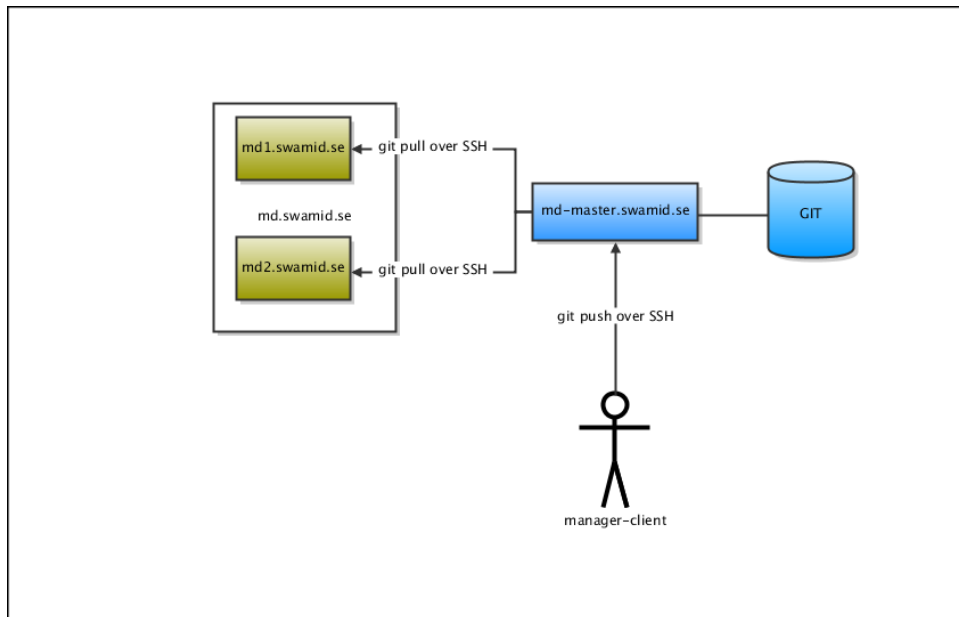


Underhåll och publicering av metadata

Inledning

I en SAML-federation är metadata av central betydelse för säkerheten och tilliten till federationen. SWAMID är en sk *full mesh* federation vilket betyder att SP:er och IdP:er pratar direkt med varandra och inte (som i sk *hub and spoke*-federationer) går igenom en central integrationspunkt. Ett exempel på en sådan federation är Danska [WAYF.dk](http://wayf.dk). I en full mesh-federation använder SP:er och IdP:er innehållet i metadata för att hitta varandra och hitta nycklar som används för att etablera säkra förbindelser, signera meddelande mm.



Distribution av metadata

SWAMID distribuerar metadata från URL:en <http://md.swamid.se/md/>. Denna URL innehåller ett antal metadata-filer som används för olika syften.

Tjänsten md.swamid.se körs på två olika servrar: md1.swamid.se och md2.swamid.se. Dessa servrar körs i två olika vmware-kluster i två av NORDUnet datacenter. Servrarna kör VRRP för IP-adressen md.swamid.se som alltså flyttar mellan servrarna för att åstadkomma en tjänst med hög tillgänglighet. Servrarna kör Ubuntu med Apache som webserver.

Tidigare har metadata distribuerats från <http://wayf.swamid.se/md>. Trafik till denna trafik vidarebefodras från Discovery-tjänsterna via en HTTP-proxy till md.swamid.se. Discovery-tjänsterna är uppbyggda med samma typ av redundans vilket betyder att både wayf.swamid.se/md och md.swamid.se/md är tillgängligt med samma nivå av säkerhet.

Underhåll av metadata

Metadata för SWAMID underhålls i ett GIT-repository som är tillgängligt via gitweb på <http://md-master.swamid.se/> för de som vill följa förändringar i metadata. Innehållet i detta repository signeras var 5:e minut och exporteras till publicerings-servrarna (md1 och md2).

Mjukvara

Vi använder följande mjukvara för att underhålla metadata:

- GIT (gits och gitweb) för lagring och versionering av metadata.
- Apache för publicering av metadata
- [saml-md-tools](#) för underhåll av saml-metadata.