UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Programa de Apoyo al Egreso de Profesionales en Actividad

TÍTULO: Gestión de identidades y accesos unificados

AUTOR: Federico Sebastian Castro

DIRECTOR ACADÉMICO: Dra. Lía Molinari

DIRECTOR PROFESIONAL: Guillermo Rocca

CARRERA: Licenciatura en Sistemas

Resumen

La gestión de identidades y control de acceso es una solución informática que permite realizar la gestión del ciclo de vida de las identidades digitales y controlar el acceso a los diferentes recursos informáticos, con el objetivo de mitigar riesgos, reducir costos y permitir que el proceso de gestión de identidades y accesos evolucione de manera segura y flexible.
Motiva el desarrollo de la presente tesina el análisis e implementación de un sistema de este tipo, debido a que, gracias a una eficiente gestión de las identidades y accesos, se espera obtener un mayor control sobre los activos de información, generando a través de esto una gestión transparente y eficaz en el manejo de recursos informáticos.

Palabras Clave

Autenticación, autorización, control de acceso, seguridad informática, permisos, sistemas de gestión de identidades, IAM.

Conclusiones

La implementación de este tipo de soluciones permite una mejora sustancial en la gestión de accesos a los sistemas informáticos y en los repositorios de información digital que se administra; a su vez que se logra asegurar un manejo transparente, seguro, auditable y eficaz del ciclo de vida de la identidad de los usuarios. La correcta gestión del ciclo de vida de la identidad de usuario y sus accesos genera un impacto positivo en la disminución de costos administrativos, reduciendo la complejidad y el tiempo requerido en la administración de cuentas de usuarios, maximizando la continuidad y productividad operativa del organismo donde se implemente.

Trabajos Realizados

Investigación sobre los sistemas de gestión y control de accesos, características y funcionamiento general.
Descripción de los componentes principales que forman parte del sistema de gestión elegido para la realización de esta tesina e implementación de dicho sistema, detallando instalación y configuración de los diferentes productos.
Descripción de las tareas realizadas en la integración de los diversos sistemas y aplicaciones informáticas existentes con la nueva implementación de gestión de identidades y accesos.

Trabajos Futuros

Extensión del sistema de gestión de identidades y control de accesos, implementando una solución que abarque no solamente los sistemas web a proteger, sino también los usuarios y accesos a los sistemas operativos de los servidores más críticos de un organismo.

Fecha de la presentación: Marzo 2020

Índice General

1.Introducción 1
1.1. Motivación 1
1.2. Objetivo 2
1.3. Estructura organizativa del trabajo 3
2. Identidades 5
2.1. ¿Qué es identidad? 5
2.2. Identidad digital 5
2.3. Propiedades de la identidad 5
2.4. Ciclo de vida de la identidad 6
3. Gestión de identidades y control de accesos..... 9
3.1. Características principales 9
3.2. Componentes 11
4. Solución Identity Manager a implementar 17
4.1. NetIQ Identity Manager IDM 17
4.2. Funciones principales 17
4.3. Arquitectura de NetIQ IDM 21
4.3.1. Arquitectura lógica 21
4.3.2. Arquitectura física 26
5. Implementación de Identity Manager..... 29
5.1. Tareas de Implementación realizadas 29
5.2. Proceso de instalación y configuración 30
5.3. Identity Applications 36
5.3.1. Identity Manager Dashboard 36
5.3.2. Identity Applications Administration - iManager 38
5.4. Integraciones 40
5.4.1. Conector de Integración con Plataforma de RRHH 42
5.4.2. Conector de Plataforma Active Directory 50
6. Solución Access Manager a implementar 59
6.1. NetIQ Access Manager AM 59

6.2. Características principales 59
6.3. Componentes y sus características 61
6.3.1. Consola de administración 62
6.3.2. Identity Server 63
6.3.3. Access Gateway..... 64
6.4. Arquitectura física..... 65
6.5. Funcionamiento Access Manager 66
7. Implementación de la solución Access Manager 69
7. 1. Proceso de Instalación y de Configuración..... 69
7.1.1. Instalación del Administration Console y el Identity Server Provider 70
7.1.2. Instalación de Access Gateway Appliance 70
7.2. Configuración de Access Manager 72
7.2.1. Configuración del componente Identity Server 73
7.2.2. Repositorio de usuario 74
7.2.3. Configuración del componente Access Gateway 76
7.3. Integración con las aplicaciones 77
7.3.1. Integración por proxy reverso 77
7.3.2. Integración por federación OAuth 81
7.4. Asegurando la comunicación de los componentes con certificados..... 84
8. Eventos de Seguridad 87
8.1. Instalación del SIEM y configuración de colectores de logs 87
9. Conclusiones y trabajos futuros 91
9.1. Conclusiones 91
9.2. Trabajos futuros 91
Anexo Diseño físico de la implementación 93
Referencias bibliográficas..... 95

Índice de figuras

2.1. Ciclo de vida de la Identidad 7
3.1. Topología de un Metadirectorio 12
4.1. Sincronización de Identity Manager y sistemas conectados 18
4.2. Ejemplo de integración entre sistemas con Identity Manager 18
4.3. Sincronización de passwords 19
4.4. Workflow de aprobación 20
4.5. Gestión de Roles 21
4.6. Arquitectura Lógica de NetIQ IDM 22
4.7. Meta Directorio de Identidades.....23
4.8. Motor de integración de identidades 23
4.9. Portal de autoservicio 24
4.10. Portal de administración 24
4.11. Integración de aplicaciones 25
4.12. Fuente autorizada de identidades..... 25
4.13. Arquitectura física de NetIQ IDM 26
5.1. Instalación para PoC o desarrollo de IDM..... 29
5.2. Servidores de la solución IDM con sus servicios 30
5.3. Portal inicial Dashboard de IDM 36
5.4. Sección aplicaciones 37
5.5. Sección nueva petición de acceso 37
5.6. Sección con información de usuarios 38
5.7. Consola de administración iManager 39
5.8. Sección Funciones y tareas 39
5.9. Administración de árbol de directorio LDAP 40
5.10. Imagen inicial de IDM sin ningún conector instalado 41
5.11. Designer de NetIQ 42
5.12. Aplicación DEMO de carga de usuarios..... 43
5.13. Carga de datos de usuarios 43
5.14. Vista de BD Postgre con datos de los usuarios 44

5.15. Designer sin ningun driver instalado 44
5.16. Configuración de Postgre 45
5.17. Parametros inicial de BD 45
5.18. Driver Postgre conectado 45
5.19. Mapeo de usuarios entre Identity Vault y BD 46
5.20. Mapeo entre sistemas Identity Vault y Postgre HR 47
5.21. Programación de eventos 48
5.22. iManager usuarios agregados 49
5.23. iManager conector funcionando 50
5.24. Selección de conector de Active Directory 51
5.25. Configuración inicial de conector Active Directory 51
5.26. Configuración del conector Active Directory 52
5.27. Conector de Active Directory Integrado al sistema Identity 53
5.28. Componente de Remote Loader 53
5.29. Configuración del componente Remote Loader 54
5.30. Remote Loader funcionando 55
5.31. Usuario agregado en sistema de HR 55
5.32. Usuario agregado en Active Directory 56
5.33. Usuario agregado en Identity Vault 57
6.1. Autorización de usuarios en NetIQ AM 60
6.2. Autorización de usuarios en NetIQ AM 60
6.3. Autenticación en NetIQ AM 61
6.4. Roles y políticas de seguridad 61
6.5. Consola de administracion Access Manager 62
6.6. Panel informativo de los componentes principales 63
6.7. Arquitectura Física de Access Manager 66
6.8. Flujo de comunicación de los componentes Access Manager 66
7.1. Selección de componentes a instalar 70
7.2. Booteo del instalador de appliance 71
7.3. Pantalla de seteo de información básica inicial del Access Gateway 71
7.4. Validación de la instalación del Access Gateway..... 72

7.5. Configuración general de Access Manager 74
7.6. Configuración inicial de directorio LDAP 75
7.7. Configuración de repositorio LDAP 75
7.10. Creación de un Proxy 76
7.11. Selección de Identity Server dentro del Proxy Reverso 77
7.12. Generación de un Proxy Reverso 78
7.13. Pestana Web Server en generación de un Proxy Reverso 79
7.14. Pestaña de configuración de recurso a proteger 80
7.15. Listado de aplicaciones aceleradas por proxy 81
7.16. Habilitación de protocolos de federación 82
7.17. Sección OAuth & OpenID Connect - Client Application 83
7.18. Aplicaciones registradas 83
7.19. Canales de comunicación SSL 84
7.20. Selección de certificado digital para SSL entre Browser y Access Gateway 85
7.21. Selección de certificado digital para SSL entre AG y Web Server 85
8.1. Instalación de Sentinel 87
8.2. Finalización de proceso de instalación 88
8.3. Inicio de login en Sentinel 88
8.4. Pantalla inicial de Sentinel 89
8.5. Conector de Identity Manager 90
8.6. Conectores configurados en SIEM 90

Capítulo 1

Introducción

Los sistemas informáticos son guiados por personas u otros sistemas informáticos. Estos sistemas, ya sean computadoras o personas, son identificados de manera tal de regular la forma en que interactúan, a qué recursos tienen acceso y de qué manera. Eso los habilita para llevar a cabo diversas acciones.
En un contexto que tiende cada vez más a la automatización y al intercambio digital, el número de identidades digitales aumenta drásticamente. Es usual además, en este mundo digital, que cada usuario o persona tenga múltiples identidades para acceder y utilizar estos sistemas.
Ante este número creciente de identidades para poder utilizar diversas plataformas y/o ambientes informáticos (en algunas referidas al mismo usuario), se plantea la necesidad de administrar adecuadamente estas identidades para poder ordenar y facilitar el uso de dichos sistemas.
Esta complejidad se da en varios ámbitos: trabajo, entretenimiento, educación, salud, entre otros. En cualquiera de estos ámbitos laborales, cada empleado que ingresa debe ser provisto de credenciales de accesos para los diversos sistemas.
La tecnología IAM (Identity and Access Manager) se utiliza para iniciar, capturar, registrar y gestionar identidades de los usuarios y sus permisos de acceso correspondiente de forma automatizada. Esto asegura que los privilegios de acceso se conceden de acuerdo con la política de seguridad establecida en el ámbito de laboral, de modo que todos los usuarios y servicios estén debidamente autenticados, autorizados y auditados.
En la presente tesina se hace inicialmente una investigación acerca de este tipo de tecnología IAM con respecto a su funcionamiento, describiendo componentes de la misma y las características principales.
Luego, se plantea la implementación de un sistema de este tipo en un organismo. El software que se eligió para demostrar la implementación de una solución IAM es el de una versión de prueba de la empresa NetIQ.

1.1. Motivación

La heterogeneidad de plataformas informáticas y la falta de políticas y procedimientos en seguridad que definan un criterio homogéneo es uno de los problemas más graves que afrontan las empresas y organismos en lo que se refiere a protección de activos de información frente a peligros externos e internos.

Las organizaciones necesitan administrar cómo acceden los usuarios a las aplicaciones sobre las diversas plataformas informáticas que posean y además extender su infraestructura para dar soporte a nuevas tecnologías.
Es común ver en distintos organismos en donde el registro de nuevos usuarios se realiza a través de una comunicación formal desde el área de Recursos Humanos al área de Seguridad. Esta forma de trabajo ocasiona que no se lleve un control estricto del ciclo de vida de la gestión de identidad, las cuentas de los usuarios y la normativa actual vigente; todo esto trae como consecuencia un incremento en el riesgo sobre la confidencialidad, disponibilidad e integridad de la información de dicho organismo.
Otro de los inconvenientes que tienen las organizaciones es el del manejo de los accesos de los usuarios a los diferentes recursos informáticos que puedan existir.
Por lo general la implementación de un sistema de accesos que soporte inicio de sesión único que habilite al usuario a acceder a varios sistemas con una sola instancia de identificación es algo complejo y de no fácil implementación.
Los diversos problemas surgen teniendo varios sistemas y aplicaciones aisladas, de diferentes tecnologías y cada uno con diferentes accesos y manejo de permisos, repositorio de identidades diferentes y en algunos casos redundantes; o la dificultad para soportar autenticación y autorización en nuevas tecnologías actuales, etc.
Por dicho motivo se plantea la necesidad de implementar un sistema del tipo Identity and Access Management (IAM por sus siglas en inglés) que centralice la administración de los usuarios y de los diferentes accesos de los mismos a diversos sistemas informáticos; permitiendo contar a su vez con mecanismos que garanticen la disponibilidad de la información y el acceso seguro a las aplicaciones y recursos.

1.2. Objetivo

El objetivo principal de esta tesina es plantear una solución de administración segura de las identidades y control de accesos.
Se presentan los aspectos generales, ventajas, desventajas, componentes y características de una solución de gestión de identidades y control de acceso, para luego explicar el diseño e implementacion de una plataforma segura de administración de identidades y control de accesos a implementar en un organismo ficticio, pero que puede ser implementado en cualquier ambito laboral que posea gran envergadura en lo que respecta a cantidad de usuarios, variedad de sistemas informaticos con diferentes tipos de accesos y roles.
Como parte de esta solución de administración segura de identidades, se promueve la unificación de los servicios alrededor de la identidad de los usuarios, conociendo y controlando que solo aquellas personas que deben consumir cierta información y recursos de TI en la organización, la hagan en tiempo y forma.
Este sistema permitirá que los usuarios realicen el procedimiento de identificación y autenticación para el acceso a los diferentes servicios y de esta manera obtener como resultado un conjunto de credenciales que pueden ser posteriormente utilizadas para demostrar su identidad en el acceso a los diferentes servicios, sin necesidad de volver a proporcionar la información de autenticación.

Lo que se implementará entonces, es una solución del tipo Identity and Access Manager (IAM) que satisfaga diferentes necesidades, entre otras:

- Contar con una solución escalable, flexible, parametrizable y que consolide diversas plataformas tecnológicas.
- Permitir la configuración en alta disponibilidad y uso de estándares y tecnologías de punta.
- Permitir el accesos de usuarios autorizados desde cualquier aplicación.
- Gestionar en forma unificada y centralizada de la seguridad e identidades
- Gestiona el acceso a información para diversos dispositivos.
- Permitir entrada única de los usuarios mediante la gestión de varias contraseñas para aplicaciones web
- Revoca el acceso a la red en forma inmediata
- Aumentar de la productividad y satisfacción de usuario
- Cumplir normas y estándares
- Federación de identidades con aplicaciones de terceros

El cumplimiento de todas estos requerimientos permitirá una mejora en la administración general de la seguridad de los sistemas de información e informática del organismo donde se implemente.

