Lietotāja instrukcija

Konfigurācija ar REST

Izmaiņas domēna autentifikācijas konfigurēšanai
Pašapkalpošanās WEB

Horizon 475.versija

Visma Enterprise
2016

SIA Visma Enterprise
Kronvalda blv. 3/5
Rīgā, LV - 1010

Tālr.: 6711 6211
Fakss.: 6711 6212
E-pasts: visma@visma.lv

Saturs

Ievads

Jaunajās izstrādēs tiek izmantoti REST lietojumi, piemēram, Darba laika uzskaite, Laikrakstis, Darbavieta.

Lai nodrošinātu vidi REST lietojumiem no Pašapkalpošanās WEB, nepieciešams veikt šajā dokumentā aprakstītās darbības.

Nepieciešams:

1) uzģenerēt sertifikātu pāri un Horizon sertifikātu glabātuvē (keystore) ieimportēt publisko sertifikātu, piešķirt piekļuves tiesības.

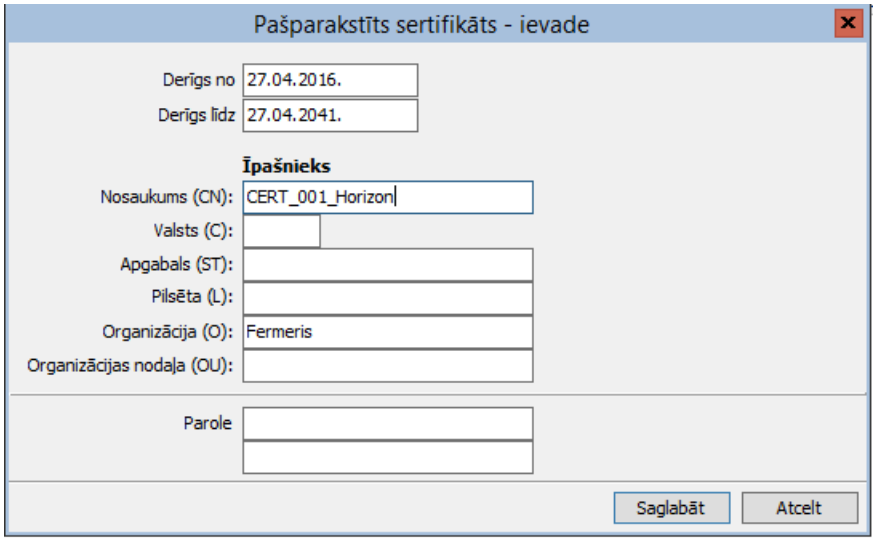
2) datoram, uz kura atrodas IIS, iekonfigurēt privāto atslēgu.

FTGserverim jābūt nokonfigurētam rest portam.
Nākamajās sadaļās pa soļiem aprakstīts risinājums, apraksts veidots izmantojot Windows Server 2012R2 standard edition, citās versijās ir iespējamas atšķirības.

Sertifikāta ģenerēšana no Horizon

Izmantojot Horizon sertifikātu glabātuvi (*Sistēma -> Administrēt -> Sertifikātu glabātuve*), jāģenerē pašparakstīts sertifikāts. To veic, nospiežot pogu **Pievienot** un no piedāvātajām darbībām izvēloties darbību **Ģenerēt pašparakstītu sertifikātu**.

Tiks piedāvāts ievadlogs sertifikāta aprakstīšanai, kā arī paroles norādīšanai. Šeit var ievadīt vērtības, kas norādītas uzņēmuma aprakstā Horizon. Ja tiek norādīta parole, tad tā jāatceras, pretējā gadījumā, nezinot paroli, nebūs iespējams sertifikātu izmantot tālāk.



Darbības rezultātā Horizon sertifikātu glabātuvē ir izveidota publiskā atslēga un sertifikātu pāris.

