versiooni korral laeb Webmedia lähtekoodi viimase versiooni SMIT-i SVN-i, SMIT-i administraatorid ehitavad uue WAR-i ja paigaldavad rakendusserverisse.

## Infrastruktuur ja serveri tarkvara

Rakendusserverisse peab olema paigaldatud:

* GlassFish v2.1+ (eelistatud) või mõni mu Java EE 5 rakendusserver
* Sun JDK 6
* Apache Ant 1.7+
* OpenOffice.org 3.1+
* ImageMagick 6.5+

Teenusena peab mõnest serverist olema kättesaadav (võib ka sama server olla):

* PostgreSQL 8.3+ andmebaas (rakendus toetab vajadusel/ettevalmistamisel ka muid andmebaasiservereid)
* CAS single sign-on teenus
* Ametnikuregister veebiteenus

GlassFish

1. Paigaldada GlassFish-i vastava versiooni kohta käiva juhendi järgi. Näiteks GlassFish 2.1 juhendid leiab siit: <http://docs.sun.com/app/docs/coll/1343.6?l=en> ja paigaldusjuhend asub siin: <http://docs.sun.com/app/docs/doc/820-4330?l=en>
2. Seadistada domeeni seadistusfailis (GLASSFISH/domains/DOMEENINIMI/config/domain.xml) Java mäluparameetrid suuremaks, nii et uued väärtused oleks:
   1. -XX:MaxPermSize=256m
   2. -Xmx768m
3. Selleks, et https ühendus rakendusserveri ja CAS serveri vahel toimiks, on vaja rakendusserveri (GlassFish) keystore-i lisada CAS serveri sertifikaat, ehk siis domains/DOMEENINIMI/config/cacerts.jks sisse on keytooliga vaja importida CAS https serveri cert.
   1. CAS https sertifikaat tuleb kõigepealt failina maha salvestada, seda saab teha näiteks brauseri abiga.
   2. Keytooli lühijuhend asub: <http://www.sslshopper.com/article-most-common-java-keytool-keystore-commands.html>

Importimiseks sobiv käsk on näiteks selline: keytool -import -trustcacerts -alias NIMI -file SERTIFIKAAT.crt -keystore cacerts.jks

1. Muid teenuseid rakendusserveris praegu seadistada vaja ei ole (näiteks andmebaasiühenduse parameetrid ja muu selline on seadistatud rakenduse enda seadistusfailis).

PostgreSQL

1. Peale andmebaasi tarkvara installeerimist tekitage login role:

CREATE ROLE alfresco LOGIN PASSWORD 'alfresco' NOSUPERUSER NOINHERIT NOCREATEDB NOCREATEROLE;

Password väärtus võib olla teistsugune, see tuleb rakenduse seadistusfailis hiljem ära määrata.

1. Ja tekitage andmebaas:

CREATE DATABASE alfresco WITH OWNER = alfresco ENCODING = 'UTF8';

## Projekti seadistus

Tõmmake SMIT SVN serverist alla lähtekood:

svn co http://SVN\_REPO\_URL\_SIMDHS simdhs

ja avage kaustas

simdhs/etc/conf/smit-test/classes/

fail

alfresco-global.properties

Vaadake üle kõik järgnevad seaded ja vajadusel tehke muudatusi (nimetatud simdhs/etc/conf/smit-test/classes/alfresco-global.properties failis on kõikide nende seadistusparameetrite kohta olemas näiteväärtused ja selgitavad kommentaarid):

