



Active Directory Federation Services 2.0

Panorama Partners Oy

Lari Savolainen, vanhempi konsultti

Haka- ja Virtu-käyttäjien kokoontuminen, 3.2.2010

Panorama Partners Oy

- Yritys
 - Perustettu 2003
 - 27 työntekijää
 - Sitoutumaton, vahva käytännön kokemus useista hankkeista sekä tärkeimmistä IdM-teknologioista
- Liiketoiminta-alueena käyttäjähallinnan (IAM/IdM) asiantuntijapalvelut
 - Hanketta valmistelevat asiantuntijapalvelut (konsultointipalvelut)
 - Hankkeen aikaiset asiantuntijapalvelut (konsultointipalvelut, järjestelmätoimitukset)
 - Hankkeen jälkeiset asiantuntijapalvelut (ylläpitopalvelut, integraatiopalvelut, konsultointipalvelut)
 - Hanke- ja projektipalvelut
- Kokemusta yli 30 eri asiakkaan IAM/IdM –hankkeista ja eri teknologioista
 - Mm. Aluehallinnon uudistamishanke (ALKU), Arek, Helsingin ja Uudenmaan sairaanhoitopiiri (HUS), Pohjois-Pohjanmaan sairaanhoitopiiri (PPSHP), ePOHJOIS-SUOMI (ePS), Suomen Asiakastieto, Tapiola-ryhmä, Tiehallinto / Liikennevirasto, Vaisala, VR-konserni, Wärtsilä jne.
 - Mm. BMC, IBM, Microsoft, Novell, Oracle, Passlogix, RM5, SAP
- Kumppaneina
 - Integraattorit sekä johtavat IAM/IdM –teknologiayritykset
 - Valtionhallinnon puitesopimustoimittaja (Hansel) kumppaniemme Netum Oy:n, HM&V Research Oy/ HMV PublicPartnerin kautta

Teknologian / ratkaisun valintakriteerejä

Hyväkin tuote voi osoittautua vääräksi ratkaisuksi – Halpa taas kalliiksi
Kokonaisuus ratkaisee!

- Tarve
- Oma osaaminen
- Sopimukset
- Olemassa olevat lisenssit
- Kumppanuudet
- Palvelun kriittisyys



- Budjetti
- Tulevaisuuden suunnitelmat
- Käyttäjämäärät
- Nykyinen infra
- Tehdyt päätökset
- Aikataulu

Microsoft Active Directory Federation Services 2.0

AD FS 2 on yksi Windows-palvelimen palveluista samoin kuin AD-hakemistopalvelu, WWW-palvelu, levypalvelut tai tulostinpalvelu

Ominaisuuksia

- SAML 2.0 tuki
- Vikasietoisuus
- Federoitu SharePoint-kirjautuminen

Lisensointi

- Kuuluu Windows Server peruspalveluihin
 - > Ei erillistä lisenssiä
- SQL Server lisenssi isompiin ympäristöihin

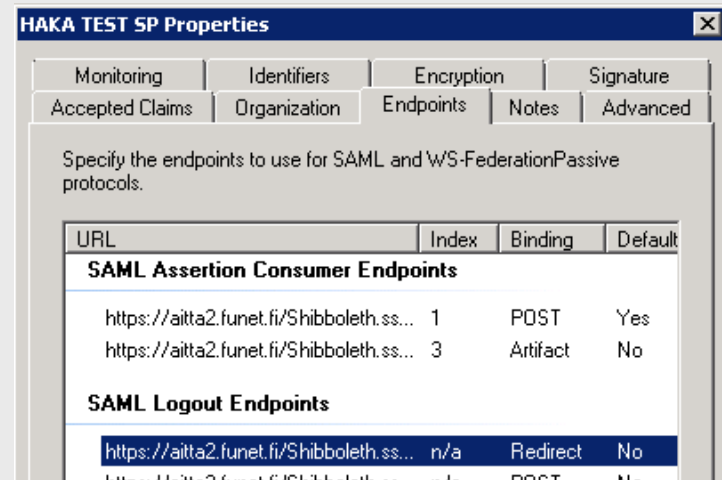
Julkaisuajankohta H1/2010

Kokemuksia

Panorama testasi AD FS 2.0 Beta 1 versiota ensimmäisen kerran keväällä 2009 CSC:n Haka-testiverkkoa vasten