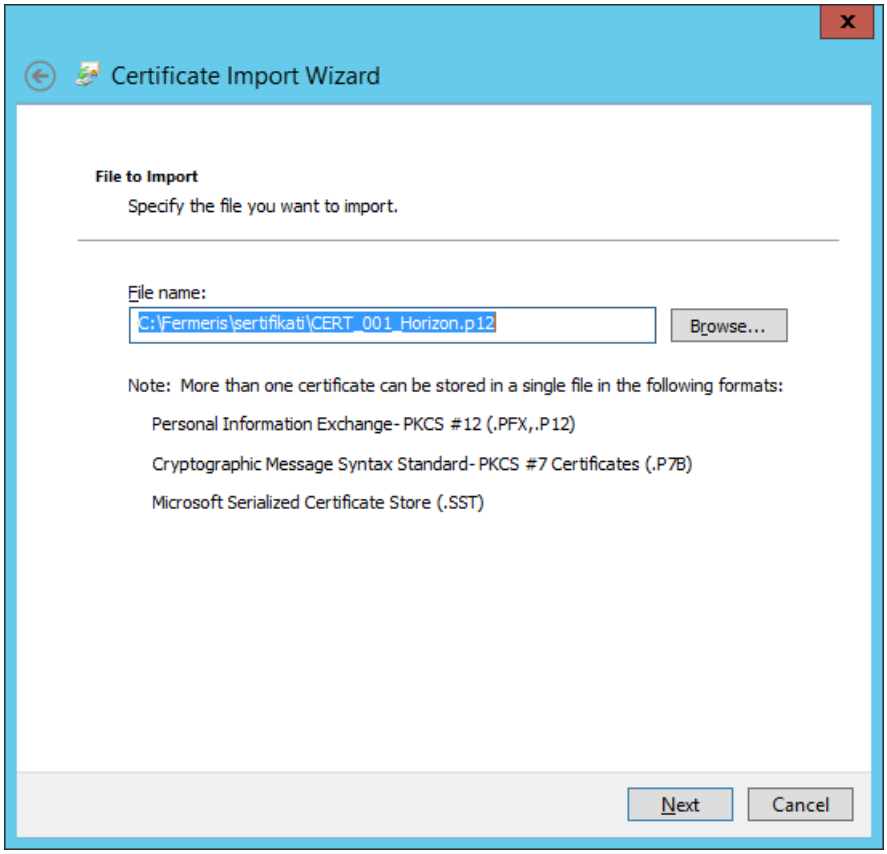
Uzģenerētā sertifikāta eksports

Izveidoto sertifikātu eksportē, izmantojot izvēlnē **Darbības** pieejamo darbību **Eksportēt sertifikāta failu**. Noklusētais eksporta formāts (.p12) ir derīgs importam Windows sertifikātu glabātuvē.

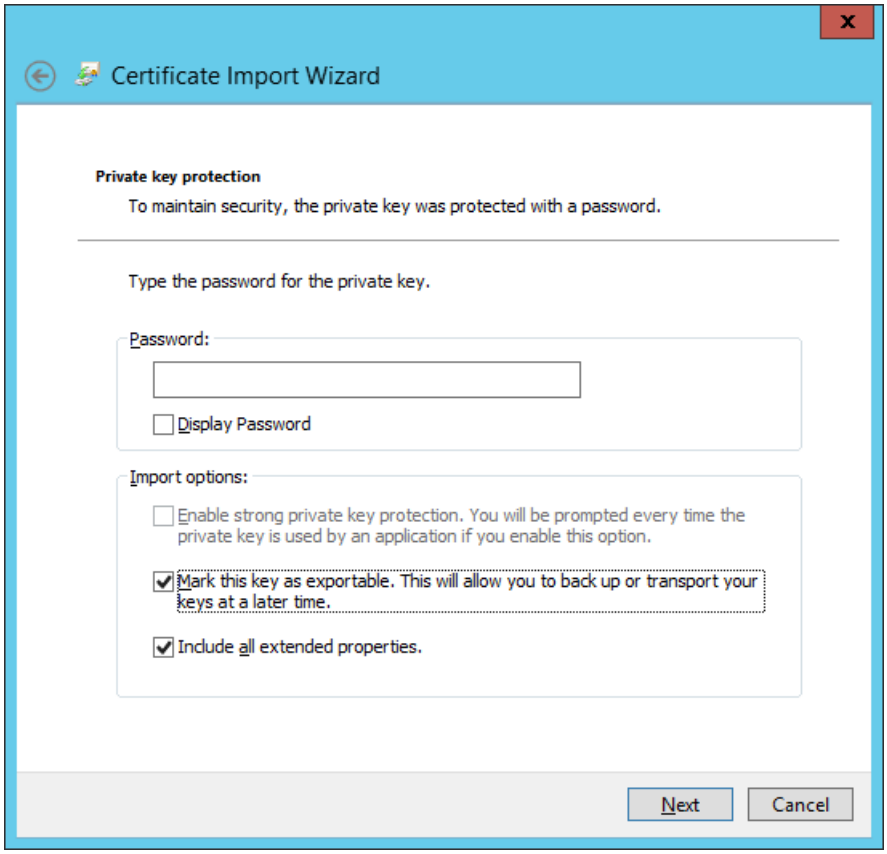
Sertifikāta imports Windows sertifikātu glabātuvē