* dir.root viitab kaustale kus alfresco hakkab hoidma oma sisu ja indeksite andmeid (näiteks võiks see viidata kasutaja kodukaustas olevale alf\_data alamkaustale).
* db.\* seaded viitavad PostgreSQL andmebaasiserverile ja sisaldavad õiget andmebaasi nime, kasutajanime ja parooli.
* ooo.exe viitab OpenOffice.org käivitusfailile.
* ooo.port [mittekohustuslik] viitab TCP pordile, mille peal OpenOffice.org käivitatakse ning mille peale DHS ühendub OpenOffice.org protsessiga ühenduse saamiseks; vaikimisi väärtus 8100.
* img.exe viitab ImageMagick käivitusfailile.
* mail.\* seaded viitavad ettevõtte SMTP serverile, mille kaudu saab e-maile välja saata.
* project.test seade määrab kas rakendus käitub kui testkeskkond (true) või mitte (false). Testkeskkonna seadetes kasutatakse kõikide kasutajatele väljaminevate e-kirjade jaoks ühist seadistatud aadressi, et vältida testimisse mittepuutuvate inimeste kirjadega spämmimist; samuti imporditakse rakendusse teavituste näidismallid.
* jdigidoc.test [mittekohustuslik] määrab kas JDigiDoc teek kasutab toodang- (false, vaikeväärtus) või testseadeid (true). Testseadete puhul kasutatakse OCSP kehtivuskinnitusteenust OpenXAdES serverist ning sealt saadud kehtivuskinnitustega allkirju kuvatakse kehtivana. Toodangseadete puhul kasutatakse OCSP kehtivuskinnitusteenust Sertifitseerimiskeskuse serverist ning allkirju, millel on testserverist omandatud kehtivuskinnitus, kuvatakse kehtetuna.
* cas.casServerUrl viitab CAS single sign-on serverile. Väärtus peab lõppema kaldkriipsuga, näiteks https://example.com/cas/
* external.authentication.defaultAdministratorUserNames sisaldab komaga eraldatud nimekirja kasutajatunnustest (isikukoodidest), kes sisselogimise järel rakenduse administraatori rolli külge saavad.
* amr.service.url viitab ametnikuregistri veebiteenusele.
* amr.org.id on vastava asutuse id AMR-is
* server.url viitab URL-ile, kus SIM DHS rakendus jooksma hakkab (sinna tulevad päringud CAS-ist tagasi ning seda kasutatakse väljasaadetavates e-mailides dokumendi linkides).
* serializingfilter.enabled peab toodangukeskkonnas false olema ja testkeskkonnas võiks ka false olla (arendajad kasutavad true väärtust)
* x-tee.\* seaded viitavad X-tee turvaserverile, mille kaudu DVK päringuid teostatakse.
  + x-tee.security-server - X-tee turvaserveri URL. See X-tee turvaserver peab olema liitunud soovitud X-tee keskkonnaga (toodang või test), mille kaudu on ligipääs soovitud DVK keskkonnale (toodang või test).
  + x-tee.institution – asutuse äriregistri kood, mida kasutatakse üle X-tee DVK päringute tegemisel
  + x-tee.id-code – isikukood, mida kasutatakse üle X-tee DVK päringute tegemisel
  + x-tee.receivedDocumentsFolder [mittekohustuslik] – kui on mittetühi, siis tähistab kataloogi kuhu salvestatakse kõik vastu võetavad DVK kapslid XML kujul; kasulik DVK-ga seonduvate probleemide uurimiseks.
  + x-tee.sentDocumentsFolder [mittekohustuslik] – kui on mittetühi, siis tähistab kataloogi kuhu salvestatakse kõik välja saadetavad DVK kapslid XML kujul; kasulik DVK-ga seonduvate probleemide uurimiseks.

Nii see äriregistri kood kui ka isikukood peavad olema registreeritud selles DVK keskkonnas (toodang või test), mille külge X-tee turvaserveri kaudu ühendatud ollakse – äriregistri koodi ja isikukoodi alusel lubab DVK keskkond sooritada päringuid.

* imap.\* seaded viitavad SIM DHS rakenduse sees serveeritavale IMAP teenusele.  
  IMAP teenus peab olema kättesaadav pordil 143. Kui SIM DHS rakendust jooksutada Unix'is tavakasutaja õigustes, siis pole privileege kasutada porte < 1024. Siis tuleks seada IMAP teenus töötama mõnel kõrgemal pordil, nt. 1143 ning lisada serveri tulemüüri pordi suunamine 143 -> 1143.
* passthru.\* seaded määravad NTLM „passthrough“ autentimise teenuse, mille poole SIM DHS IMAP teenus pöördub.
* email.\* seaded viitavad SIM DHS rakenduse sees serveeritavale SMTP teenusele. SMTP teenus peab olema kättesaadav pordil 25. Kui SIM DHS rakendust jooksutada Unix'is tavakasutaja õigustes, siis pole privileege kasutada porte < 1024. Siis tuleks seada SMTP teenus töötama mõnel kõrgemal pordil, nt. 1025 ning lisada serveri tulemüüri pordi suunamine 25 -> 1025. SMTP teenus on mõeldud selleks, et skanner saaks saata e-maili otse DHS rakendusse. SMTP teenus võtab vastu ainult ühele kindlale aadressile saadetud e-maile, ülejäänutest keeldub. Aadress, millele saadetud kirju vastu võetakse (näiteks [scan@dhs.example.smit](mailto:scan@dhs.example.smit)) pannakse kokku kahest osast, @-märgist vasakpoolne osa defineeritakse seadega email.to.scanned.local-part ning parempoolne osa seadega email.server.domain.
* ocr.url viitab tekstituvastuse veebiteenuse SOAP aadressile. Kui väärtus jätta tühjaks, siis rakendus ei kasuta tekstituvastuse veebiteenust.
* mso.url viitab MSO veebiteenuse SOAP aadressile. Kui väärtus jätta tühjaks, siis rakendus ei kasuta MSO veebiteenust. Kui väärtus on täidetud, siis kasutatakse DOC/DOCX/RTF 🡪 PDF teisendamiseks MSO veebiteenust; muude teisenduste jaoks kasutatakse OpenOffice teenust.