AD FS -asennus tehty helpoksi

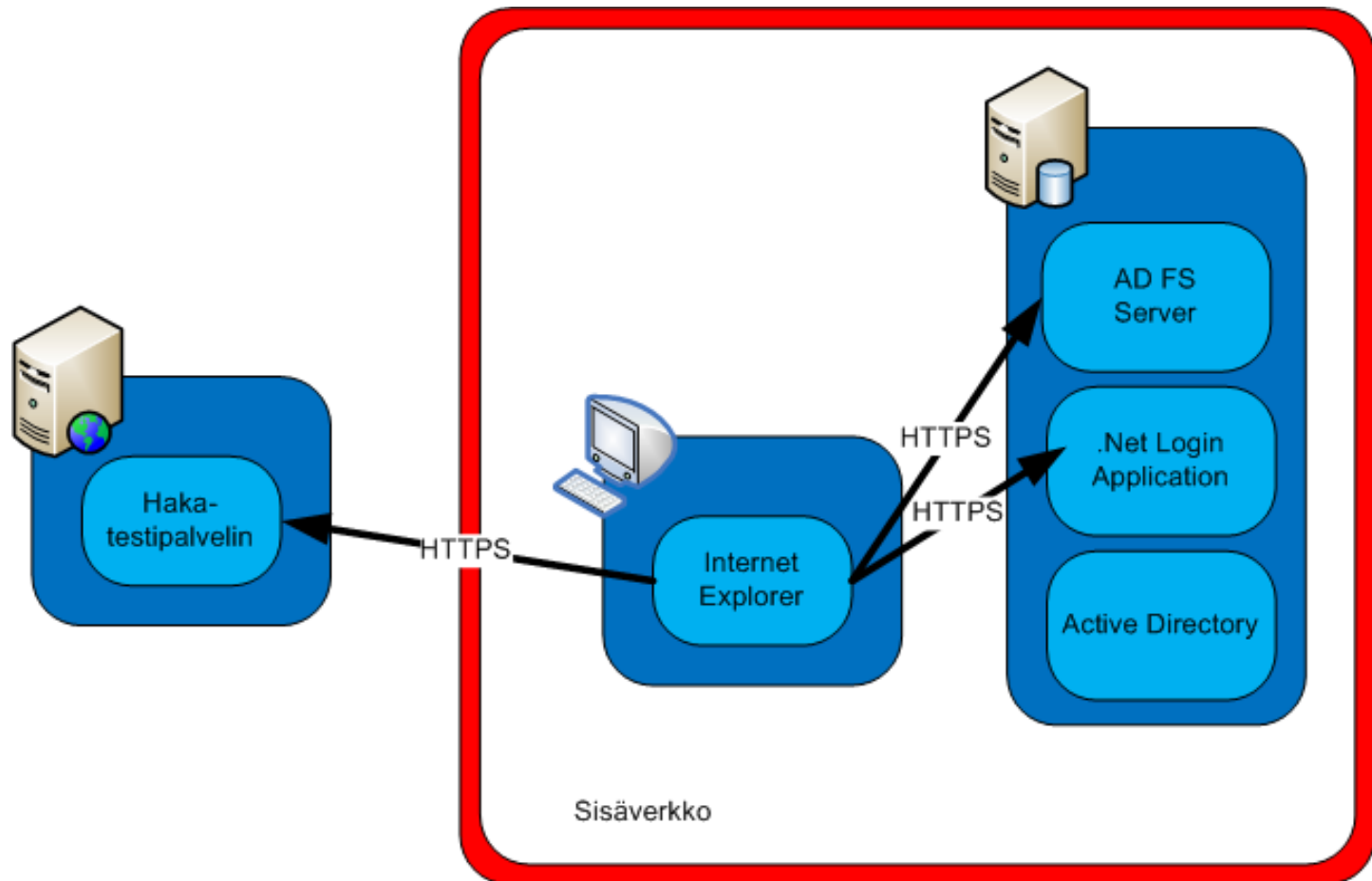
- Haka-testipalvelimen määrittely onnistui AD FS:ssa ohjatun toiminnon avulla



AD FS IdP:n liittäminen Haka-luottamusverkostoon

- Samoin kuin Shibbolethilla
- Luottamusverkon ylläpitäjille ilmoitettiin palvelimen nimi, käytetyt varmenteet, osoitteet yms.

Testiympäristö



Huomioita

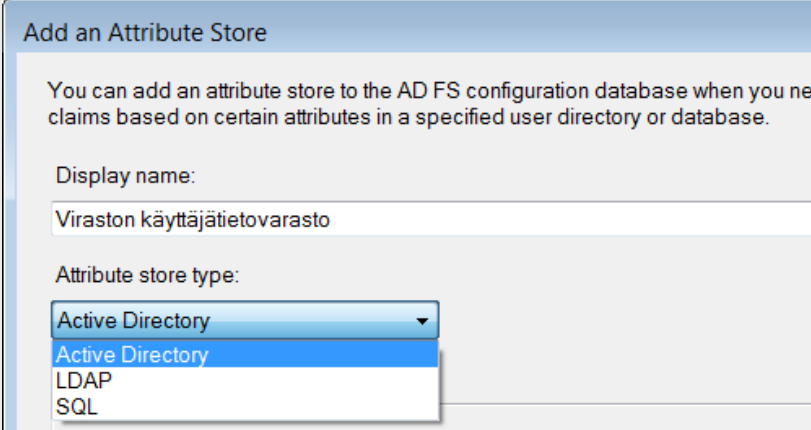
Asetusten määrittely tapahtuu valikoiden kautta. Hallintaan voidaan käyttää myös PowerShell-komentoja.