Tālāk jāizmanto Windows standarta funkcija sertifikāta importam un jāimportē izveidotais sertifikāts Windows sertifikātu glabātuvē uz Web servera. To veic, uzklikšķinot uz eksportētā sertifikāta faila. Windows automātiski atpazīst formātu .p12 un iedarbina importa vedni. Tālāk pa soļiem jāseko importa vednim un jāspiež poga **Next**, lai pārietu uz nākamo soli.

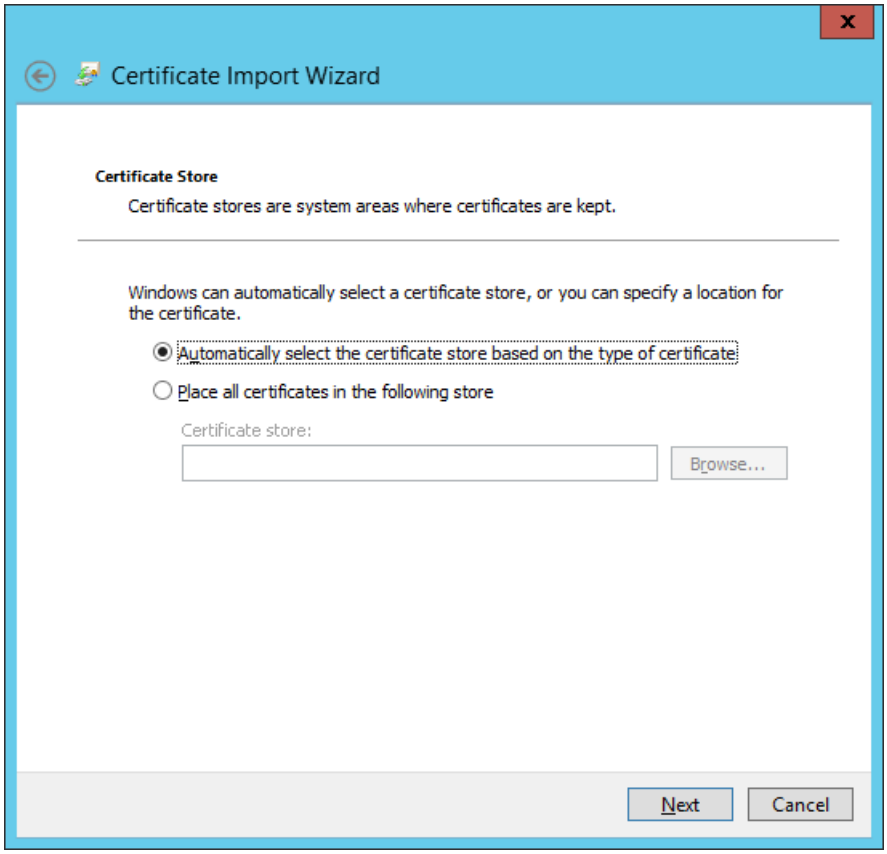
Glabātuve jāizvēlas “Local Machine”.



