SWAMID

Swedish Academic Identity Federation

Uppgradering till Shibboleth IdP v5

SWAMID

Shibboleth IdPv4 End-of-Life

- Shibboleth IdPv4 får ingen support eller säkerhetsuppdateringar från och med 1 september 2024
- SWAMIDs teknologiprofil för SAML punkt 5.4.11 definierar att endast supporterad programvara får användas
- Kvarvarande osupporterade Shibboleth IdP kommer att avregistreras från SWAMID 1 december 2024

SWAMID

Uppgradera, inte nyinstallera!

- Rekommenderat
  - Uppgradera befintligt IdPv4 till IdPv5
  - Inget byte av certifikat, entityID, metadata osv

- Inte rekommenderat
  - Nyinstallation
    - Shibboleth Consortium beskriver i release-notes för IdPv5 att befintliga konfigurationsfiler bara kan användas om uppgraderingen görs i befintlig installation. Installern för IdPv5 installerar systemet på ett sätt som gör att man inte kan kopiera konfigurationsfiler från ett v4 system till en nyinstallerat v5 system. Det kommer INTE att fungera.
    - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199500367/ReleaseNotes

SWAMID

Arbetsgång

- Installera en ny server
- Kopiera Shibboleth IdP från befintligt produktionsserver till den nya servern
- Gör all städ/uppgraderingsarbete på den nya server i lugn och ro
- Testa utan att påverka
  - Du kan peka din IdPs hostname/alias till den nya servern genom att lägga in en override i din lokala hosts fil

SWAMID

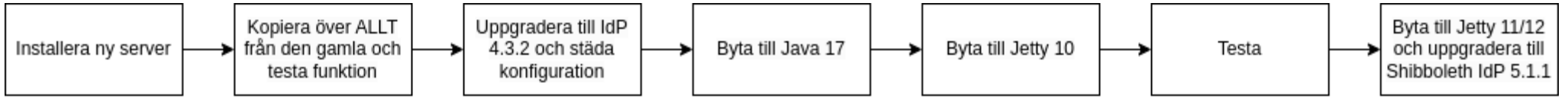
Arbetsgång

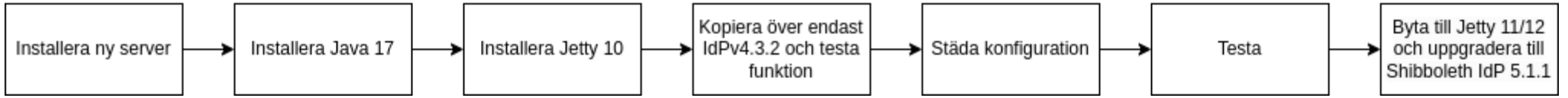
- Om man ha en testserver, uppgradera den först innan man jobba med produktion
  - testservrar ska migreras från SWAMID-Testing till SWAMIDs QA-federation
  - mer information:
    - https://wiki.sunet.se/display/SWAMID/QA+for+SWAMID+SAML+WebSSO
    - https://wiki.sunet.se/pages/viewpage.action?pageId=166330502
  - SWAMID avråder kraftigt från att system med riktiga personuppgifter och applikationsdata registreras i QA-miljön.
    - Rekommendation: installera en LDAP server lokalt på test-IdPn och lägg in testdata

SWAMID

Arbetsgång

- Finns olika sätt att jobba och ni måste välja det som passar er situation





SWAMID

Förberedelser innan uppgradering

- Uppgradera till senast v4 release (2024-04-01: 4.3.2)
- Se till att alla deprecation (förutom SAML2NameID) varningar är borttagen från loggarna!
- Rekommenderat att städa systemet
  - stänga av oanvända moduler
  - konfigurationsändringar (t.ex. xml till properties)
  - https://shibboleth.atlassian.net/wiki/spaces/KB/pages/1469908146/Example+4.1+Upgrade
- Ändringar som SWAMID rekommenderar

SWAMID

Kontrollera SecretKeyManagement

- Kontrollera funktionen av IdP-installer's dailytasks.sh (körs nog från roots crontab)
  - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199501624/SecretKeyManagement
  - Lätt att glömma, den bara rullar på men den är en viktig komponent!
  - Se till att funktionen migreras till den nya servern!
  - Finns nog motsvarig konfiguration under Windows.

SWAMID

Sessioner server-side till local storage?