Lähetettävät tiedot

- Oletuksena lähteenä Active Directory
- Myös LDAP ja SQL
- Tiedot voidaan koostaa useasta lähteestä

Käyttäjän tunnistaminen

- Web-sivu, jolla kysytään tunnus ja salasana
- Kertakirjautuminen (SSO) työasemaan kirjautuneen käyttäjän tiedoilla
- Muita vaihtoehtoja esimerkiksi Kerberos tai SAML IdP



Add an Attribute Store

You can add an attribute store to the AD FS configuration database when you need claims based on certain attributes in a specified user directory or database.

Display name:
Viraston käyttäjätietovarasto

Attribute store type:
Active Directory
Active Directory
LDAP
SQL

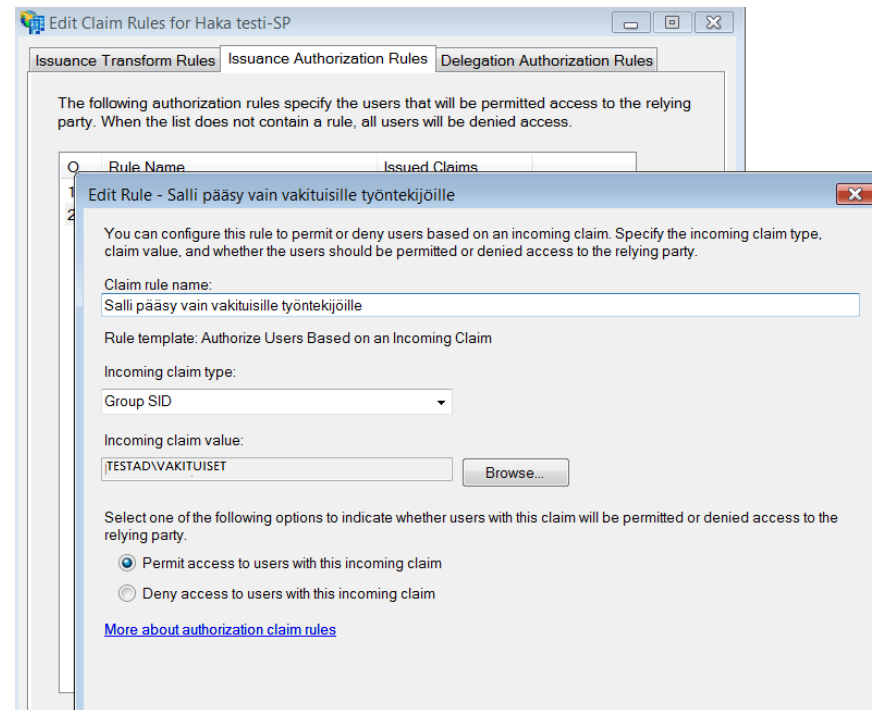
Kokemuksia

Entä, jos omassa AD:ssa on myös muita kuin organisaation omia käyttäjätunnuksia?

Pääsyn rajaaminen Haka / Virtu verkkoon omasta AD:sta

- Onnistuu helposti mm. AD-ryhmien tai attribuuttien perusteella

- Monimutkaisempien sääntöjen rakentamiseen *Claim rule language*



Laajennettavuus

Jos tunnistuspalvelu ei toimi,
silloin eivät toimi sen takana olevat sovelluksetkaan.

AD FS Proxy Server

- Tietoturvan parantamiseksi verkon rajalle voidaan asentaa Proxy-palvelin
- Välittää viestit sisäverkossa sijaitsevalle AD FS –palvelimelle

AD FS –palvelinfarmi

- Skaalautuvuus tuotteen tasolla
- Vikasietoisuuden ja suorituskyvyn parantaminen palvelinten määrää kasvattamalla

Summa summarum

Yleisesti ottaen AD FS täyttää Virtu tai Haka luottamusverkoston vaatimukset. Kokonaisuus ratkaisee onko Active Directory Federation Services oikea työkalu.