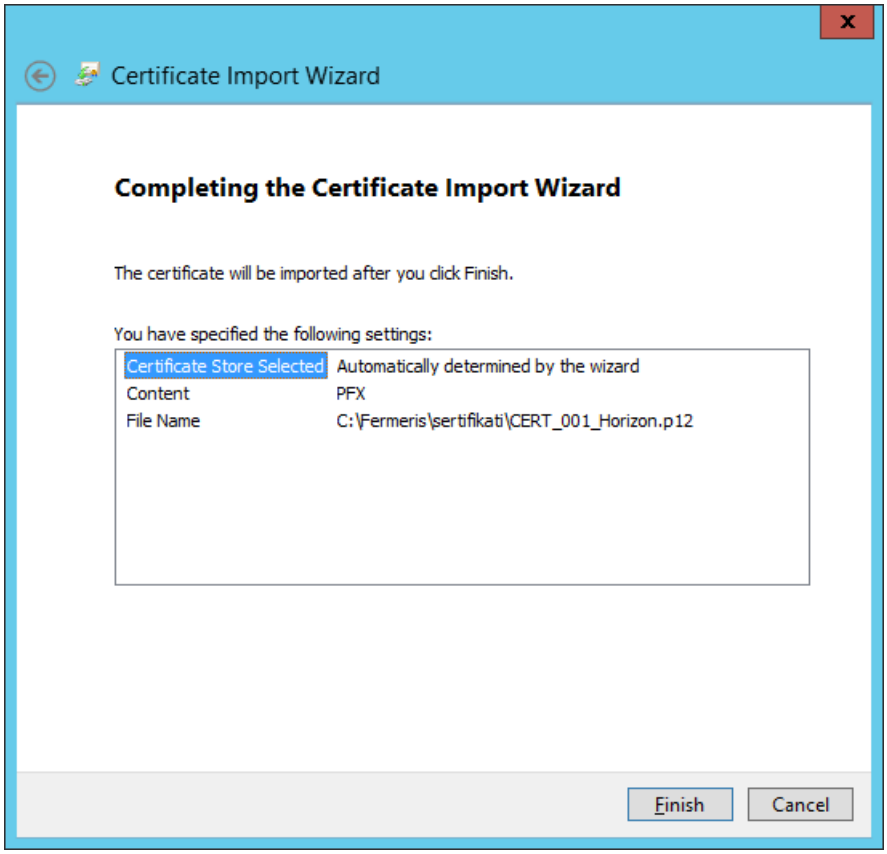
Nākamajā solī jānorāda parole, ar kuru ir aizsargāts sertifikāts. Ja sertifikāts nav aizsargāts ar paroli, tad tā nav jānorāda. Obligāti jāatzīmē opcija “Mark this key as exportable”.



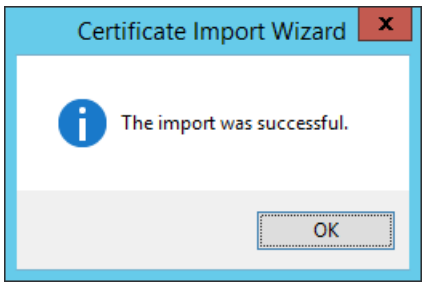
Sertifikāta faila novietošanai atstāj opciju "Automatically select the certificate store based on the type of certificate".



Nākamais solis ir fināla solis, kurā redzami norādītie uzstādījumi. Lai pabeigtu importu, jānospiež **Finish**.