- Tidigare standardkonfiguration var en databas för server-side storage av sessioner
  - data lagras i storageservice.StorageRecords
- Överväga att flytta till klienten med HTML local storage
  - Möjligheten att kunna ta bort databas helt längre fram
  - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199509576/StorageConfiguration
- Om du bestämma att inte byta till HTML local storage kan collate i StorageRecords tabellen behöva bytas till utf8_bin för att hantera case-sensitivity i flera kolumner

SWAMID

Migrera från JPAStorageService

- Även om man migrera till HTML local storage används en storage service fortfarande för ePTID
  - ePTID data lagras i shibboleth.shibpid
- Migrera till JDBCStorageService
  - https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/2989096970/JDBCStorageService
- Uppdatera HikariCP och mysql-connector till senaste versioner

SWAMID

Städa metadata

- SWAMID rekommendera att ta bort stöd för SAML1
- Ta bort SAML1 saker från metadata
  - ArtifactResolutionService urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding
  - SingleSignOnService urn:mace:shibboleth:1.0:profiles:AuthnRequest
- Justera relying-party.xml:
  - Bean parent Shibboleth.SSO samt beans för SAML 1.1 kan disablas helt
  - Bean SAML2.AttributeQuery kan disablas (SAML 2 Attribute Query over SOAP)

SWAMID

Java 17 och Jetty 10

- Byta till Java 17
  - Installera Nashorn scripting engine
  - https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/1374027996/Nashorn
- Byta till Jetty 10
  - Jetty-base måste göras om
  - Vi rekommenderar att ta bort Backchannel stöd (mer info i nästa bild)
  - https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/2936012848/Jetty10

Ta bort Backchannel

- Backchannel är en kvarleva från SAML 1, rekommendationen är att ta bort den
  - i den nya jetty-base kan man bortse i från att konfigurera jetty-base/start.d/idp-backchannel.ini
  - flytta undan den gamla keystore filen idp-backchannel.p12
  - städa bort backchannel certifikatet ur metadata/idp-metadata.xml
  - stänga port 8443 i brandväggar/filtrar
- Det är inte möjligt att konfigurera Backchannel som en sekundär TLS-port under Jetty 12.

SWAMID

Uppgradera IdPn

- Uppgradera Jetty från 10 till 11 eller 12
  - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199500883/Jetty11
  - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3516104706/Jetty12
  - Jetty 12 utreds fortfarande av Shibboleth projektet och kan vara den rekommenderad versionen beroende på när i tid ni kommer till denna fas i uppgraderingsarbetet. Vi bevakar detta och återkommer under våren.
  - https://endoflife.date/eclipse-jetty
- Uppgradera IdPn
  - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199500925/Upgrading

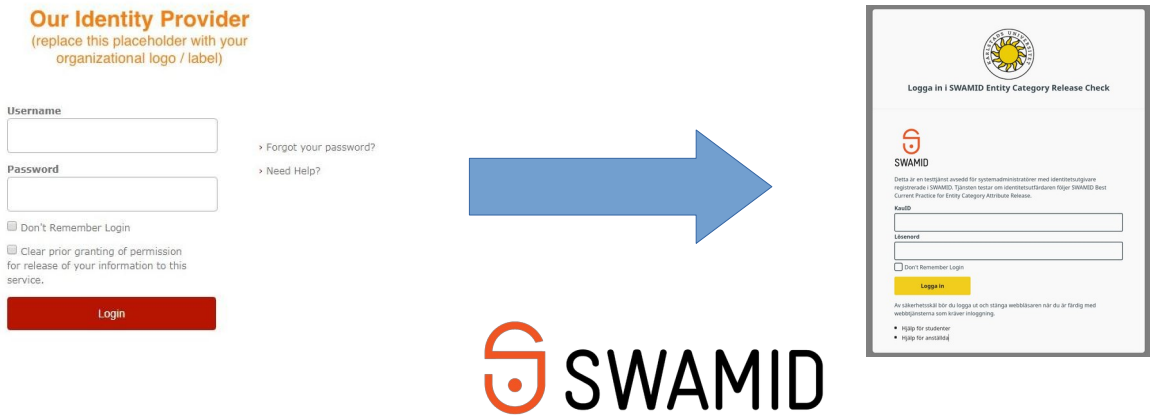
SWAMID

Kontrollera idpnew.5XX filer

- Uppgraderingsprocessen skapar nya versioner av properties och xml filer under conf/
- Dessa filer bör jämföras med de aktuella filer och ändringar kopieras över

Views

- Sedan v4.2 har Shibboleth en uppdaterad UX design
  - mer modern och tillgänglighetsanpassad
- Version 5.1 innehåller förbättrad CSP (Content Security Policy) stöd
- Om man kör views < v4.2 bör man överväga en fullständig refresh
- Om man kör views >= v4.2 bör man kontrollera ändring i idpnew.5XX filerna



Efter driftsättning

- Kom ihåg att uppdatera metadata i SWAMID efter driftsättning
  - för att ta bort SAML 1
  - för att ta bort Backchannel-certifikat

SWAMID

Testa och få hjälp

- Öppna diskussionsmöten våren 2024 - Frågor som dyker upp under uppgraderingsarbetet till Shibboleth IdPv5
  - Som uppföljning bjuder SWAMID Operations till ett antal öppna möten där det är möjligt att få hjälp av SWAMID Operations och andra som genomför uppgraderingen.
  - 9.00 – 10.00 torsdagarna den 18 april, 2 maj, 16 maj, 30 maj och 13 juni
  - Mer info https://wiki.sunet.se/pages/viewpage.action?pageId=185139336

SWAMID

Frågor?

SWAMID