1.3. Estructura organizativa del trabajo

La presente tesina de grado se compone de 8 capítulos, que contienen la parte de investigación y la parte de implementación del sistema de manejo de identidades y control de acceso que se implementó en el organismo.
En el capítulo 2 se da un breve resumen del significado de Identidad, haciendo hincapié principalmente en la identidad digital, explicando las propiedades de la misma, y su ciclo de vida. Luego se describen los requerimientos y características principales que debe poseer un sistema de gestión de identidades típico.
En el capítulo 3 se explican las características que poseen los sistemas de gestión de identidades y control de accesos, destacando las ventajas y desventajas de su uso e implementación; explicando los distintos componentes que lo integran y su función dentro de todo el sistema de gestión.
En el capítulo 4 se describe las características de la solución elegida para realizar la implementación de la gestión de usuarios. Cada fabricante de este tipo de soluciones implementa su sistema de Identity Manager (IDM por sus siglas en inglés) de forma particular y en este capítulo se muestran las funcionalidadeses principales del software elegido y la arquitectura que posee, tanto lógica (en la que se detalla su funcionamiento interno, procesos y funcionalidades), como física explicando la arquitectura que posee y servicios que interactúan entre sí.
En el capítulo 5 se describe la implementación de la sistema en sí, ya que es donde se describen las diferentes tareas que se llevaron a cabo en el organismo, como es el proceso de instalacion y configuracion de todo el software que compone la solución de

IDM, mostrando pantallas del proceso de instalación y archivos de configuración, como también explicando las integraciones realizadas con los sistemas principales que por lo general posee cualquier organismo para el manejo de sus usuarios, siendo estos la integración con un sistema de base de datos como también con un sistema de repositorio de usuario del tipo LDAP.
Con el mismo concepto de los capítulos 4 y 5, con una descripción primero del software de manejo de identidades y una explicacion despues de las tareas realizadas, los capítulos 6 y 7 poseen la misma estructura pero esta vez del sistema de manejo de accesos a los sistemas web, llamado Access Manager (AM por sus siglas en inglés).
Como último capítulo de la implementación de gestión de identidades y control de accesos se describe la solución elegida para el manejo de los eventos de seguridad y de repositorio de logs a auditar, siendo esta una parte fundamental en el proceso de control y auditoría de todo sistema IAM que se quiera implementar.

Capítulo 2

Identidades

Antes de introducirnos en los detalles de los modelos de manejo de identidades y tecnologías fundamentales, es bueno tener una visión de lo que es identidad, que tipos de identidades hay y qué tipo de información está asociada con ella.
En este capítulo se dará una descripción de lo que se denomina “identidad”, haciendo hincapié principalmente en la “identidad digital”.

2.1. Qué es Identidad?

Identidad es una palabra que describe "el hecho de ser quién o qué es una persona o cosa".
La palabra identidad se deriva de la palabra latina idem, que significa “lo mismo”. [1]
La identidad lleva consigo el significado de igualdad, teniendo las mismas características que otra identidad. Además, la identidad también puede referirse a la identidad de las cosas en lugar de solo a las personas

2.2. Identidad Digital

La definición de identidad digital se puede definir de la siguiente manera [2]:

"*La identidad digital se refiere a la representación de la identidad de una persona en entornos digitales, en particular en términos de la representación de las características (atributos y propiedades) de la persona*".

En el mundo de hoy, donde el mundo físico y el mundo digital cada vez más informatizado se mezclan cada vez más, la diferencia entre la identidad tradicional y la identidad digital es cada vez más vaga y estrecha.

2.3. Propiedades de la Identidad

El problema fundamental en la interacción digital es saber con certeza con quién está interactuando. Actualmente, es imposible obtener una garantía completa sobre la

identidad de la contraparte. Por lo tanto, la interacción digital tiene mucho que ver con el nivel de confianza y autorización entre los sistemas. Esto significa también asegurar la integridad de la identidad. Por lo tanto, gestionar identidades en la sociedad actual de la información significa siempre gestionar la seguridad de la información.
Los sistemas de gestión de identidad forman parte de los “Sistemas de Gestión de Seguridad de la Información (SGSI)”. En el SGSI, la seguridad de la información se define por tres aspectos [4]:

- *Confidencialidad*: propiedad que información no está disponible o divulgadas a individuos no autorizados , entidades o procesos.

- *Disponibilidad*: propiedad de ser accesible y usable bajo demanda por una entidad autorizada.

- *Integridad*: propiedad de mantener con exactitud la información de tal cual fue generada, sin ser manipulada ni alterada ante por personas o procesos no autorizados

2.4. Ciclo de Vida de la Identidad

En la misma forma que las criaturas vivientes, las identidades tienen “una vida”; y respecto al manejo de identidades, las mismas tienen una vida útil.
Primero, tiene un nacimiento (ej cuando una cuenta de usuario es creada), luego un uso durante un tiempo determinado, y luego su muerte.
Antes de la “muerte” de la identidad, esta puede ser modificada y/o mantenida.
Fundamentalmente, la gestión del ciclo de vida de la identidad siempre tiene la misma idea. Primero, se crea la identidad. Luego, se usa y se pueden hacer algunos cambios, por ejemplo, en los atributos de la identidad. Una vez que termina la "vida" de la identidad, se retira del uso.
Según el sistema de gestión de identidad que se gestiona, estas fases se pueden dividir en muchas subfases. Además, dependiendo de la identidad, algunas de estas fases se pueden volver a aplicar a la identidad varias veces.
Según [5], el ciclo de vida de la identidad consiste en aprovisionamiento, propagación, uso, mantenimiento y desaprovisionamiento:

- *Aprovisionamiento*: El aprovisionamiento es un proceso en el que se crea un nuevo registro de identidad y se asocia con ciertos atributos como el nombre y el correo electrónico. El aprovisionamiento puede realizarlo el administrador o uno puede hacerlo por autoservicio, como crear una cuenta de usuario en un sitio web. [5]
  Cuando se crea la identidad, los atributos generalmente se corroboran primero, dependiendo de la importancia de la identidad. Por ejemplo, se verificará la edad y la dirección de la persona y documento de identidad. Después de una prueba

exitosa, se emiten las credenciales y la identidad se forma y está lista para ser usada. [3]

- *Propagación*: Si la identidad necesita ser integrada en otros sistemas durante su ciclo de vida, debe haber una fase de propagación. Esto significa que el sistema original y el sistema donde se propaga la identidad se vinculan entre sí. La propagación debe ocurrir cada vez que hay un cambio en el registro de identidad y debe hacerse de manera confiable para garantizar la funcionalidad mutua de ambos sistemas. [5]

- *Uso*: Este es el paso más obvio y la fase a la que apunta toda la gestión de identidad: el uso confiable y fluido de las identidades.

- *Mantenimiento*: Mantener identidades, incluidos sus atributos y credenciales, es vital para mantener el Sistema de Gestión de Identidades funcional y bajo control. Ya sea un agente como una impresora de red cuya dirección IP ha cambiado o una persona que ha cambiado su nombre, la integridad de los atributos debe estar intacta en todo momento. Además, es posible que las personas quieran cambiar sus contraseñas, por lo que sus credenciales deben actualizarse.

- *Desaprovisionamiento*: Tener un protocolo adecuado para el desaprovisionamiento de identidades debe considerarse tan importante como el aprovisionamiento. Al igual que en el mantenimiento, para preservar el sistema de gestión de identidad limpio de cuentas antiguas e inválidas, las identidades deben ser desaprovisionadas, eliminadas del uso, inmediatamente después de que ya no sean necesarias. Si todavía quedan cuentas antiguas, pero activas en el sistema, podrían representar una amenaza para la seguridad. Por ej, un pirata informático podría abusar de ellos o, un ex empleado aún podría tener acceso a la información de la empresa después de salir de la misma, etc. [5]

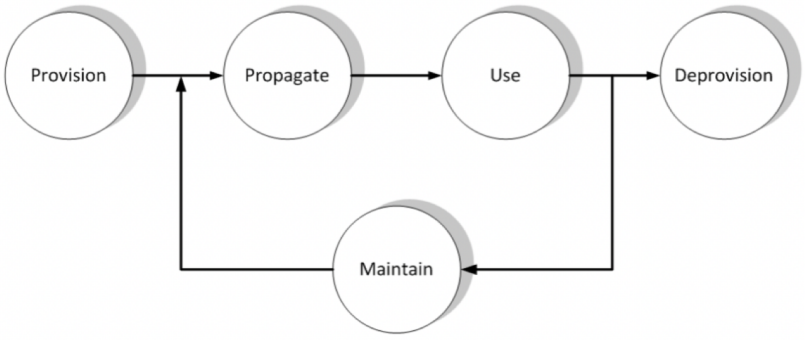


Figura 2.1: Ciclo de vida de la Identidad

Capítulo 3

Gestión de Identidades y Control de Acceso

En este capítulo se explica que es un sistema de gestión de identidades y control de accesos; dando las ventajas y las desventajas que tiene su uso e implementación.
A su vez, se describen los componentes principales que forman un sistema de este tipo, detallando cada uno y sus características. Por último, se detalla la arquitectura de estos sistemas de gestión y cómo interactúan los distintos componentes.

3.1. Características principales

Un sistema de administración de accesos e identidades (IAM, por sus siglas en inglés) se define como un conjunto de procesos de tecnologías, infraestructura y políticas que permite gestionar las identidades de los usuarios y controlar el acceso de los mismos a los recursos de las organizaciones [6].
La tecnología IAM se puede utilizar para iniciar, capturar, registrar y gestionar identidades de los usuarios y sus permisos de acceso correspondientes de forma automatizada. Esto asegura que los privilegios de acceso se conceden de acuerdo con una interpretación de la política, de modo que todos los individuos y los servicios están debidamente autenticados, autorizados y auditados [7].

V*entajas*:

Entre los beneficios [6] que se pueden lograr implementando una solución de gestión de identidades y control de accesos son:

- *Control de accesos basado en roles*: esto permite que un usuario tendrá accesos sólo a los que su rol dentro del organismo le permita; no teniendo más privilegios que los asignados según su función y cargo.
- *Autoservicio*: debido a que este tipo de soluciones permite la autogestión de la propia identidad digital de los usuarios, pudiendo estos recuperar contraseñas, solicitar permisos, etc. Esto ayuda a su vez favorece la reducción de tareas administrativas asociadas con la gestión de cuentas de usuarios, altas, bajas, modificación de las mismas o asignación de permisos dentro del organismo. A su vez que se le delega al usuario la solicitud de recursos y accesos a aplicaciones y a los dueños de las mismas la potestad de permitir o denegar dichas solicitudes.

- *Automatización*: este tipo de sistemas permite la automatización de todos los procesos relacionados con el usuario y sus accesos; como por ejemplo la creación, la baja y la modificación de las cuentas de usuarios. Además permite la automatización de aprobaciones de diversos permisos, acceso o revocación de diversos permisos, asignación de roles , etc.
- *Reducción de tiempo de accesos y recursos*: al estar automatizado todo el proceso de gestión de identidades, permite que un usuario acceda a todos los recursos asignados según se cargo una vez que se informa su alta en el organismo; aprovisionando de forma automática e inmediata todo lo necesario para su labor dentro del mismo.
- *Administración centralizada*: estos sistemas IAM centralizan los diversos repositorio de usuario que puedan existir en un organismo, en un solo repositorio central de identidades. Esto facilita la administración de las cuentas de usuario debido a que con una sola cuenta se tiene accesos a diferentes sistemas informáticos o aplicaciones
- *Eliminación de cuentas huérfanas*: como los procesos están automatizados, ante la notificación de una baja o de un cambio en la situación contractual de un usuario, este es automáticamente dado de baja y/o revocación de permisos y accesos, generando a su vez una mejora en la seguridad.

Desventajas:

Las principales desventajas que se pueden observar en la implementación de una solución de gestión de identidades y control de acceso son:

- Al permitir y facilitar la administración de cuentas, haciendo que un usuario solo requiere el conocimiento de una contraseña para acceder a todos los sistemas y aplicaciones que tiene permitido, hace que ante el robo o pérdida de la misma aumente el riesgo en la seguridad del organismo.
- Como el proceso de autenticación y acceso a las distintas aplicaciones se realiza autenticación ante un único repositorio central de identidades, ante la falla o mal funcionamiento del mismo repercute en los accesos a todos las aplicaciones integradas con este, siendo necesario para evitar o reducir dicho riesgo la instacion y configuracion de servicios redundantes y de alta disponibilidad.
- Requiere mucha reestructuración de las definiciones de roles de negocio y su relación con los roles técnicos, debiendo relevar diferentes accesos y permisos a las distintas aplicacione y plataformas informáticas.
- La implementación de este tipo de solución no es sencilla y requiere de recursos, reestructuración y/o modificaciones en algunos casos de aplicaciones a integrar; así como también procesos del negocio. Los mecanismos de autenticacion y autorizacion a los sistemas cambian sustancialmente debiendo adecuarse al nuevo sistema. Además que este tipo de solución por lo general son del tipo propietarias y tienen un alto costo económico.

- La integración de las aplicaciones depende de la complejidad que tengan y los métodos de autenticación y autorización que se deban re-adecuar y configurar al nuevo sistema. Es necesario por eso tener un gran conocimiento de las distintas aplicaciones a integrar, siendo complejo en situación de aplicaciones obsoletas o legacy que dejaron de tener algún soporte técnico.

3.2. Componentes

Una solución de gestión de identidades y control de acceso cuenta con los siguientes componentes:

1. *Servicio de directorios*: Los directorios son tipos especiales de bases de datos que están optimizadas para búsquedas y lecturas de datos. Aunque los directorios pueden verse como bases de datos, difieren de las bases de datos tradicionales en muchos aspectos. Por su dinámica, no son adecuados para almacenar datos que cambian rápidamente. Además, los servicios de directorio no admiten métodos de acceso similares a las bases de datos de uso general, como el lenguaje de consulta estructurado SQL, sino protocolos de acceso más simples. [11]
   Muchas de las soluciones modernas de servicios de directorio se basan en el protocolo X.500 estandarizado por la Organización Internacional de Normalización (ISO) y ITU-T en 1988.
   En X.500, se utilizó un protocolo llamado Protocolo de Acceso a Directorio (Directory Access Protocol - DAP). en comunicación entre el cliente de directorio y el servidor de directorio. Sin embargo, al ser demasiado pesado e intensivo en recursos, se desarrolló una versión más ligera llamada Lightweight Directory Access Protocol (LDAP). [10]
   Las entradas en un sistema LDAP se organizan en una estructura similar a un árbol llamada Árbol de información de directorio (Directory Information Tree - DIT).
   Hoy en día, hay varios servicios de directorio en uso. El más común de ellos es Microsoft Active Directory (o AD en resumen). Otros incluyen NetIQ eDirectory (solía ser Novell eDirectory), Sun Java System Directory Server, Red Hat Directory Server (anteriormente la solución de Netscape) y otros. El factor común para todos los servicios de directorio es que todos admiten LDAP. [10]

2. *Meta-Directorios*: Los Metadirectorios son un tipo particular de directorio que tienen la particularidad de almacenar información de distintos fuentes de datos [5], proporcionando un flujo de datos entre uno o más servicios de directorio y bases de datos, para mantener la sincronización de esos datos, y es una de las partes más importante de los sistemas de gestión de identidad.
   En la Figura 3.1 a continuacion se presenta un ejemplo de meta- directorio, en el cual se integra la información proveniente de los servicios de directorios de empleados y terceros. La comunicación con los servicios de directorios se realiza a través del protocolo LDAP y la información almacenada en éste es consultada por las aplicaciones de negocio y las aplicaciones integradas por medio del portal

corporativo, las cuales sólo deben consultar un repositorio de información y no dos como sería en el caso de no contar con el meta-directorio.