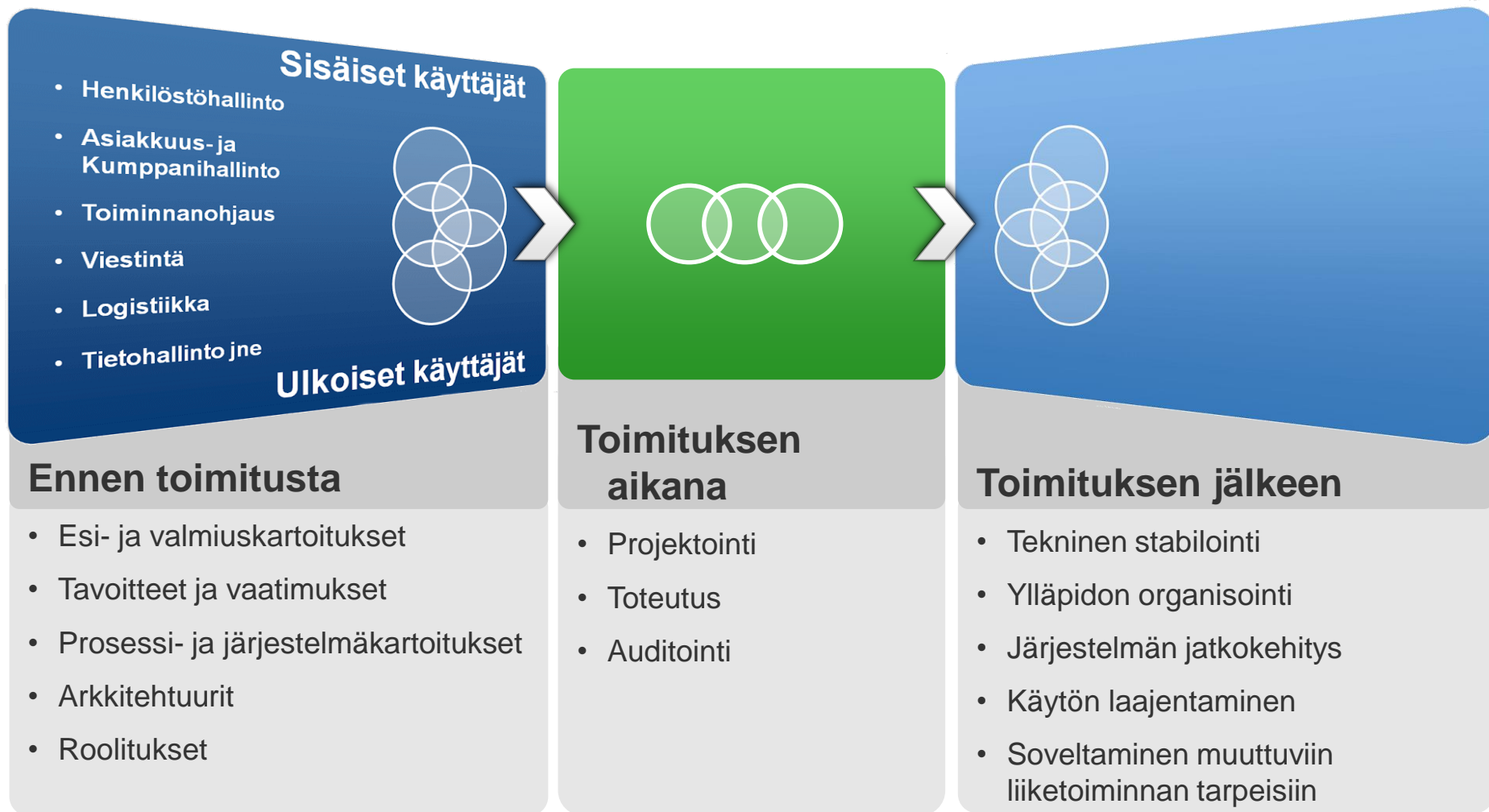
Puolesta

- Organisaatiossa on jo Microsoft-osaamista ja -infrastruktuuria
- Windows Server -lisensoijia käytettävissä
- Organisaatiossa ei aiempaa panostusta AM-tuotteisiin
- Käyttäjätiedot ovat AD:ssa ajan tasalla
- Käytössä on SharePoint-sivustoja
- MS-koulutusta ja koulutettuja osaajia löytyy markkinoilta

Vastaan

- Käytössä on jo jokin SAML 2.0 Access Management -tuote
- Vahvempi Open Source kuin Microsoft osaaminen

Panorama Partnersin palvelut IAM/IdM –hankkeen eri vaiheissa



Lisätietoja

Kysyvä ei tieltä eksy!

Microsoftin AD FS -sivuilta

- <http://www.microsoft.com/windowsserver2008/en/us/ad-fs.aspx>

Panorama Partnersilta

- <http://www.panoramapartners.fi>



Kiitos!

Lari Savolainen

lari.savolainen@panoramapartners.fi