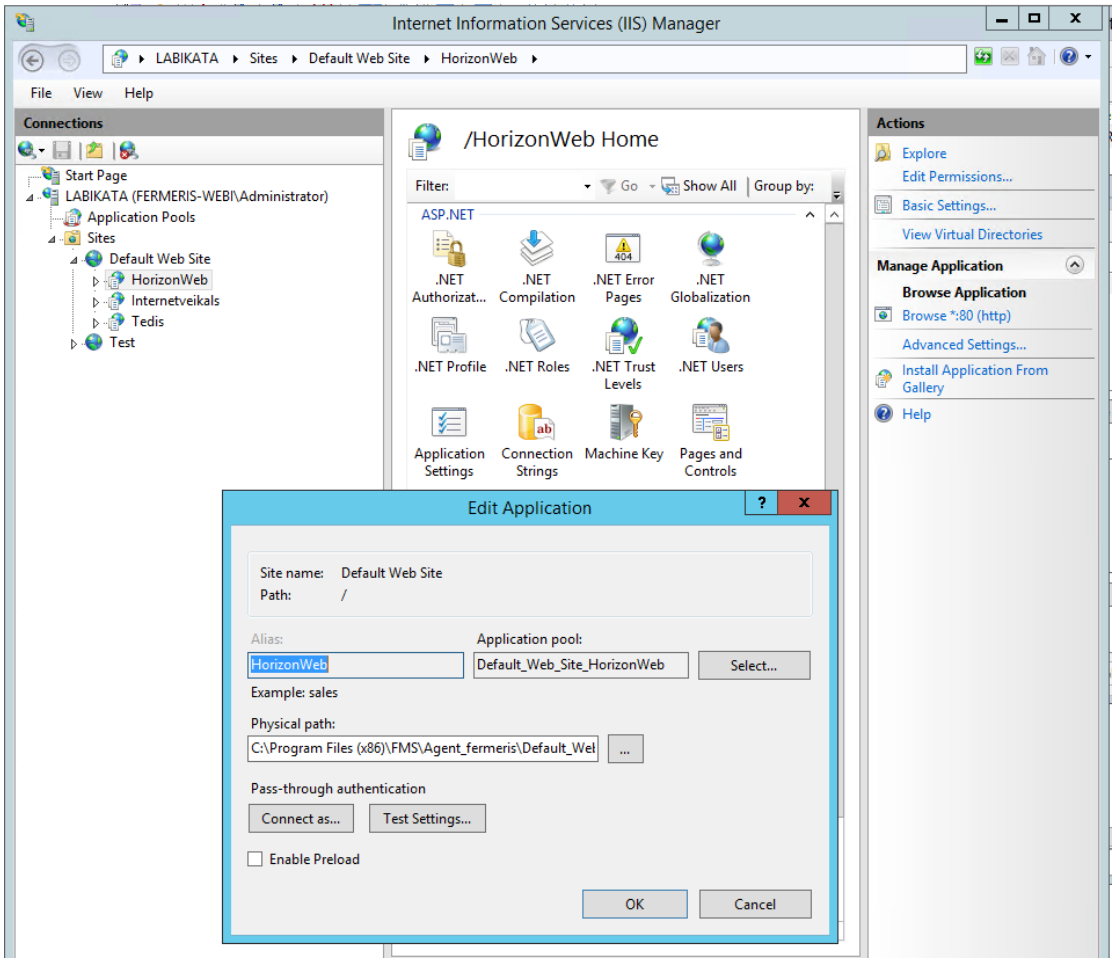


Par veiksmīgu sertifikāta importu liecina paziņojums:

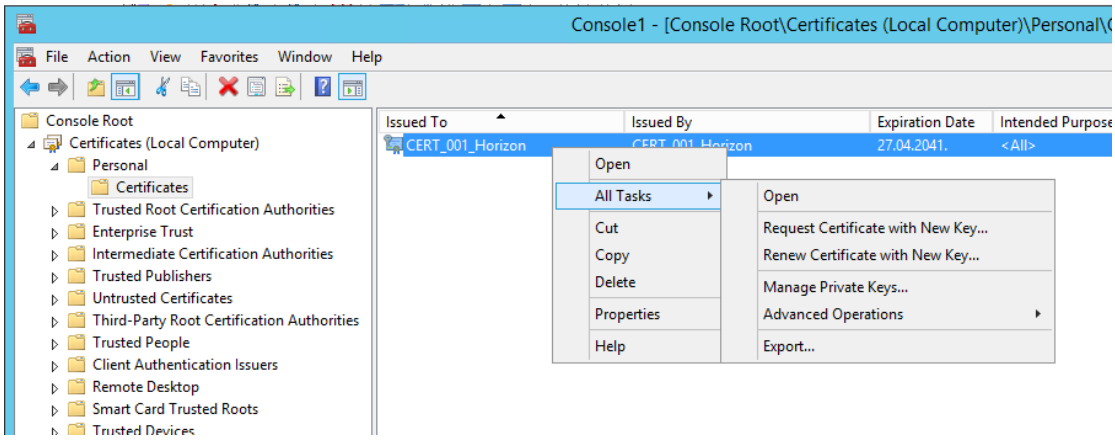


Šī procesa rezultātā ir pabeigts sertifikāta imports.