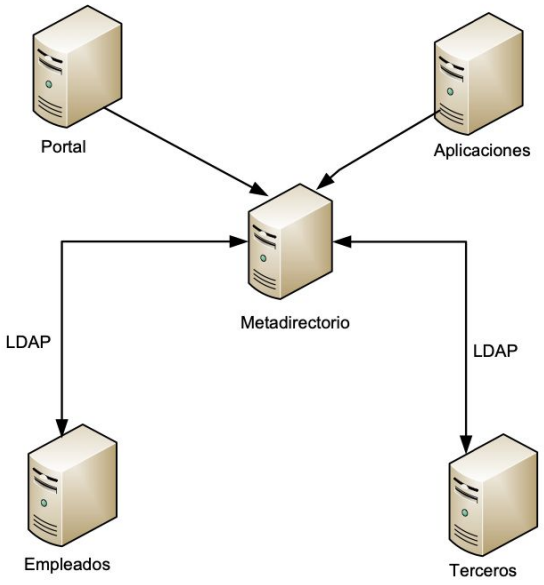


Figura 3.1: Topología de un Meta-directorio [7]

3. *Sistema de Gestión de identidades*: Uno de los sistemas principales es la gestión de identidades, ya que este permite gestionar el ciclo de vida de las identidades de los usuarios dentro de la organización. Entre las funciones de un sistema de gestión de identidades se encuentran el aprovisionamiento/desaprovisionamiento de las identidades, creando modificando y dando de baja las identidades en los diversos sistemas integrados, bases de datos y servicios de directorios.
   A su vez en este sistema se realizan los procesos de reconciliación (sincronización) con las fuentes de autoridad y aprovisionamiento con las aplicaciones y sistemas se integran con la solución de gestión de identidades y control de acceso.

4. *Sistema de gestión de roles*: El sistema de gestión de roles es un componente intermedio que se encuentra entre la gestión de identidades y el control de acceso. Es así como la gestión de identidades se encarga del gobierno de las identidades, la gestión de roles asigna los roles de acuerdo al cargo y funciones del usuario y la gestión del control de acceso se encarga de definir las políticas que regulan el acceso a los diferentes recursos dentro de la organización.
   Por medio de la gestión de roles se busca garantizar que cada usuario recibe las autorizaciones que corresponden al rol de negocio y a las funciones desempeñadas dentro la organización mejorando los aspectos de seguridad y cumplimiento.

4. *Fuentes de autoridad:* Compuesta por la nómina y recursos humanos. En estos repositorios de aplicaciones se almacena la información de los usuarios y son los encargados de disparar los eventos dadas las novedades de contratación, terminación de contrato, vacaciones, incapacidades, licencias, etc. Por ejemplo, cuando se contrata un empleado, se almacena en una tabla de eventos la información del usuario para ser creada en el gestor de identidades y replicada en los demás sistemas. Para el caso de las vacaciones se almacena en la tabla de eventos la información del usuario para indicarle al gestor de identidades que dicha cuenta se debe deshabilitar en un determinado período y a su vez realizar la des-habilitación en las diferentes aplicaciones y sistemas.

5. *Sistema de gestión de autenticación y control de acceso*: En este componente se realiza la configuración de las políticas de autenticacion y control de acceso tomando la información de usuarios y roles consolidada en el Metadirectorio. La autenticación es un proceso mediante el cual un sistema verifica la identidad de un usuario que desea acceder a él. Dado que el control de acceso normalmente se basa en la identidad del usuario que solicita acceso a un recurso, la autenticación es esencial.
   El sistema de autenticación principal en un sistema IAM es el de inicio de sesión único o Single Sign-On (SSO por sus siglas en inglés).
   Básicamente, SSO es un método para compartir datos de autenticación. SSO permite al usuario iniciar sesión una vez y luego usar el mismo nombre de inicio de sesión para conectarse a múltiples sistemas sin tener que iniciar sesión en cada uno de ellos nuevamente.
   Aunque el inicio de sesión único proporciona una forma de acceder a múltiples servicios con una autenticación, esto no significa necesariamente que la información de inicio de sesión esté unificada en todos los sistemas.
   El sistema SSO utiliza el mapeo del inicio de sesión del usuario en cuentas locales y transmite información de autenticación que es aceptada por todos los sistemas dentro del ámbito del SSO [3].
   Entre los diferentes modelos de implementación de SSO podemos encontrar:

   - Basado en intermediario. Este tipo de soluciones se basan en servidores que manejan la autenticación y la administración de cuentas de los usuarios. La forma más común de implementar SSO basado en intermediario es mediante Kerberos. En Kerberos, un servidor de confianza actúa como intermediario. Kerberos es diferente de los métodos de autenticación de nombre de usuario/contraseña. En este sistema, el cliente que desea contactar con un servidor para que le dé un servicio, debe pedir primero un ticket de una tercera parte de mutua confianza, el KAS("Kerberos Authentication Server"). Respectivamente, Kerberos tiene tres "cabezas": el cliente, el servidor de autenticación KAS y el servidor de destino deseado. Kerberos usa cifrado simétrico y el proceso de autenticación tiene básicamente tres pasos [9]:
     1. El cliente envía un mensaje al servidor que autentica los usuarios

2. Una vez que autentica el servidor le da un “ticket” al cliente válido por X tiempo y que incluye la información del cliente
3. El cliente puede acceder a la red y a los recursos a los que su ticket le de acceso durante el tiempo que este sea válido

- Basado en agente. En las soluciones basadas en agentes, se utiliza un programa de agente para reconocer al usuario con la ayuda de listas o claves criptográficas. Este agente puede estar ubicado en el lado del cliente o servidor. Ejemplo de este tipo de método es el agente SSH.
- Basado en proxy-reverso o gateway: Un servidor proxy reverso es un tipo de servidor proxy que dirige las solicitudes de los clientes al servidor que se quiere acceder. El servidor proxy sólo permite el acceso de usuarios con credenciales válidas y redirige a los no válidos al servidor que permite que los clientes se registren [14]. Un proxy reverso de SSO es un tipo de proxy reverso que ejecuta un software de SSO que inspecciona las solicitudes de acceso. Estas solicitudes pueden ser, por ejemplo, tickets Kerberos válidos. Si la solicitud no es válida (por ejemplo, el usuario ha introducido credenciales incorrectas), el usuario es redirigido a un servidor de autenticación.

6. *Sistemas de gestión de Identidad Federada*: La Identidad federada significa vincular y usar las identidades electrónicas que tiene un usuario en varios sistemas de gestión de identidad.
   En términos más simples, una aplicación no necesariamente necesita obtener y almacenar las credenciales de los usuarios para autenticarse. En cambio, la aplicación puede usar un sistema de administración de identidad que ya está almacenando la identidad electrónica de un usuario para autenticarlo, dado que, por supuesto, la aplicación confía en ese sistema de administración de identidad.
   De aquí surge que la federación implica la delegación de responsabilidades, a través de relaciones de confianza entre las partes federadas.
   Este enfoque permite el desacoplamiento de las funciones de autenticación y autorización. También facilita la centralización de estas dos funciones en el organismo para evitar una situación en la que cada aplicación tenga que gestionar un conjunto de credenciales para cada usuario. También es muy conveniente para los usuarios, ya que no tienen que mantener un conjunto de nombres de usuario y contraseñas para cada aplicación que utilizan.

   Existen dos protocolos principales para la identidad federada: OpenID y OAuth:

   - OpenID Connect: es un estándar abierto patrocinado por Facebook, Microsoft, Google, PayPal, Ping Identity, Symantec y Yahoo. OpenID permite que el usuario se autentique utilizando servicios de terceros llamados proveedores de identidad (Identity Providers).
     Los usuarios pueden elegir usar sus proveedores OpenID preferidos para iniciar sesión en sitios web que aceptan el esquema de autenticación OpenID.
     La especificación OpenID define tres roles:

- ❏ El usuario final o la entidad que busca verificar su identidad
- ❏ La parte que confía (RELAYING PARTY), que es la entidad que busca verificar la identidad del usuario final
- ❏ El proveedor de OpenID (IDENTITY PROVIDER), que es la entidad que registra la URL de OpenID y puede verificar la identidad del usuario final

- OAuth: es otro estándar abierto y difiere de OpenID en ser exclusivamente para fines de autorización y no para fines de autenticación.
  OAuth proporciona un método para que los clientes accedan a los recursos del servidor en nombre del propietario del recurso (como un cliente diferente o un usuario final). También proporciona un proceso para que los usuarios finales autoricen el acceso de terceros a los recursos de su servidor sin compartir sus credenciales (generalmente, un par de nombre de usuario y contraseña), utilizando redirecciones de agente de usuario.

  Las especificación OAuth define los siguientes roles:

  - ❏ El usuario final o la entidad propietaria del recurso en cuestión.
  - ❏ El servidor de recursos (OAuth Provider), que es la entidad que aloja el recurso
  - ❏ El cliente (consumidor de OAuth), que es la entidad que busca consumir el recurso después de obtener la autorización del cliente
  - ❏ El usuario final o la entidad propietaria del recurso en cuestión.
  - ❏ El servidor de recursos (OAuth Provider), que es la entidad que aloja el recurso
  - ❏ El cliente (consumidor de OAuth), que es la entidad que busca consumir el recurso después de obtener la autorización del cliente

Capítulo 4

Solución Identity Manager a Implementar

En el siguiente capítulo se realiza la explicación del software elegido para gestionar las identidades. Se explica en detalle cuales son las características de dicho software y cuales son sus principales funciones.
Luego se detalla la arquitectura que tiene dicho software, diferenciando la misma en parte lógica y parte física.

4.1. NetIQ Identity Manager IDM

La solución por la que se optó para la la gestión de Identidades interna es la de la empresa Micro Focus NetIQ IDM [12].
Dicho producto es una solución de administración de identidades y aprovisionamiento de usuarios, que provee un entorno de identidades seguro, e incluye un control de acceso empresarial, manejo de passwords, y funcionalidades de autoservicio. Estas capacidades permitirán gestionar las identidades y recursos eficientemente y en forma segura.
Es habitual que las organizaciones tengan sus datos de identidades guardadas en múltiples sistemas informáticos, ya que cada sistema, sea web, de correo electrónico, bases de datos, etc; cuentan por lo general con su propio repositorio usuarios. Por eso el manejo de identidades y monitoreo de la actividad de los usuarios en entornos físicos y virtuales conlleva a diferentes desafíos que IDM trata de solucionar:

- Sincronizando la identidad a través de los sistemas conectados
- Asegurando que los usuarios tienen accesos sólo a los recursos requeridos para sus trabajos.
- Aprovisionando o de-aprovisionando accesos de usuarios de acuerdo a sus roles
- Aprovisionando según políticas de negocio u otros requerimientos regulatorios.

4.2. Funciones principales

Como funciones principales de dicho producto de gestión de identidades se destacan:
Sincronización de la información de la identidad: permite sincronizar, transformar y compartir información a través de un amplio rango de sistemas conectados (por ej.

Microsoft Sharepoint, Exchange, Active Directory, eDirectory, Oracle, etc); permitiendo controlar el flujo de datos entre los sistemas conectados, determinar qué dato el compartido, que sistema es la fuente autorizada para una parte de los datos, y como los datos se interpretan y transforman para cuplir con los requisitos de otros sistemas.

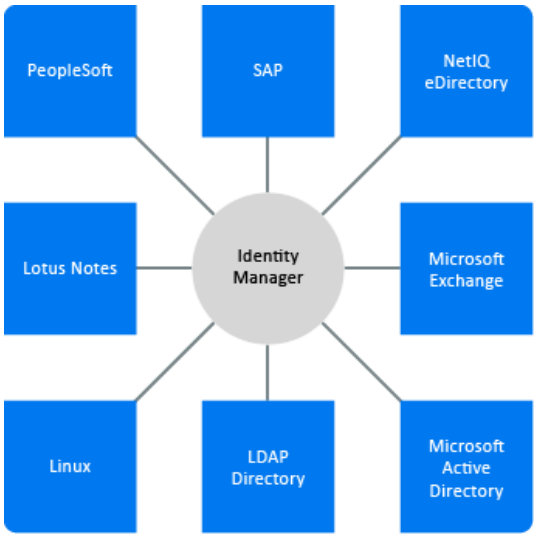


Figura 4.1: Sincronización de Identity Manager y sistemas conectados

Un ejemplo de sincronismo e integración entre distintos sistemas lo podemos ver en la figura 4.2, donde se observa a un sistema Lotus Note que es la fuente autorizada para la cuenta de correo de un usuario. La base de datos SAP HR de Recursos Humanos también usa direcciones de correo, entonces IDM transforma la cuenta de correo en un formato que se requiera y lo comparte con la base de datos de SAP HR. Cuando el correo cambia en el sistema Lotus Notes, esta se sincroniza con la base de datos de SAP HR.

Figura 4.2: Ejemplo de integración entre sistemas con Identity Manager

Si un administrador de SAP HR modifica una dirección de correo en el sistema, el cambio no tiene efecto porque este debe hacerse en el sistema Lotus Notes para que este sea efectivo, ya que este es lo que se llama la fuente autorizada para la cuenta de correo del usuario.

A su vez, NetIQ IDM permite sincronizar password entre sistemas. Por ejemplo si un usuario cambia su password en un sistema Active Directory, IDM puede sincronizar esos passwords a otros sistemas que tenga conectados (por ejemplo Lotus Notes, SAP, Oracle, etc).
Otra funcionalidad es la de creación de nuevas cuentas de usuarios y eliminación de las cuentas existentes en sistemas conectados. Por ejemplo cuando se da de alta un nuevo usuario en la base de datos SAP HR de recursos humanos, IDM puede automáticamente crear un nueva cuenta de usuario en otros sistemas conectados.

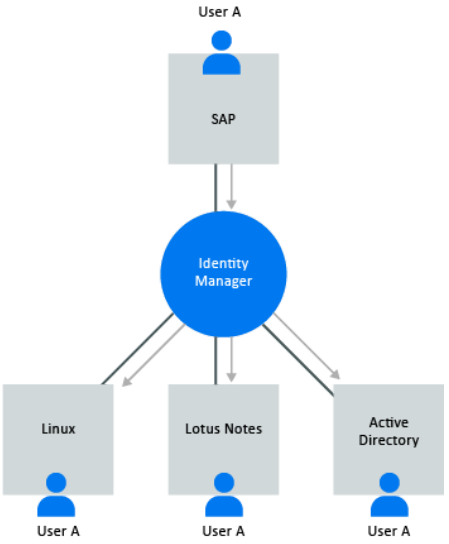


Figura 4.3: Sincronización de passwords

Automatización de procesos de IT con Workflows: Los usuarios usualmente requieren accesos a varios fuentes para cumplir tareas basadas según sus roles dentro del organismo. NetIQ IDM provee la capacidad de workflows para asegurar que el proceso de aprovisionamiento involucre a los apropiados aprobadores de dichos recursos.

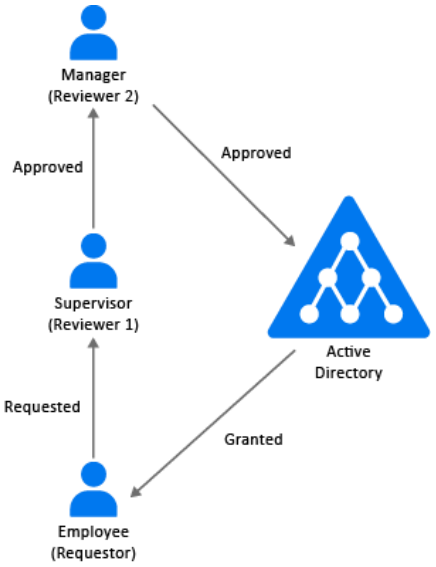


Figura 4.4: Workflow de aprobación

NetIQ IDM también provee capacidades de workflows de aprobación (o flujos de trabajo) para asegurar que el proceso de aprovisionamiento involucre a los aprobadores correspondientes. Por ejemplo asumiendo que un usuario X, quien ha sido aprovisionado con una cuenta de Active Directory, necesita acceso a algún reporte financiero a través de dicho sistema; este requiere la aprobación de ambos superiores, por ejemplo su jefe de Departamento y/o Gerente.
De esta manera, se puede setear un workflow de aprobación que rutea el pedido del usuario a su jefe y luego a la aprobación de su gerente. La aprobación final automáticamente aprovisiona los derechos de Active Directory necesarios para que dicho usuario acceda y vea el documento financiero.
Los workflows pueden ser iniciados automáticamente cuando un cierto evento ocurre (por ejemplo un nuevo usuario es agregado el sistema de recursos humanos) o se pueden inicializar manualmente a través de un pedido de usuario.