Kui seadistusfail on uuendatud, võiks selle värske seisu edastada ka Webmediale, siis saame sama seisu oma repositooriumisse panna ja hiljem on uuenduste ning muudatuste korral palju lihtsam faili õiget seisu saavutada

See seadistusfail kopeeritakse Paigaldamine peatükis GlassFish domeeni alla.

## Ehitamine

Projekti simdhs kataloogis käivitage

ant clean-all war

mis (kui ehitamine õnnestub) tekitab projekti build kataloogi simdhs.WAR arhiivi. Esimesel ehitamisel küsitakse seadistuskataloogi nime, sisestage smit-test.

## Paigaldamine

1. Seisake GlassFish rakendusserver.
2. Kontrollige, et pärast rakendusserveri seiskamise lõppemist oleks seisatud ka OpenOffice protsess (soffice), mis DHS rakenduse alt käivitatud oli. Kui OpenOffice protsess ei ole seisatud, siis peab selle seiskama (kill). Kui OpenOffice protsess ei allu seiskamisele, siis peab selle seiskama jõuga (kill -9).
3. Kui tegemist on versioonivahetusega, siis teostada andmete varundamine (vt. peatükk 8).
4. Kui tegemist on versioonivahetusega, siis paigaldatava DHS rakenduse versiooninumber peab olema sama või suurem, kui oli sama andmebaasi ja andmekausta peal varem käivitatud DHS rakenduse versiooninumber. Vastasel juhul vt. peatükk 7.1.
5. Kopeerige simdhs/etc/conf/smit-test/classes/alfresco-global.properties fail GlassFishi domeeni alla /lib/classes kausta (GLASSFISH/domains/DOMEENINIMI/lib/classes).
6. Paigaldage simdhs.war
7. Juhul, kui on palutud KUSTUTADA alfresco depositoorium, siis:
   1. kustutage maha andmebaasist „alfresco“ database
   2. looge „alfresco“ database uuesti (juhend peatükis 4, teemas PostgeSQL, punktis 2)
   3. kustutage maha peatükis 5 „dir.root“ väärtuses viidatud kataloogi sisu (näiteks kodukataloogis olev alf\_data kausta kogu sisu koos alamkataloogidega)
   4. nüüd rakendusserveri käivitamisel luuakse nullist uus repo ja indeksid.
8. Käivitage rakendusserver.
9. Kui tegemist on versioonivahetusega ja DHS rakenduse uus versioon mingi vea tõttu ei käivitu ning on vaja minna tagasi eelmisele versioonile, siis:
   1. Järgida käesoleva peatüki punkte 1-2.
   2. Taastada varukoopiast DHS rakenduse andmed, mida kasutati eelmise versiooni või sellest vanema versiooni ajal (vt. peatükk 8.3). See on vajalik, sest versiooni uuendamise käigus võidi muuta olemasolevaid andmeid ning selle tõttu ei ole vanemale versioonile tagasi minek toetatud kui andmed on uuendatud (või andmete uuendamist on alustatud).
   3. Järgida käesoleva peatüki punkte 4-8.

Märkus: Rakenduse mahukuse tõttu tekitab redeploy ilma serverit seiskamata (vana versiooni otsa deploytakse uus versioon nii et server kogu aeg töötab) üleval näidatud MaxPermSize ja heap size väärtuste korral vea OutOfMemoryError: PermGen space, mis tuleneb levinud Java EE rakenduste probleemist, kus paljud teegid jätavad undeploy järel osa ressursse PermGen mälualasse alles. Kui on soov teha jooksvaid redeploy-sid, siis tuleb MaxPermSize muuta oluliselt suuremaks (pool gigabaiti või rohkem).

### Rakenduse viimine madalamale versioonile

Kui on alustatud DHS rakenduse mingi versiooni Y käivitamist, siis sellest väiksema numbriga versiooni X enam ei tohi käivitada sama andmebaasi ja andmekausta peal. Selle kohta teeb DHS rakendus käivitumisel ka kontrolli, aga see kontroll toimub ainult juhul kui versioon Y varem käivitus edukalt. Aga kui alustati DHS rakenduse mingi versiooni Y käivitamist ja see ebaõnnestus, ning siis käivitati sellest väiksema numbriga versioon X, siis kirjeldatud kontrolli ei toimunud. Seega kuigi kirjeldatud juhul DHS rakenduse poolne kontroll puudub, siis sellest olenemata ei tohi väiksema numbriga versiooni käivitada.

Väiksema numbriga versiooni X käivitamiseks peab taastama varukoopiast DHS rakenduse andmed, mida kasutati versiooni X või sellest vanema versiooni ajal (vt. peatükk 6 punkt 10).