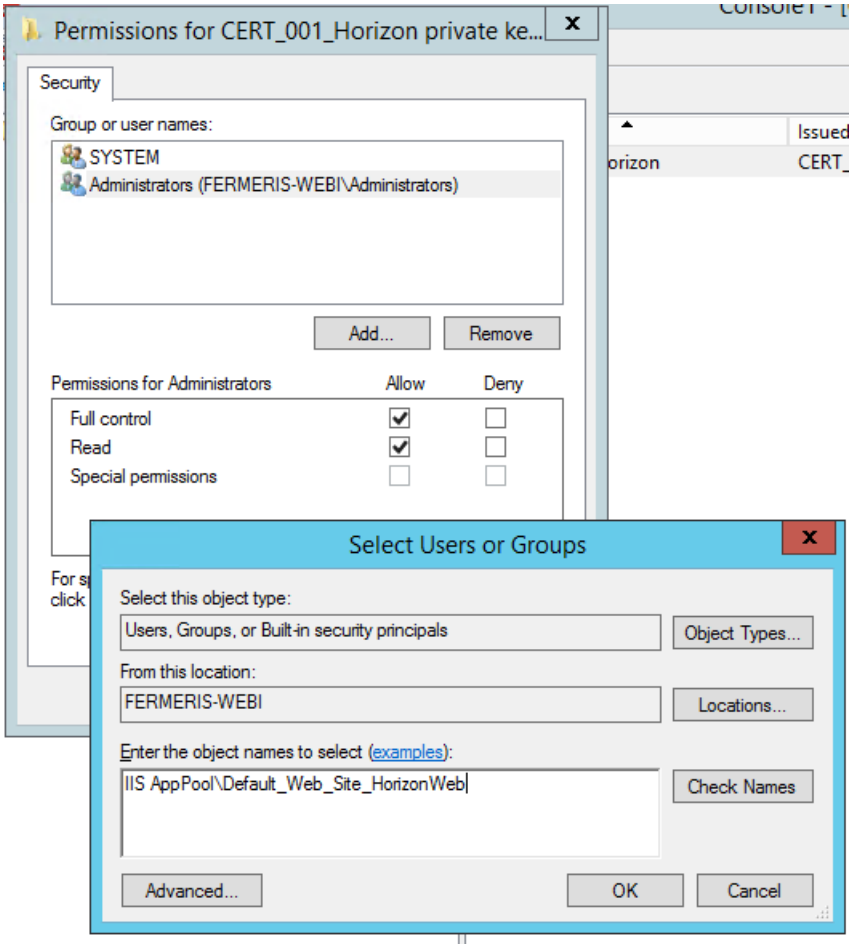
Horizon Web “Application Pool” jāpiešķir tiesības piekļūt Sertifikāta privātai atslēgai. Vispirms jānoskaidro “Application Pool” nosaukums. Lai to izdarītu, jāatver “IIS manager” un nostājoties uz Horizon web aplikācijas jānospiež “Basic settings”.



Šajā piemērā “Application Pool” nosaukums ir Default_Web_Site_HorizonWeb.
Tālāk ir jāatver sertifikātu “MMC Snap-in“ jāizvēlas “Computer account”.
Uz ieimportētā sertifikāta jāizvēlas “Manage Private Keys”.



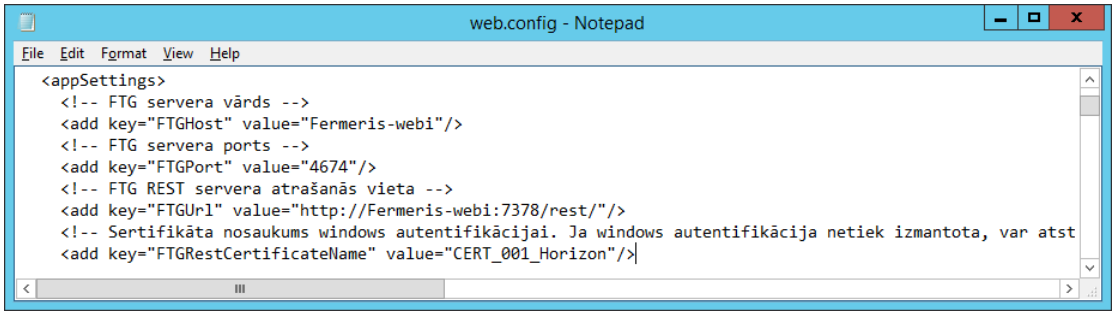
Jāpievieno iepriekš noskaidrotais “Application Pool” nosaukums papildināts ar “IIS AppPool\” – mūsu gadījumā “IIS AppPool\ Default_Web_Site_HorizonWeb”.