Accesos basados en roles a los usuarios: El aprovisionamiento involucra procesos automáticos de agregación, modificación y borrado de usuarios y sus atributos. Esto incluye el manejo de atributos de los perfiles de los usuarios, incluyendo sus roles y sus accesos asociados.
IDM permite aprovisionar usuarios basados en sus roles dentro de la organización, permitiendo que se definan los roles y haciendo la asignación de acuerdo a las necesidades de la organización.
Cuando un usuario es asignado a un rol, IDM aprovisiona el usuario con los accesos a los recursos asociados a el rol.
Los usuarios que tienen múltiples roles reciben accesos asociados a todos los roles, como se muestra en la siguiente figura 4.5:

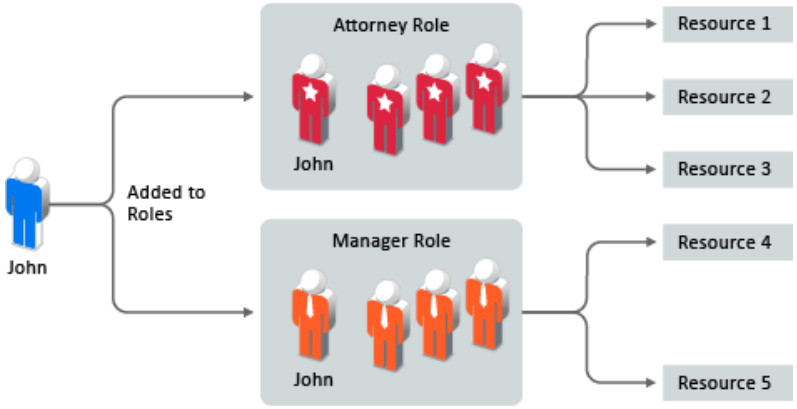


Figura 4.5: Gestión de Roles

Habilitación de autoservicio para los usuarios: NetIQ IDM utiliza la identidad como base para autorizar a los usuarios el acceso a sistemas, aplicaciones y bases de datos.
Los roles de cada usuario administrados en Identity Manager pueden incluir derechos de acceso específicos a las aplicaciones conectadas.
Además, se pueden delegar tareas administrativas a las personas que deben ser responsables de ellas. Por ejemplo, se puede permitir que los usuarios individuales puedan administrar sus propios datos personales, viendo y editandolos desde la interfaz de autoservicio (estos datos automáticamente se modifican en todos los sistemas sincronizados a través de IDM); o cambiar sus propias contraseñas y configurar preguntas de seguridad y respuestas en el caso que se les olviden; como también solicitar accesos a los diferentes recursos informáticos de la organización.

4.3. Arquitectura de NetIQ IDM

NetIQ IDM consta de componentes que se encuentran en el front-end (osea la parte que interactúa con los usuarios), y que están separados lógicamente del motor de aprovisionamiento que se encuentra en back-end (siendo esta la parte que procesa la entrada desde el front-end).
Este enfoque de computación distribuida le permite implementar alta disponibilidad y recuperación de desastres en cada capa. También proporciona flexibilidad de implementación, lo que permite comenzar con una implementación básica y agregar capacidad y funcionalidad a lo largo del tiempo.

4.3.1. Arquitectura Lógica

A continuación, se describe la solución de Identity Manager desde un punto de vista técnico, mostrando la arquitectura y sus distintos componentes de forma conceptual, así como una explicación de los productos de software de que hacen posible esta solución.

El enfoque que se le da a la solución y que se presenta a continuación, considera la existencia de un punto centralizado de identidades y administración que es el que tendrá contacto con las aplicaciones y sistemas a integrar.
Es desde este punto centralizado que se distribuyen las identidades a las distintas aplicaciones y sistemas del organismo. Según el tipo de usuario del que se trate, el usuario fluye desde el Metadirectorio de Identidades hacia las aplicaciones y sistemas integrados por la solución, a los cuales, con base a su perfil y reglas de negocio definidas, el usuario deba tener acceso teniendo en cuenta los principios básicos de seguridad y control de accesos basados en roles, los cuales indican que siempre se debe aprovisionar el acceso mínimo con el cual el usuario sea capaz de cumplir sus funciones.
En la figura 4.6 vemos la arquitectura lógica del sistema NetIQ IDM, donde se muestran los diferentes componentes y se relacion entre ellos.

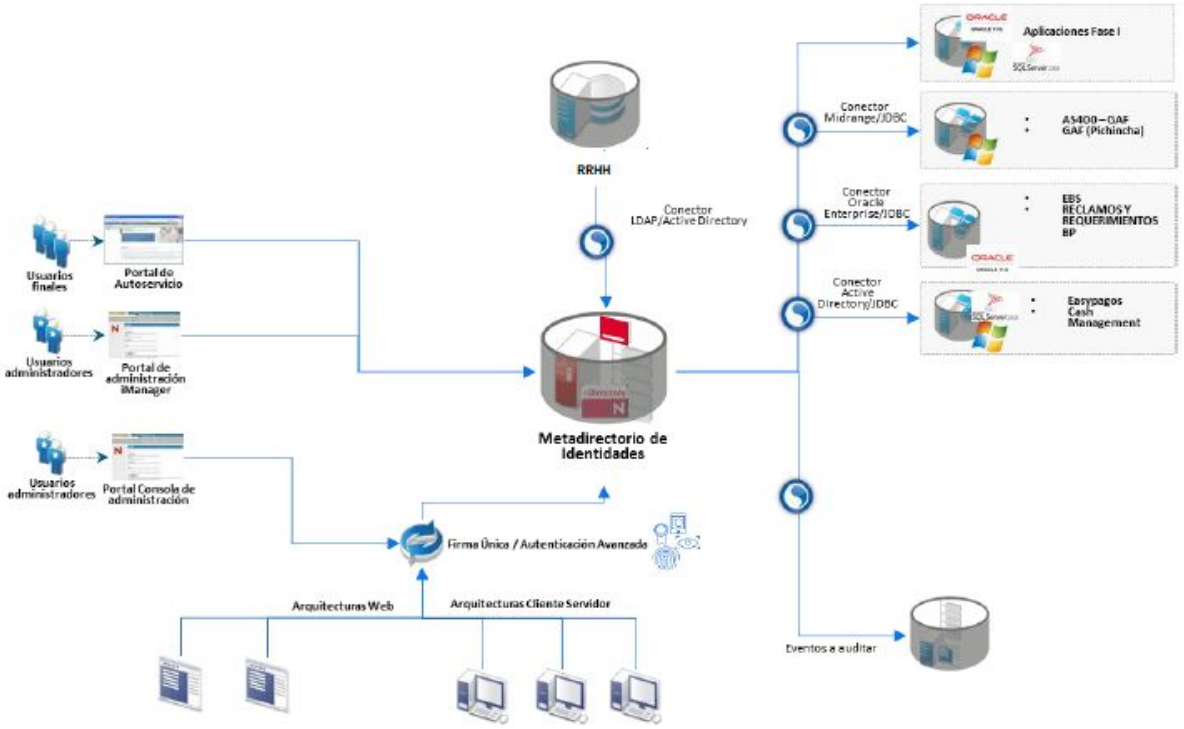


Figura 4.6: Arquitectura Lógica de NetIQ IDM

Como dijimos, el sistema IDM posee varios componentes informáticos que sirven ya sea para la interacción con los usuarios finales, como componentes que procesan los datos de los usuarios y que permiten la sincronización entre los diferentes sistemas a integrar, como ser bases de datos, directorios LDAP, sistemas web, etc. Entre los principales componentes podemos describir:

Meta-Directorio: El Metadirectorio o "Directorio maestro de identidades" es una base de datos jerárquica implementada a través de tecnologías de directorios, en la cual se encuentran concentradas las identidades participantes dentro del organismo, sirviendo adicionalmente como repositorio de cuentas, contraseñas, certificados, grupos roles, políticas y reglas de negocio las cuales forman parte adicional de la identidad y son utilizados para realizar el aprovisionamiento adecuado de la identidad en las diferentes aplicaciones y recursos.

Figura 4.7: Meta Directorio de Identidades

Motor de integración de identidades: El motor de integración de identidades es un sistema basado en reglas de negocio, integrado dentro del meta directorio mediante el cual se realiza el aprovisionamiento (creación, mantenimiento y baja de cuentas) la sincronización de contraseñas y el autoservicio para las diferentes aplicaciones que conforman el universo del organismo.
El motor de integración de identidades cuenta con conectores pre construidos que facilitan la configuración de reglas de negocio para integrar aplicaciones como: Bases de datos con soporte a JDBC (Oracle, DB2 DB, MYSQL) sistemas operativos (Linux, Windows,AIX, RACF para Mainframes), Directorios (Active Directory, eDirectory, LDAP), Correo Electrónico (MS Exchange, Lotus Notes, Groupwise) y soporte adicional para archivos de texto, así como un SDK (software development kit) para el desarrollo personalizado de conectores con cualquier tipo de aplicación. Estos conectores de integración, son los encargados de llevar la información de altas, bajas y cambios desde el Meta Directorio hacia las aplicaciones integradas.

Figura 4.8: Motor de integración de identidades

Portal de autoservicio: Este portal es la parte de front-end del sistema IDM, que incluye los componentes del subsistema de workflows (flujos de autorización), solicitudes de accesos y permisos, y el módulo de autoservicio para contraseñas.
Este módulo también permite a los usuarios aprobadores de un flujo de autorización, pudiendo otorgar, denegar o delegar la tarea de aprobación/denegación a otros usuarios de su confianza (por ejemplo para periodos vacacionales o de ausencia prolongada del aprobador inicial).
El back-end del subsistema de workflow, es el encargado de recibir del portal de servicio de usuarios finales las peticiones y los pedidos de acceso a nuevas aplicaciones así como también la solicitud de roles por parte de dichos usuarios, iniciar las actividades definidas dentro del flujo de aprobación.

Figura 4.9: Portal de autoservicio

Portal de administración: Todas las operaciones de administración que se definen y configuran para el portal de autoservicios, como por ejemplo, definición de los flujos de autorización (workflows), los diferentes niveles de accesos a los sistemas, los diferentes roles que se configuran, los delegados y usuarios intermedios que se definan, la auditoría, entre otras cosas, se realiza desde este portal de administración.

Figura 4.10: Portal de administración

Integración de Aplicaciones: Estos sistemas y aplicaciones se definen en base a las necesidades que se tenga según los sistemas a integrar. Para este caso particular, las aplicaciones que el organismo requiere integrar en esta solución de IDM son principalmente, driver conector de Base de Datos JDBC, driver conector de Active Directory.

Figura 4.11: Integración de aplicaciones

Fuente autorizada de identidades: La fuente autorizada de identidades es el repositorio de datos a partir del cual es posible identificar la creacion, modificacion o baja de una identidad dentro de la solución; ejemplos típicos son la bases de datos de Recursos Humanos (HR), los cuales son fuente autorizada para la creación, mantenimiento y baja de empleados como parte del sistema de identidades.

Figura 4.12: Fuente autorizada de identidades

4.3.2. Arquitectura Física

Anteriormente se describió lógicamente los componentes de NetIQ IDM, a continuación se dará un detalle de los componentes físicos de esta solución. Cada uno de estos componentes es un software con una característica y configuración particular
El siguiente figura 4.13 muestra cómo los componentes interactúan entre sí para proporcionar las capacidades de NetIQ Identity Manager: sincronización de datos, flujo de trabajo, funciones, autoservicio y auditoría / informes.

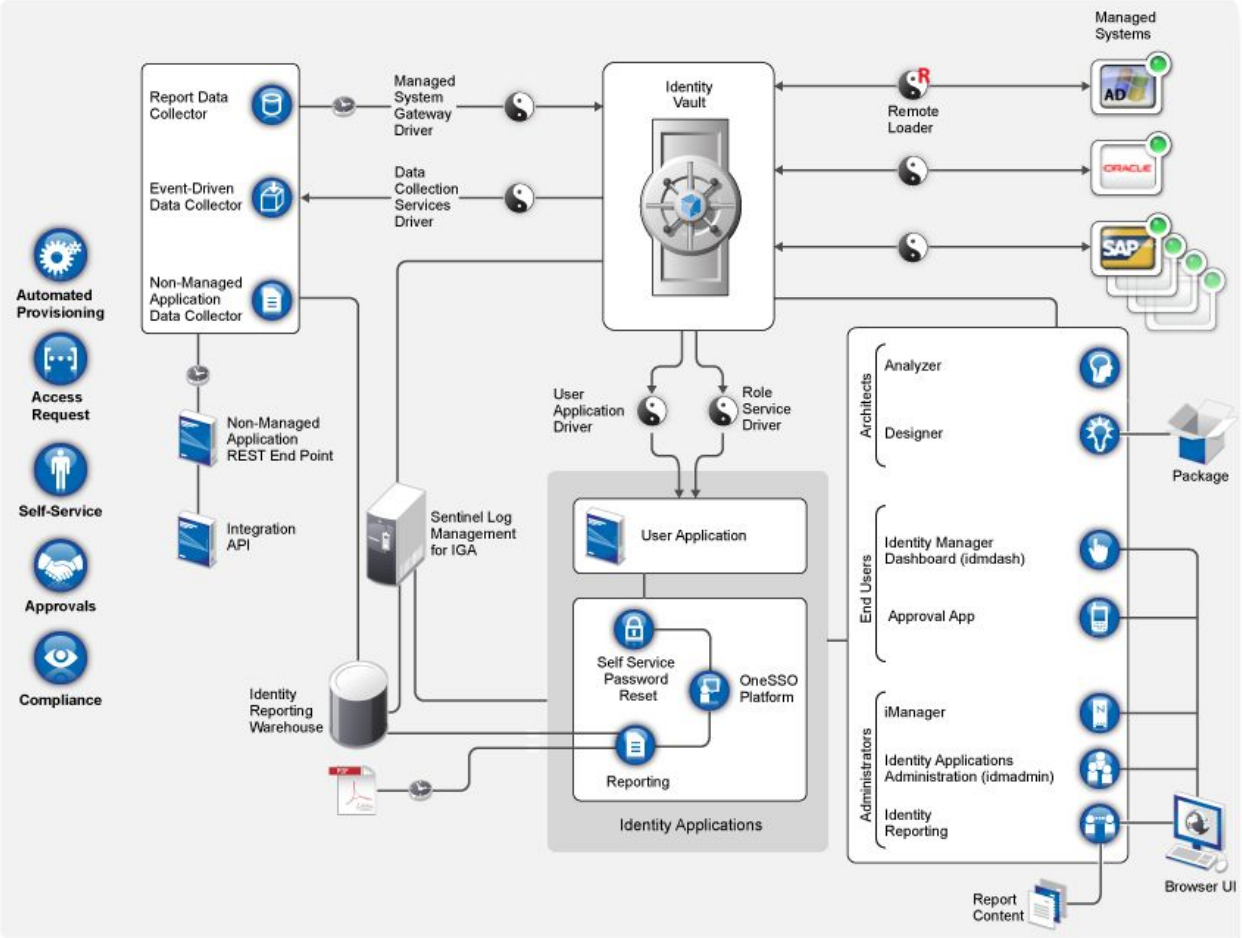


Figura 4.13: Arquitectura física de NetIQ IDM [16]

Como se aprecia en la figura 4.13, una solución de IDM posee varios componentes que interactúan entre sí para gestionar las identidades en forma segura y confiable. Entre los diferentes componentes de la solución elegida los principales son:

1. Identity Vault: este contiene toda la información que el sistema IDM necesita para su funcionamiento. Identity Vault guarda los datos que se quieren sincronizar entre los sistemas conectados. Por ejemplo, los datos sincronizados desde un sistema SAP a Lotus Notes se agregan primero a Identity Vault y luego se envían al sistema Lotus

Notes. El sistema Identity Vault también almacena información específica de IDM, como configuraciones de controladores y driver, parámetros y políticas.Identity Vault utiliza una base de datos propietaria de NetIQ eDirectory [13].