## Varundamine

Varukoopia tuleb teha samal ajal nii andmebaasist kui ka Alfresco andmete kaustast alf\_data (ainult teatud alamkaustad) ning neid tuleb säilitada üksteisega koos.

Vt. ka varundamise originaaljuhend:

http://wiki.alfresco.com/wiki/Backup\_and\_Restore#Backing\_up\_the\_File\_system

### Kuumvarundamine (hot backup)

Kuumvarundamist tehakse samal ajal kui DHS rakendus töötab. Kuumvarundamine peab kindlasti toimuma sellises järjestuses:

1. Alfresco teeb igal öösel kell 03:00 lucene-indexes kaustast ise koopia kausta backup-lucene-indexes, seega peab järgnevate punktide teostamine toimuma hiljem, näiteks kell 04:00.
2. Teha varukoopia andmebaasist.
3. Kui andmebaasi varundamine on lõppenud, siis teha varukoopia järgmistest alf\_data (dir.root parameetriga viidatav kaust) alamkaustadest:
   1. audit.contentstore
   2. backup-lucene-indexes
   3. contentstore
   4. contentstore.deleted

Varukoopiat ei tohi teha järgmistest alf\_data alamkaustadest:

* 1. lucene-indexes
  2. oouser

### Külmvarundamine (cold backup)

Külmvarundamist tehakse siis, kui DHS rakendus on seisatud. Külmvarundamise puhul tegevuste järjekord ei ole oluline, teostada tuleb:

1. DHS rakendus peab olema seisatud.
2. Teha varukoopia andmebaasist.
3. Teha varukoopia järgmistest data (dir.root parameetriga viidatav kaust) alamkaustadest:
   1. audit.contentstore
   2. lucene-indexes
   3. backup-lucene-indexes
   4. contentstore
   5. contentstore.deleted

Varukoopiat ei tohi teha järgmistest data alamkaustadest:

* 1. oouser

1. DHS rakenduse võib käivitada.

### Varukoopiast taastamine

1. DHS rakendus peab olema seisatud.
2. Liigutage olemasolev data kaust (dir.root parameetriga viidatav kaust) teise nimega või teise kohta.
3. Taastage varukoopiast data kausta sisu.
4. Kui tegemist oli kuumvarukoopiaga, siis nimetage backup-lucene-indexes kaust ümber lucene-indexes kaustaks. Kui tegemist oli külmvarukoopiaga, siis ei ole vaja midagi ümber nimetada.
5. Taastage varukoopiast andmebaasi sisu.
6. Käivitage DHS rakendus.

## Arendaja kontaktandmed

Kui paigaldamise või haldamise käigus tekib tehnilisi küsimusi, siis arendajaga suhtlemiseks on võimalik kasutada erinevaid kanaleid:

* Juba toimiv Skype grupivestlus „SIM DELTA“
* Projekti üldlist [simdhs@list.smit.ee](mailto:simdhs@list.smit.ee)
* Webmedia projektijuht Kaido Vaade, [kaido.vaade@webmedia.ee](mailto:kaido.vaade@webmedia.ee), +37256225599

## Muu

### WebDAV + HTTPS + Windows Vista / Windows 7

Probleem ilmneb järgmistel tingimustel:

1. kui DHS rakendust serveeritakse üle HTTPS protokolli
2. kui kasutaja arvutis on operatsioonisüsteem Windows Vista või Windows 7

Probleem ilmneb järgmisel kujul: kui DHS rakendusest avatakse MS Office fail muutmiseks, siis MS Office viskab ette kasutajanime-parooli küsimise akna.

Põhjus: Alates Windows Vistast nõuab Windowsis olev WebDAV protokolli implementatsioon, et serveri HTTPS sertifikaat oleks kasutaja arvutis usaldatud.

Lahendus 1: Signeerida DHS serveri HTTPS sertifikaat usaldatud juursertifitseerija poolt.

Lahendus 2: Paigaldada DHS serveri HTTPS sertifikaat kasutaja arvutisse. Selleks tuleb:

1. Käivita Internet Explorer administraatori õigustes (*Run as Administrator*)
2. Mine DHS rakenduse lehele, IE peaks ütlema et „*There is a problem with this website’s security certificate.*“, vajuta „*Continue to this website (not recommended).“*, aadressiriba peaks olema punane
3. Vajuta aadressiriba paremas ääres nupule „*Certificate Error“*, vajuta „*View certificates*“
4. Vajuta „*Install Certificate...“* ja „*Next >*“
5. Vali „*Place all certificates in the following store“* ja vajuta „*Browse...*“
6. Vali „*Trusted Root Certification Authorities“* ja vajuta „*OK*“
7. Vajuta „*Next >“* ja „*Finish*“
8. Küsitakse „*Do you want to install this certificate?“*, vajuta „*Yes*“, vajuta „*OK*“
9. Vajuta „*OK*“