Pašapkalpošanās WEB konfigurēšana

Pēc tam Pašapkalpošanās WEB konfigurācijas failā web.config jānorāda, kuru sertifikātu jāpaņem no Windows sertifikātu glabātuves, lai lietotājs varētu veikt sekmīgu autorizāciju HorizonWEB, izmantojot domēna autorizācijas iespēju.

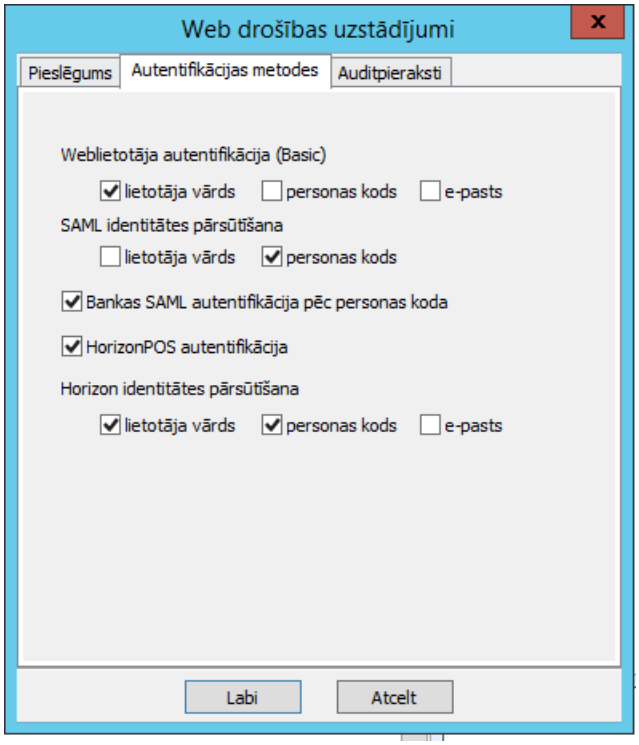
To norāda, web.config failā pievienojot vai labojot atribūtu FTGRestCertificateName un norādot kā value vērtību to, kas tika ierakstīta laukā Nosaukums (CN), sertifikātu ģenerējot.



Horizon uzstādījumi

Sistēma -> Administrēt -> Web drošības uzstādijumi.

Jābūt uzstādītai Horizon identitātes pārsūtīšanai – “lietotāja vārds”.

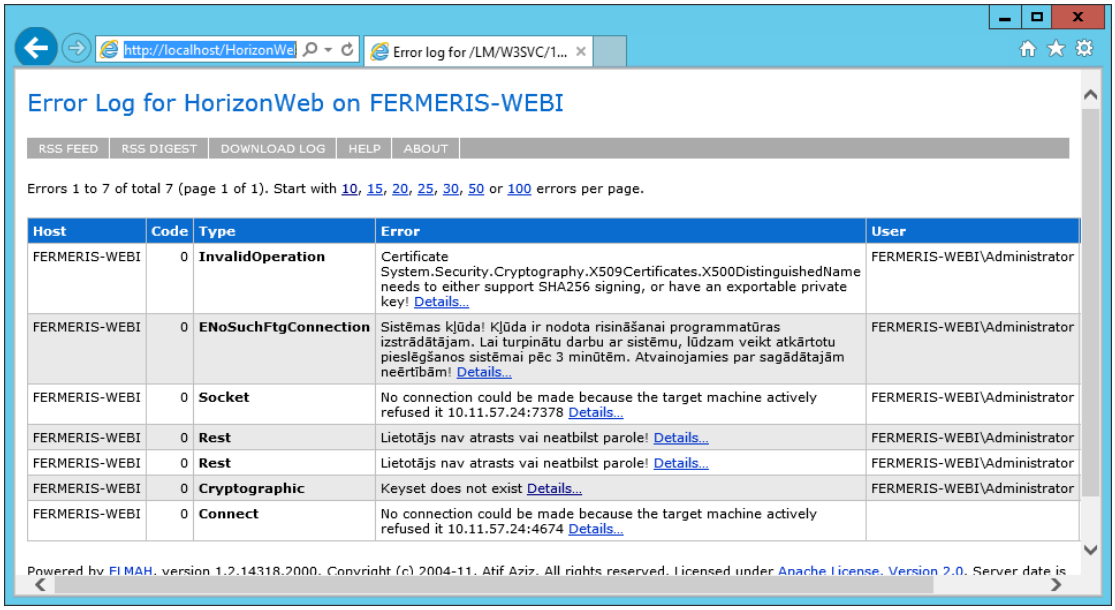


Iespējamās kļūdas

Lai pārbaudītu vai konfigurācija veikta pareizi jāatver kāds no apgabaliem, kur izmantoti REST lietojumi.