2. Motor de Identity Manager: El motor de Identity Manager procesa todos los cambios de datos que se producen en Identity Vault o una aplicación conectada. Para los eventos que ocurren en Identity Vault, el motor procesa los cambios y emite comandos a la aplicación a través del conector o driver. Para los eventos que ocurren en la aplicación, el motor recibe los cambios del conector, procesa los cambios y emite comandos al Identity Vault. El motor Identity Manager también se conoce como motor de Metadirectorio. El servidor en el que se ejecuta el motor de Identity Manager se conoce como el servidor de Identity Manager.

3. Sistemas Conectados: En NetIQ IDM, un sistema integrado, también llamado sistema o aplicación conectada, es cualquier sistema, directorio, base de datos o sistema operativo cuya información de identidad se desea administrar. Por ejemplo, los sistemas conectados pueden ser una aplicación Microsoft o un directorio LDAP. Un conector, como el conector de Active Directory, proporciona la conexión entre Microsoft Active Directory e Identity Vault. La aplicación debe proporcionar APIs que un controlador pueda usar para determinar los cambios en los datos de la aplicación y efectuar cambios en los datos de la aplicación.

4. Identity Manager Driver (conectores): Los conectores se conectan a las aplicaciones cuya información de identidad se desea administrar. También permite la sincronización de datos y el intercambio entre sistemas. Un driver o conector tiene dos funciones básicas: reportar cambios de datos (eventos) en la aplicación al motor de Identity Manager, y llevar a cabo cambios de datos (comandos) enviados por el motor de Identity Manager a la aplicación. Estos también permiten la sincronización de datos y el intercambio entre sistemas.

5. Remote Loader: Este componente es el encargado de la comunicación entre los conectores de integración de las distintas aplicaciones y el motor de Identity Manager. Si la aplicación a integrar se ejecuta en el mismo servidor que el motor de Identity Manager, se puede instalar el componente de remote loader en dicho servidor. Sin embargo, si la aplicación no se ejecuta en el mismo servidor que el motor de Identity Manager, se debe instalar el remote loader en el servidor de la aplicación a integrar. Para ayudar con la carga de trabajo, se puede instalar el remote loader en un servidor independiente de los servidores que tienen el servidor de aplicaciones y el servidor de Identity Manager.

6. Identity Applications: Las Identity Applications son un conjunto interconectado de aplicaciones Web basadas que permiten gestionar las cuentas de usuario y los permisos asociados a la amplia variedad de funciones y recursos disponibles para los mismos. Desde ellas se pueden configurar las diferentes aplicaciones de identidades para que proporcionen soporte de autoservicio para sus usuarios, como solicitar

roles o cambiar sus contraseñas. También se pueden configurar flujos de trabajo para mejorar la eficiencia en la gestión y asignación de funciones y recursos. Entre las principales herramientas se encuentran:

- NetIQ iManager [15]: es una consola de administración web de la solución identity manager, siendo único punto de administración para objetos, esquemas, particiones y réplicas de NetIQ eDirectory, etc.
- NetIQ Identity Manager Dashboard sirve como portal de entrada principal a las aplicaciones de identidad, permitiendo que los usuarios puedan auto-administrar su perfil y contraseña, solicitar permisos para roles, recursos o procesos. Según el tipo de permisos que se posean, también se puedan aprobar solicitudes de acceso de los usuarios comunes, revocar accesos, etc.
- SSPR (Self Service Password Reset): aplicación web de administración de contraseñas. Este sistema elimina la dependencia de los usuarios de la ayuda de los administradores para cambiar las contraseñas, ya que proporciona un sistema de autoservicio para que los mismos autogestiones sus claves.

Capítulo 5

Implementación del sistema Identity Manager

El presente capítulo contiene el desarrollo de todas tareas de implementación realizadas en la implementación de la solución de Identity Manager en el organismo.
Entre las configuraciones realizadas se encuentran la instalación y configuración de todos los servicios en los servidores que componen la solución de Identity Manager. Se muestra a través de ejemplos con figuras los diferentes pasos de la implementación realizada.

5.1. Tareas de implementación realizadas

La instalación del entorno de Identity Manager se realizó en forma distribuida en distintos servidores con sistema operativo Linux.
Todo la solución de Identity Manager se puede instalar en forma básica que incluye todos los componentes de Identity Manager en una sola computadora.
Esta implementación de todo en uno es adecuada sólo para la instalación de Identity Management Proof-of-Concept (POC) o para entornos de desarrollo.
En el organismo, para dicho entorno se propone la instalación de todos los componentes en un solo servidor en un ambiente virtualizado, como se muestra en la figura 5.1:

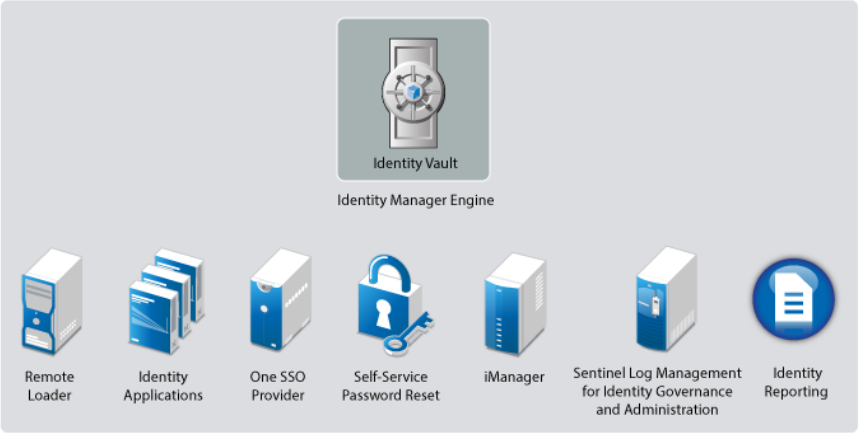


Figura 5.1: Instalación para PoC o desarrollo de IDM [16]

Para las etapas de Test y Producción se han instalado los componentes en distintos servidores, cada uno con los servicios requeridos según la necesidad.
Como se muestra en la figura 5.2, en los casos de Test y Producción , se instalaron:

- Server 1: Componente de Identity Manager Engine, motor del sistema que incluye el sistema de repositorio de usuarios MetaDirectorio (Identity Vault).
- Server 2: Los servicios de Remote Loader, Identity Applications, SSPR y iManager.
- Server 3: Sistema de Logs Sentinel y Sistema de reportes.

La diferencia entre los sistemas de test y producción radica principalmente en la redundancia de ciertos servicios principales (ver Anexo para más información).

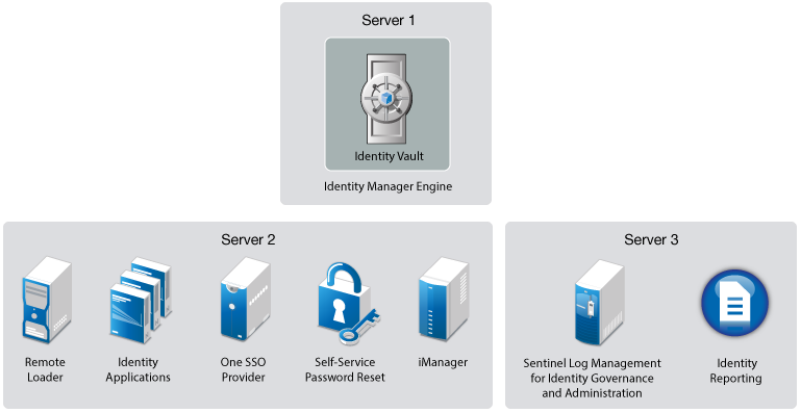
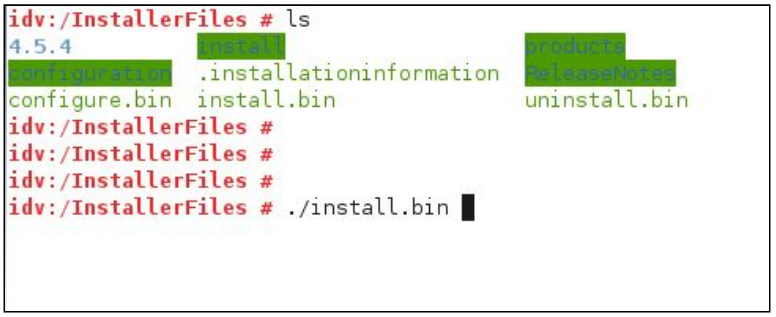


Figura 5.2: Servidores de la solución IDM con sus servicios [16]

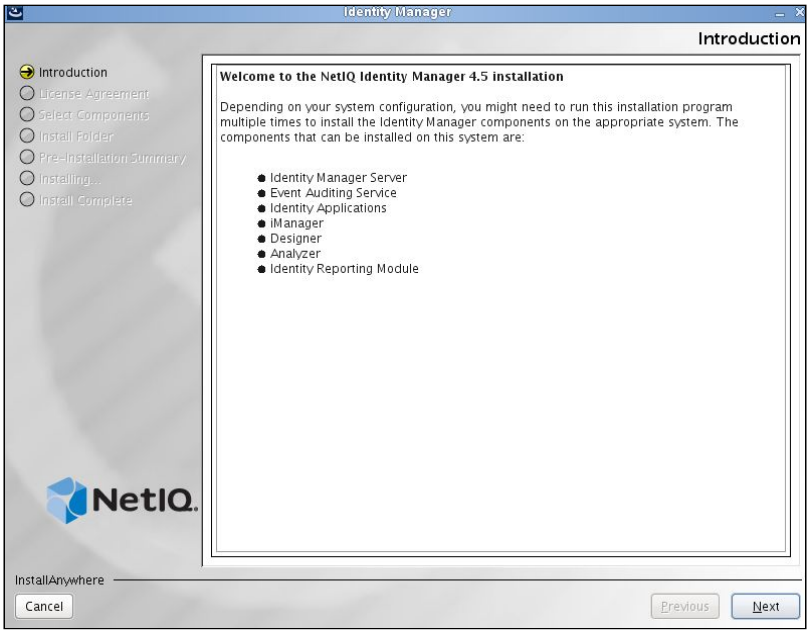
5.2. Proceso de Instalación y de Configuración

El producto NetIQ Identity Manager provee un script de instalación para instalar ya sea componentes individuales como un grupo de componente en dos fases separadas: la instalación y la posterior configuración.
Este script de instalación, install.bin, se encuentra en una imagen de disco .iso del producto.
Como muestra para esta tesina se mostrará la instalación en servidores con interfaz gráfica (la instalación también puede hacerse por consola).

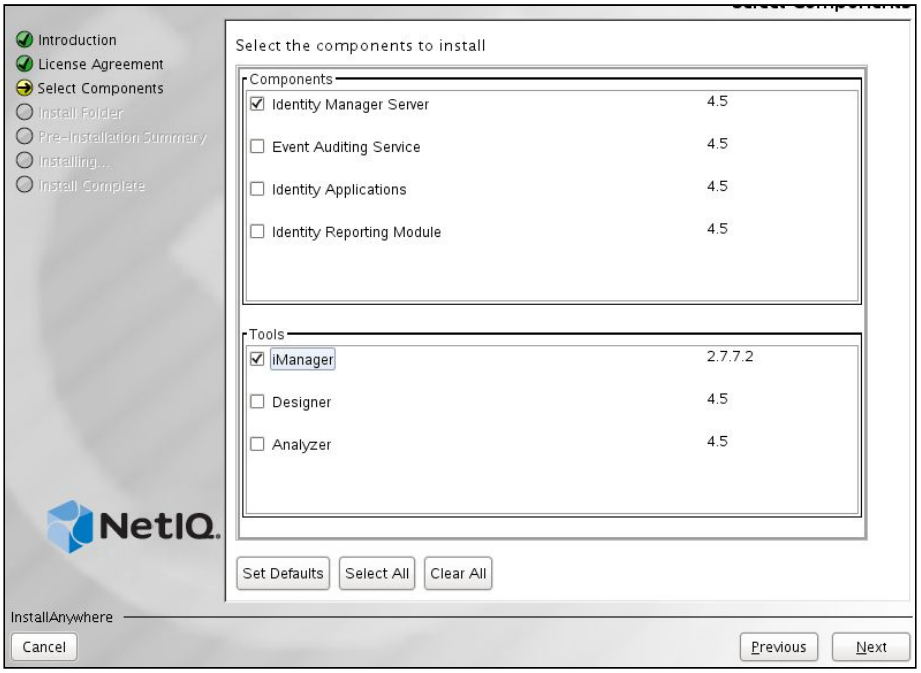
1. Proceso de instalación es inicialmente ejecutando el script “install.bin”



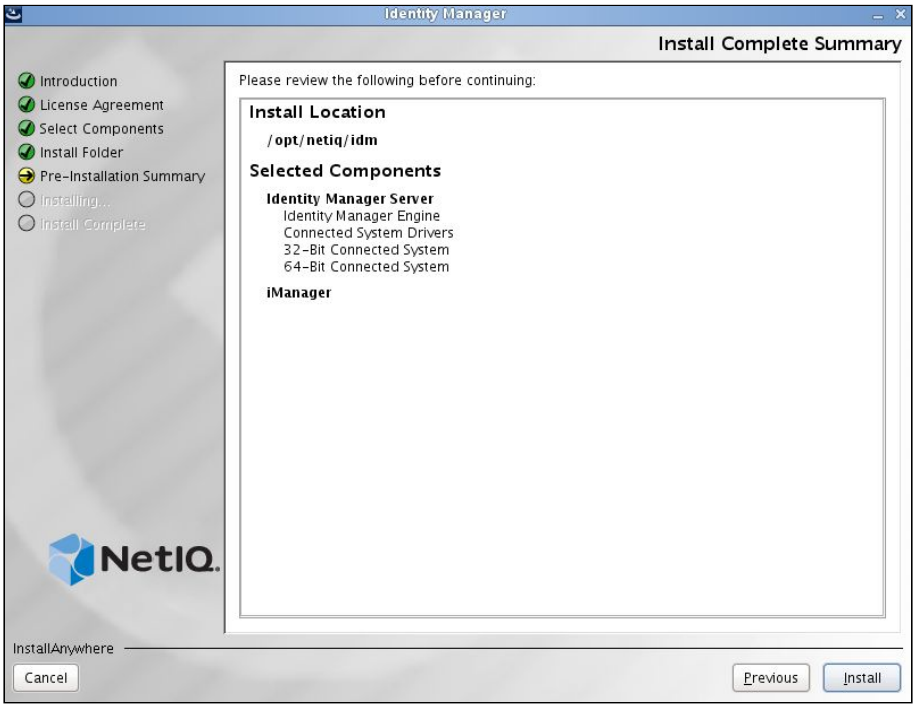
2. Luego de la ejecución del script de instalación, se muestra la información de los productos que pueden ser instalados:



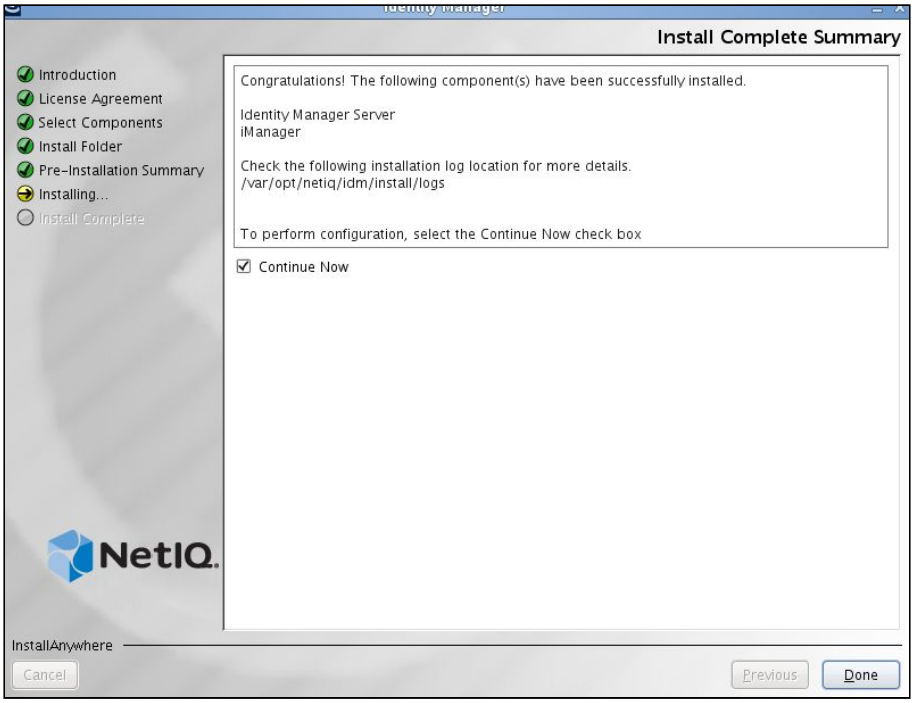
3. A continuación se selecciona los servicios a Instalar, en nuestro caso en el servidor numero 1 seleccionamos la opción de Identity Manager Server y de la consola de administración iManager:



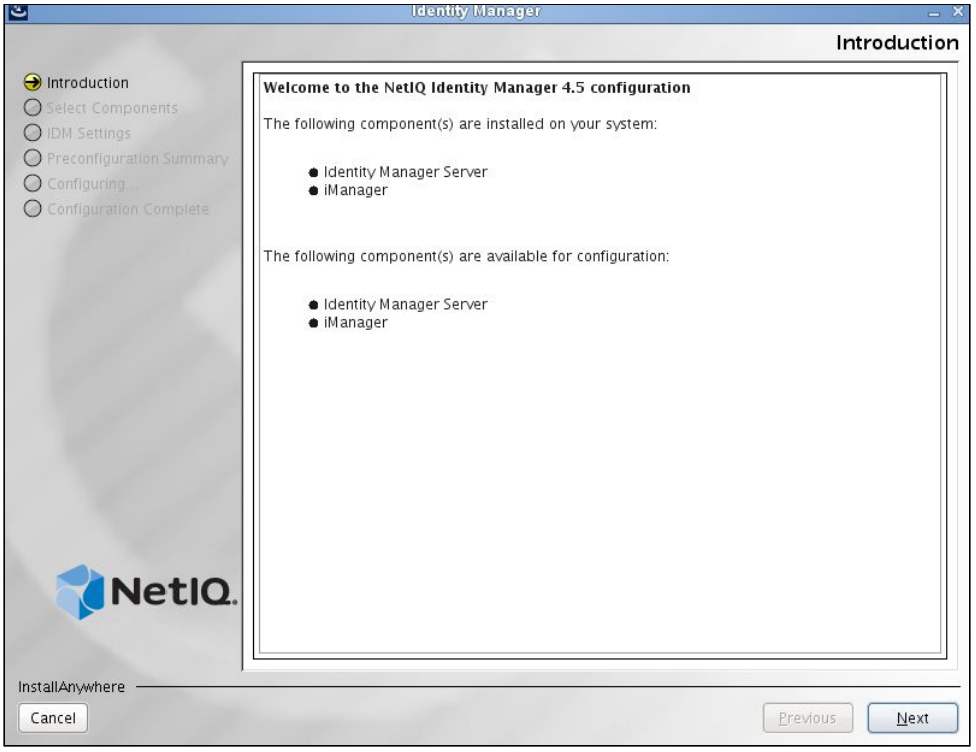
4. Pantalla informativa con los productos seleccionados:



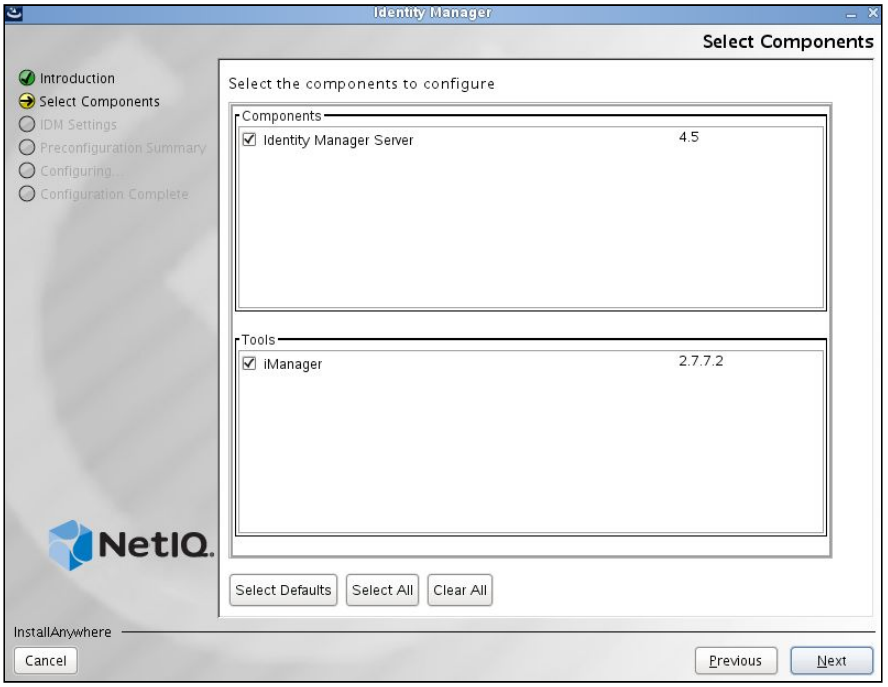
5. Pantalla informativa que informa el fin de la instalación:



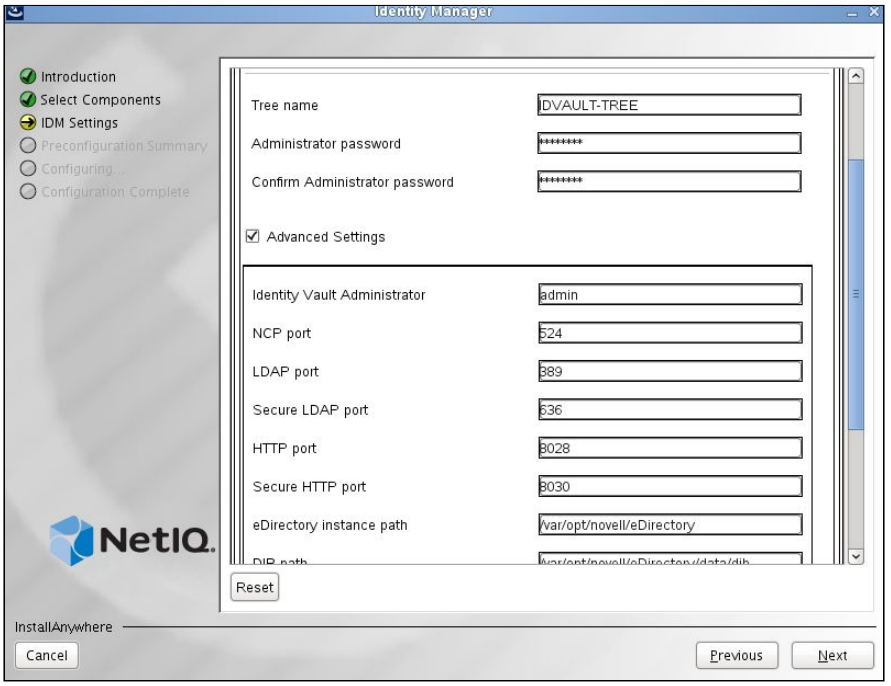
6. Luego de la instalación, comienza el proceso de configuración



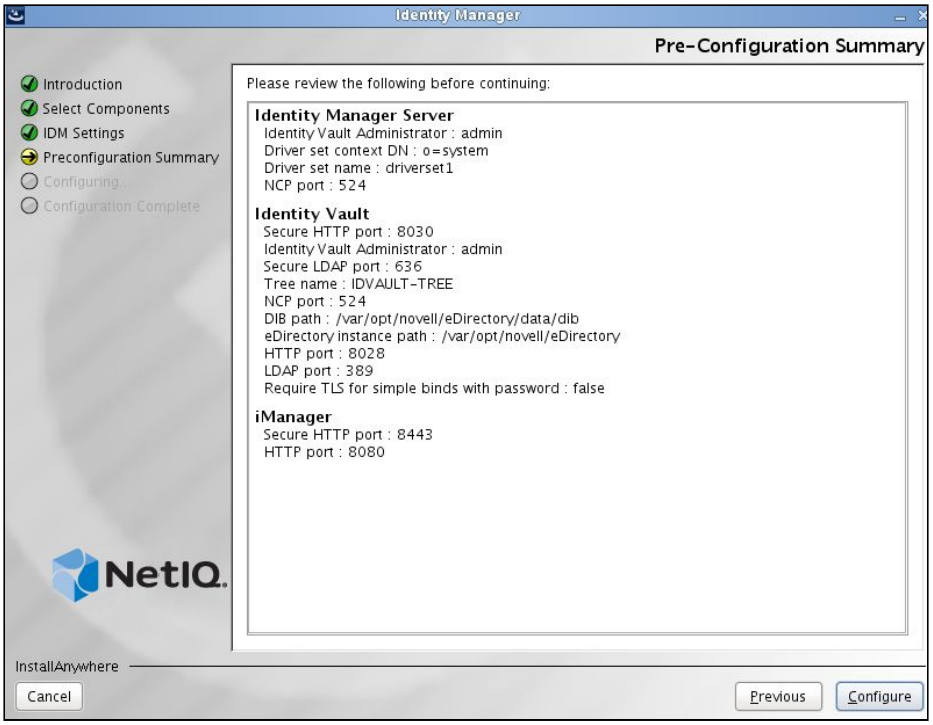
7. Selección de componentes a configurar:



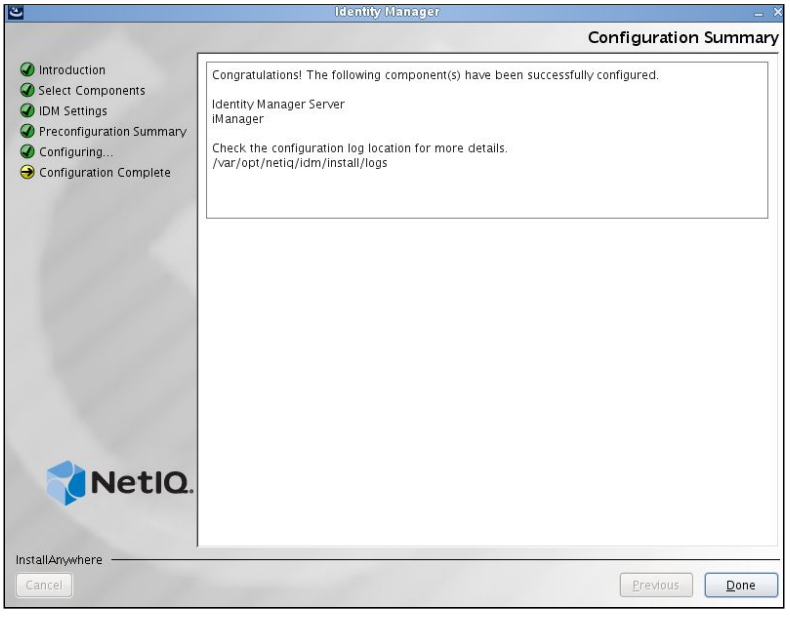
8. En la configuración de Identity Manager Server, se configuran las opciones como nombres de árbol de directorio, passwords de accesos, puertos y paths de la instalación:



9. En la finalización se muestra la información con la configuración definida:



10. Por último la información de la finalización de la instalación de los componentes previamente seleccionados:



5.3. Identity Applications

En el siguiente apartado se muestran las aplicaciones web que permiten la administración del sistema IDM.
El sistema de gestión de identidades posee distintas consolas web llamadas Dashboards, que permiten ya sea para los usuarios finales, como para los administradores de la plataforma poder acceder al sistema de gestión de identidades.
A continuación, se mostrarán pantallas de estas consolas, mostrando características básicas y funcionalidades.

5.3.1 Identity Manager Dashboard

Identity Manager Dashboard es el portal de entrada para los usuarios finales. Desde esa consola los usuarios principalmente realizan tareas relacionadas con su propia identidad (reseteo y cambio de password), como además solicitar y ver estados de solicitudes de accesos realizados.
Entonces, como actividades principales se destacan las siguientes:

- Gestión del perfil del usuario
- Gestión de contraseña
- Visualización del Organigrama
- Accesos a las peticiones pendientes de acciones, como aprobarlas o denegarlas
- Solicitar permisos
- Revisar el estado y el historial de las peticiones realizadas
- Delegar sus tareas a otros usuarios

Desde este panel se provee una vista rápida de la información del usuario, como las tareas, permisos y requerimientos.

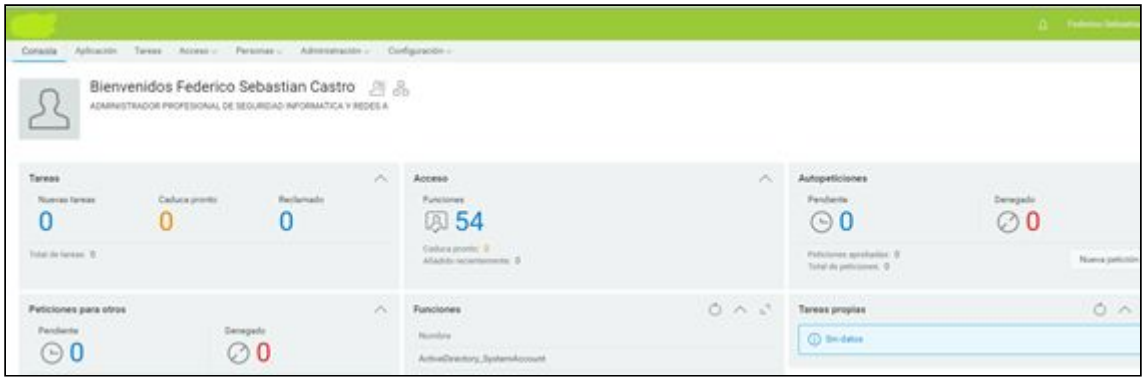


Figura 5.3: Portal inicial Dashboard de IDM

Desde allí podemos ver las peticiones a accesos a sistemas realizados y el estado de las mismas (si están pendientes de aprobación o se han denegado), los accesos que uno ya tiene asignado y funciones que tiene otorgadas dentro del organismo.
Por ejemplo, dentro del apartado de “Aplicaciones”, el usuario puede lanzar aplicaciones por defecto, pedir acceso cambiar su perfil, etc.

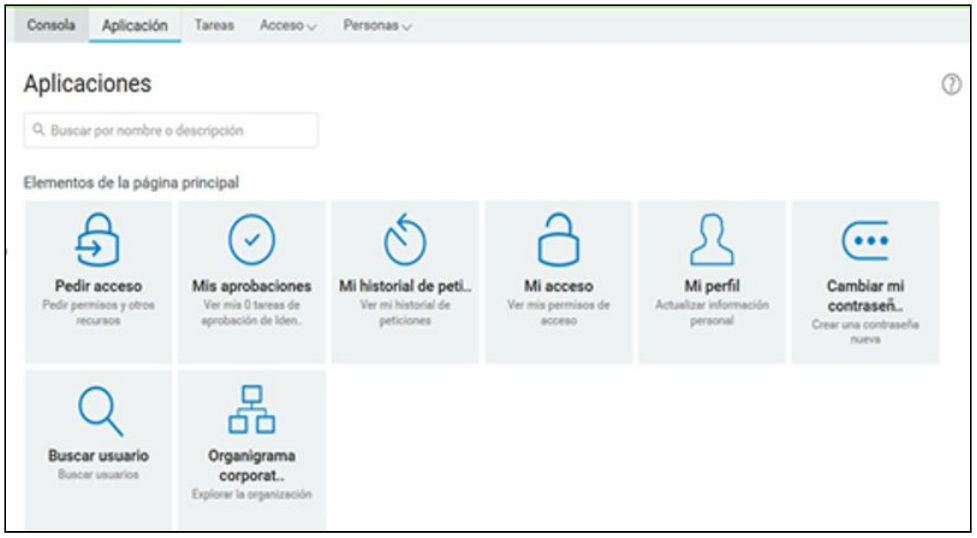


Figura 5.4: Sección aplicaciones

Por ejemplo, para solicitar acceso, se selecciona nueva petición de lo que el usuario requiera y espera a su aprobación.

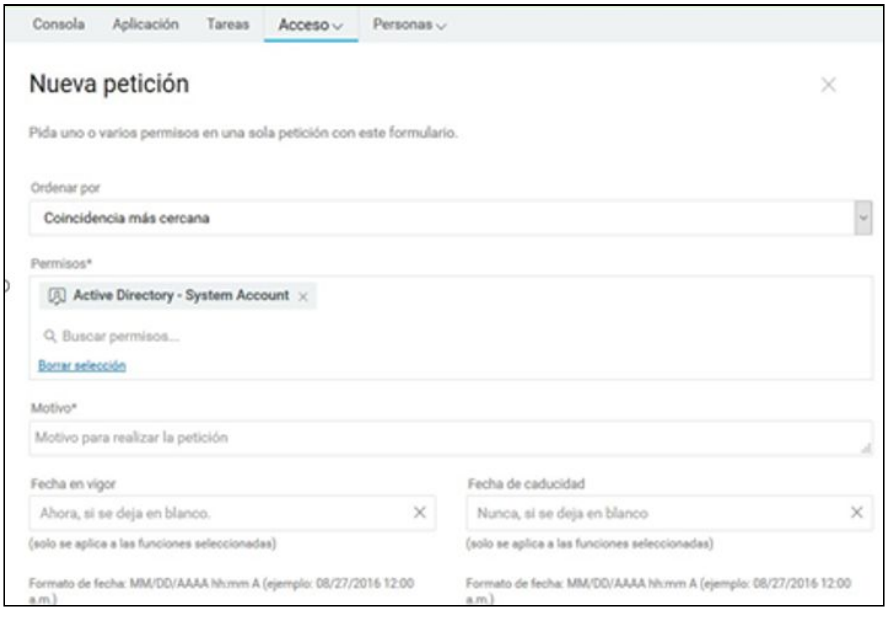


Figura 5.5: Sección nueva petición de acceso

Dentro del apartado de Personas, permite la visualización de usuarios y grupos y el organigrama del organismo.

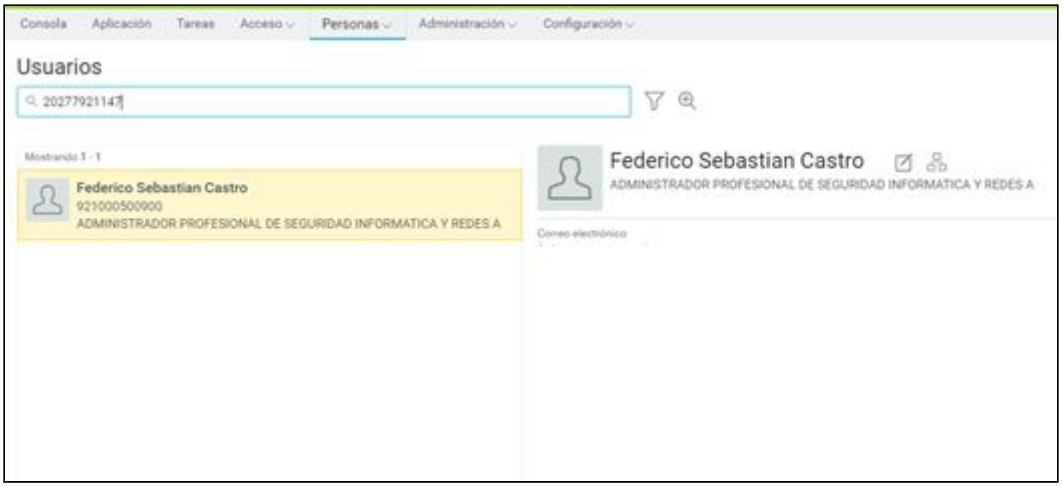


Figura 5.6: Sección con información de usuarios

También permite la búsqueda de usuarios, grupos, equipos de trabajo, etc.

5.3.2. Identity Applications Administrations - iManager

La consola de administración NetIQ iManager [15] es una consola de administración web que proporciona acceso personalizado a las utilidades de administración de red y al contenido.

Desde esta consola iManager proporciona lo siguiente:

- Punto único de administración para objetos, esquemas, particiones y réplicas de NetIQ eDirectory
- Punto único de administración para muchos otros recursos de red.
- Gestión de muchos otros productos NetIQ y Novell utilizando los complementos de iManager
- Servicios basados en roles para administración delegada

A continuación, se muestra la pantalla de acceso al sistema iManager.
Este sistema es por donde el sector de administración de seguridad del organismo administra configura toda la plataforma IDM.

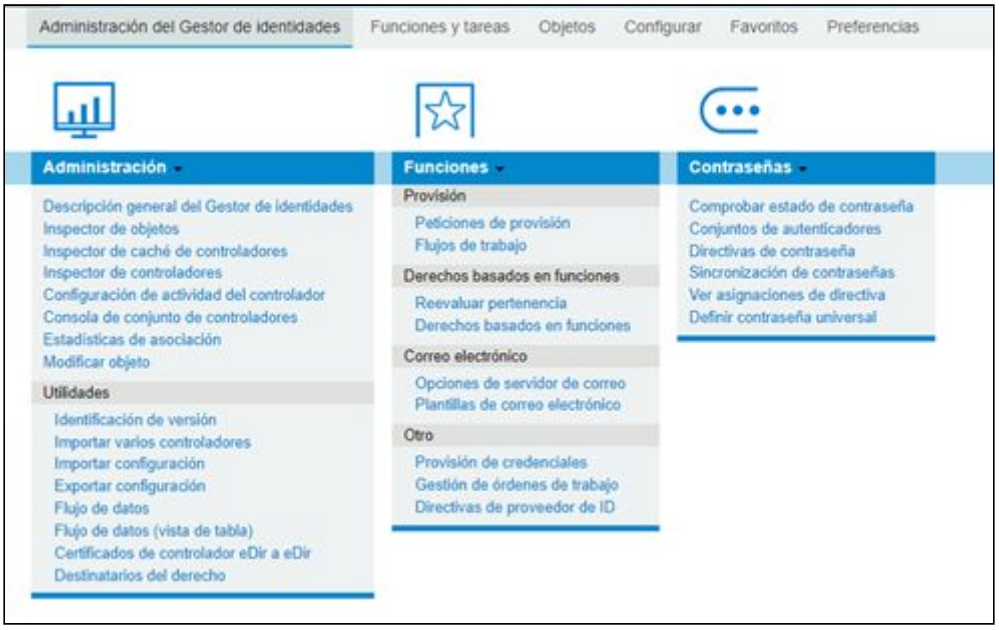


Figura 5.7: Consola de administración iManager

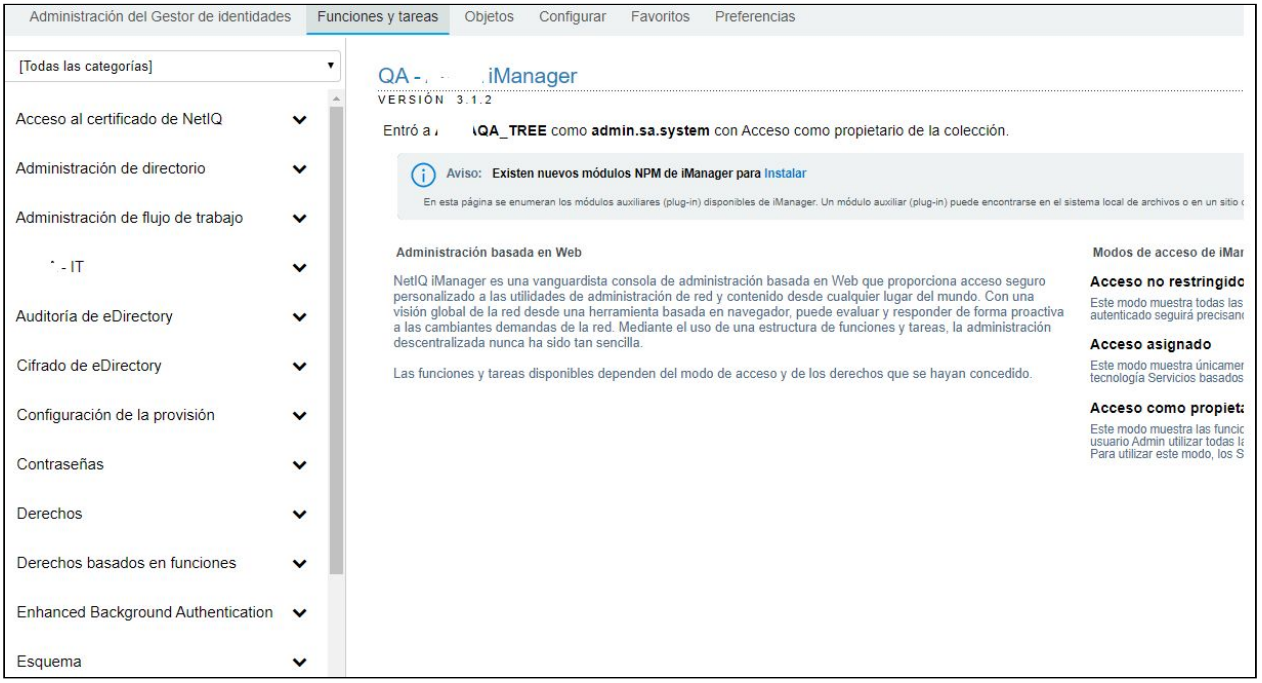


Figura 5.8: Sección Funciones y tareas

Entre diversas configuraciones podemos ver manejo de certificados digitales para comunicación segura entre los componentes, administración del directorio LDAP, administración de flujo de trabajo.

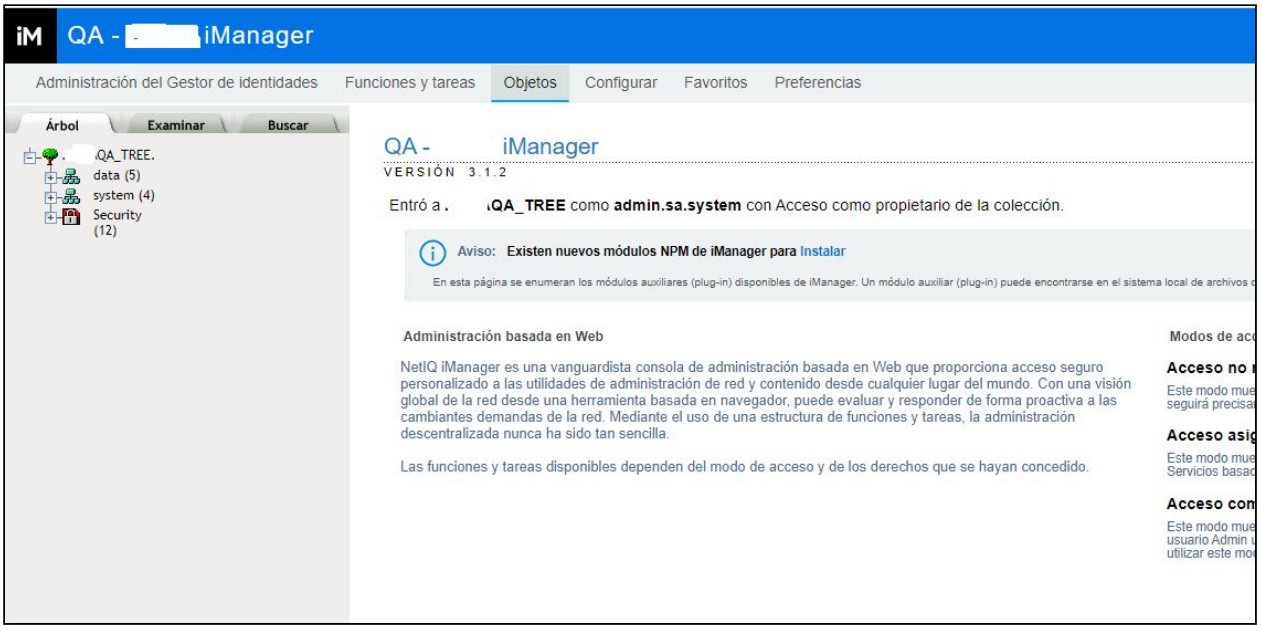


Figura 5.9: Administración de árbol de directorio LDAP

A su vez, como se verá en la próxima sección, desde esta consola de administración se controlan los conectores de integración con las diversas plataformas de identidades a integrar, ya sean Active Directory, LDAP, Base de datos, etc.

5.4 Integraciones

Como se explicó con anterioridad, la solución de Identity Manager IDM de NetIQ funciona integrando los diversos sistemas y repositorios de usuarios con un metadirectorio principal.
Para poder mantener sincronizada y actualizar la información de los usuarios, IDM utiliza los conectores de integración para poder comunicarse con los diferentes sistemas a integrar y así poder hacer un tratamiento de eventos según se requiera.
Estos conectores de integración permiten conectar la información entre las diferentes aplicaciones comerciales, directorios ldaps y bases de datos.
El motor de Identity Manager procesa todos los cambios de datos que se producen en Identity Vault o en una aplicación conectada. Para los eventos que ocurren en el Identity Vault, el motor procesa los cambios y emite comandos a la aplicación a través del conector.
Para los eventos que ocurren en una aplicación, el motor recibe los cambios del conector, procesa los cambios y emite comandos a Identity Vault.
Por lo tanto, los conectores de integración conectan el motor de Identity Manager a las aplicaciones.