Ja tiek saņemts kļūdas paziņojums, pēc tā var identificēt iespējamo iemeslu.

Vispirms jāatver kļūdu reģistrs:
http://localhost/HorizonWeb/elmah



Kļūdu iemesli:

InvalidOperation	Certificate System.Security.Cryptography.X509Certificates.X500DistinguishedName needs to either support SHA256 signing, or have an exportable private key! Details...

Pie sertifikāta importa nav norādīta opcija “Mark this key as exportable”.

Rest	Lietotājs nav atrasts vai neatbilst parole! Details...

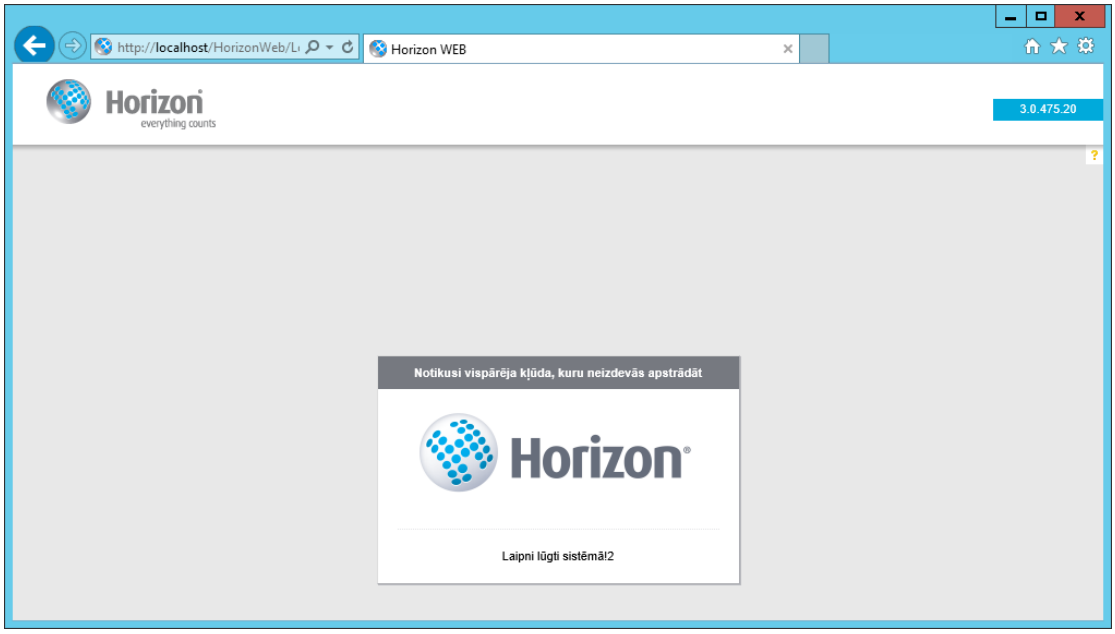
Nav uzstādīts Horizon identitātes pārsūtīšanai – “lietotāja vārds”

Cryptographic	Keyset does not exist Details...

Horizon Web “Application Pool” nav piešķirtas tiesības piekļūt Sertifikāta privātai atslēgai.

DependencyResolution	A delegate registered to create instances of 'FTGRestClient.IFtgRestConnection' returned null. Details...

Web.config failā nav norādīts rest servera interfeiss



Web.config failā norādīta nekorekta rest servera adrese, jābūt formātā http://servera vārds:ports/rest/

Izmaiņu lapa

Datums	Ver. Nr.	Izmaiņu apraksts	Autors
30.11.2014.	1.0	Izveidots jauns apraksts	A.Ozoliņa
02.05.2016	2.0	Veikti papildinājumi	I.Freimane