Inicialmente el sistema no posee ningún conector dentro de su conjunto de conectores (llamados Driver Set), por lo que según el tipo de sistema que se quiera conectar, ya sea una base de datos, un repositorio de directorio LDAP o cualquier otro sistema que posea su conector definido, se debe instalar y configurar específicamente. En la figura 5.10 vemos el inicio de un sistema IDM sin ningún conector configurado en el mismo.

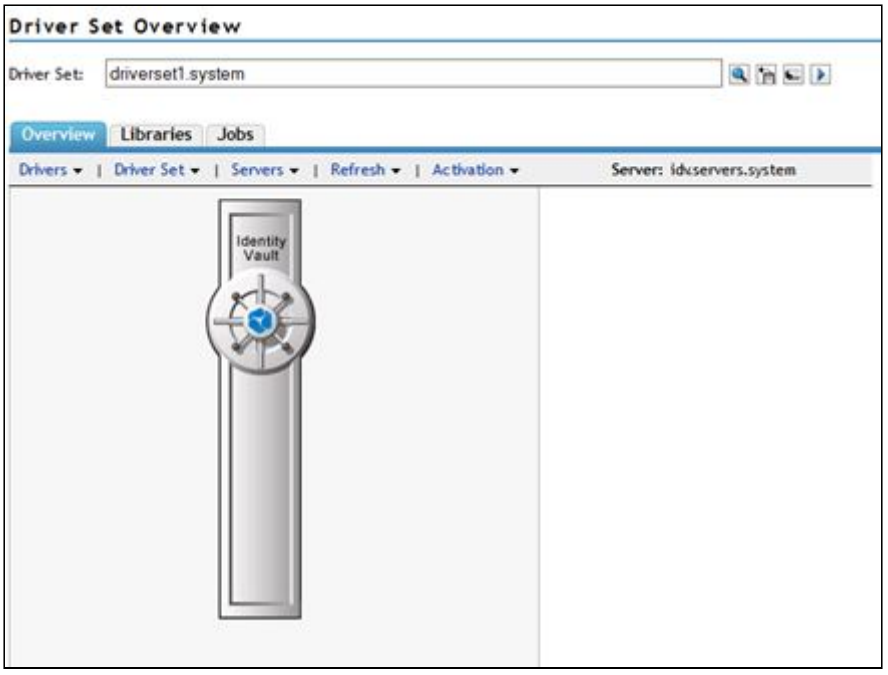


Figura 5.10: *Imagen inicial del sistema IDM sin ningún conector instalado*

Cada uno de estos conectores se instala y configura utilizando el software propio de NetIQ llamado Designer [22]. Esta es una herramienta de desarrollo que permite programar, instalar y configurar cada uno de los conectores que se deseen instalar. a su vez que permite programar la lógica que tendrá y cómo procesa cada uno de los eventos que se procesan en el motor de Identity Manager.

Figura 5.11: Designer de NetIQ [22]

En el marco de esta tesina se hará una demostración de la instalación y configuración de dos de los conectores principales para un funcionamiento general de una solución de Identity Manager.
El primero es un conector con un sistema de Recursos Humanos externo, el cual se registran los usuarios, se dan de alta, baja y modificación. Este es un conector del tipo de base de datos (en el caso de esta tesina se decidió el conector de BD de Postgresql).
El segundo conector que se detalla es el de conexión con un sistema de repositorio de usuarios LDAP (en este caso se eligió el sistema de LDAP de la empresa Microsoft Active Directory), donde se guardan la información interna de los usuarios del organismo.

5.4.1. Conector de integración con plataforma Recursos Humanos HR

Inicialmente, el sistema de Identity Manager está vacío, eso significa que el repositorio de usuarios interno, el Identity Vault está sin ningún dato o usuario cargado.
Para poblarlo con usuarios de una fuente autorizada de Recursos Humanos, se debe configurar un conector especifico para eso.
En el ejemplo a continuación, se simula una aplicaciones de administración de recursos humanos, que da de alta, baja y modifica a usuarios.
En el ejemplo a continuación, el sistema externo de recursos humanos guarda la información de los empleados en una base de datos relacional, por lo tanto el conector que se utiliza para conectar con un sistema de recursos humanos (HR de ahora en mas) es un conector de este tipo.
En el ejemplo, este conector de HR toma la información proveniente de una vista denominada *hr_pers* dónde ocurrirán los eventos de alta, modificación y baja de usuario.

Cada cambio que se realice en dicha vista, el conector procesa dicho cambio y modificara la información relacionada con el usuario dentro del Metadirectorio (Identity Vault).

A continuación se muestra un sistema de HR ficticio que sirve para demostración de un sistema de este tipo.
Este sistema es una aplicación web, y en el caso de demostración, es la fuente autorizada para toda la creación de identidad. La aplicación de recursos humanos utiliza una base de datos SQL Postgre que publicará eventos en Identity Vault.
En la figura 5.12 y 5.3 vemos el ejemplo del inicio de la aplicación web de HR.

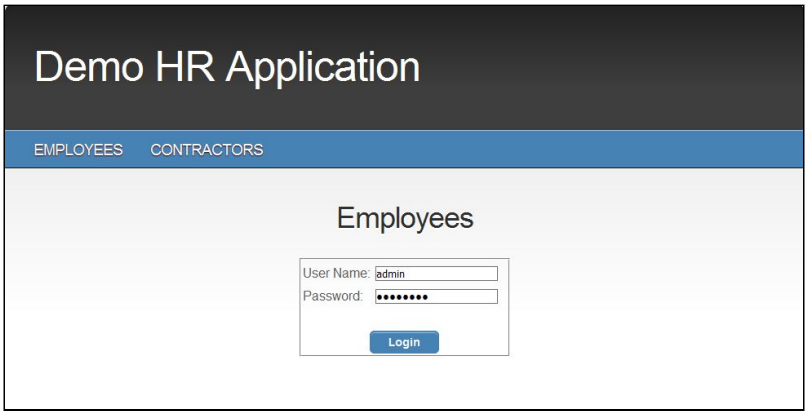


Figura 5.12 : Aplicación DEMO de carga de usuarios

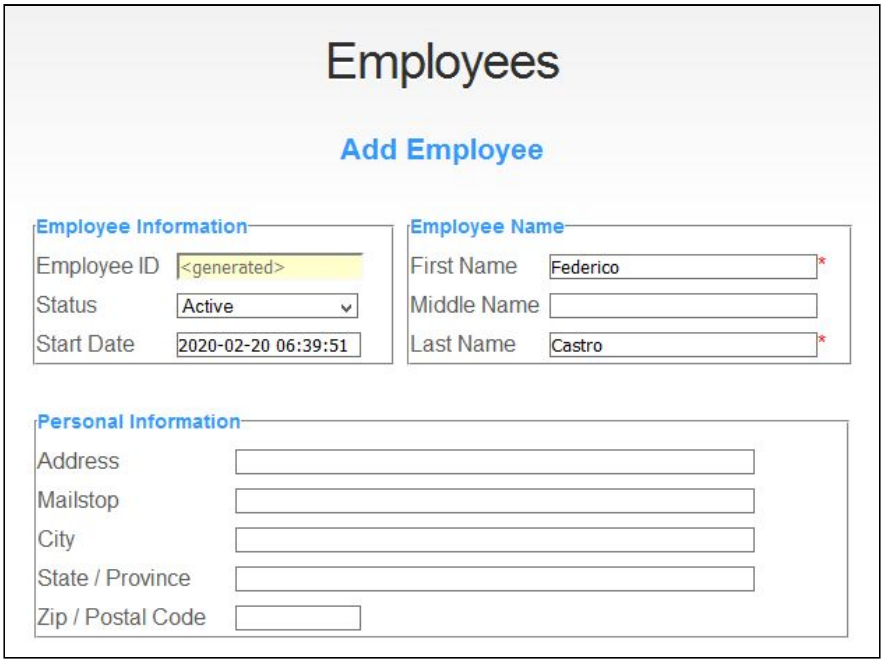


Figura 5.13: Carga de datos de usuarios

La aplicación de muestra es muy simple, pero sirve como ejemplo para ver qué sucede cuando se da de alta un usuario. Por ejemplo, cuando agregamos un usuario, el sistema

guardada la información del mismo guardada en su propia base de datos. En la figura 5.14 vemos el usuario “Federico Castro” agregado efectivamente a la base:

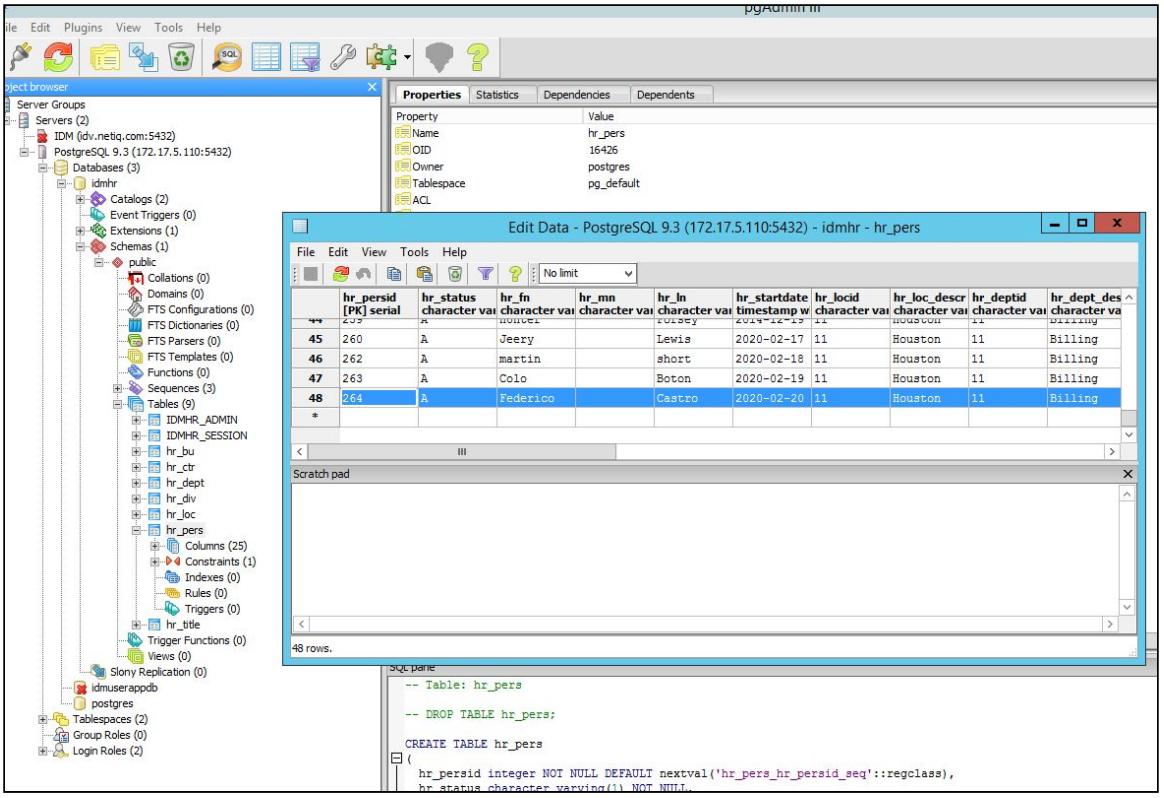


Figura 5.14: Vista de BD Postgre con datos de los usuarios

Luego, como vimos, la instalación de cada conector y programación de su funcionalidad se realiza mediante la herramienta Designer.
En la siguiente figura vemos el Designer que nos muestra un Identity Vault inicial sin ningún conector instalado.

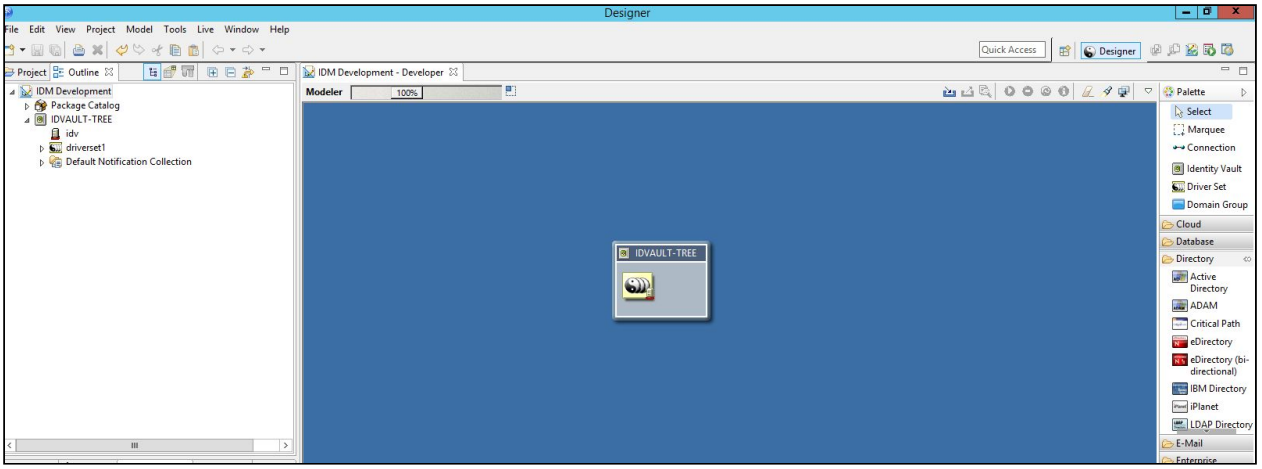


Figura 5.15: Designer sin ningun driver instalado

Cuando se instala un nuevo conector, según el tipo de conector que se quiera instalar lleva consigo una configuración particular.
En las siguientes figuras vemos por ejemplo la carga de la información básica para un conector de base de datos Postgre, donde se cargan inicialmente datos básicos de configuración como por ejemplo, dirección IP de la base a conectar, puertos, nombre de la base donde se guardan los datos, etc.

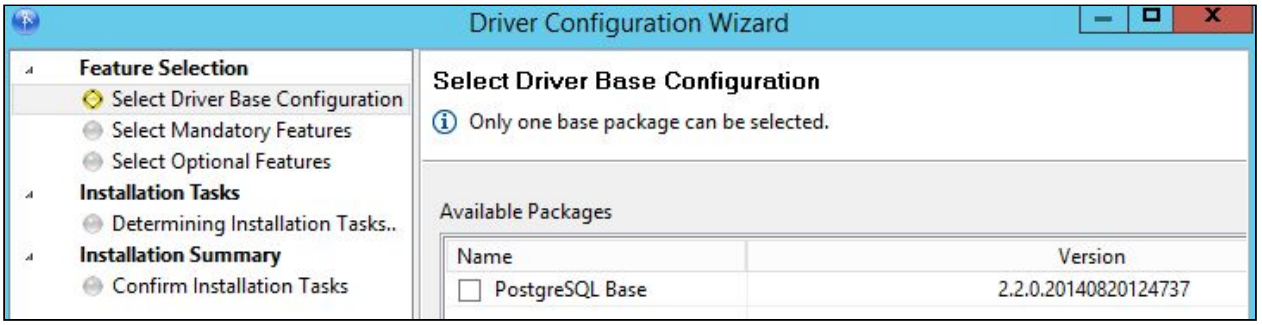


Figura 5.16: configuración de Postgre

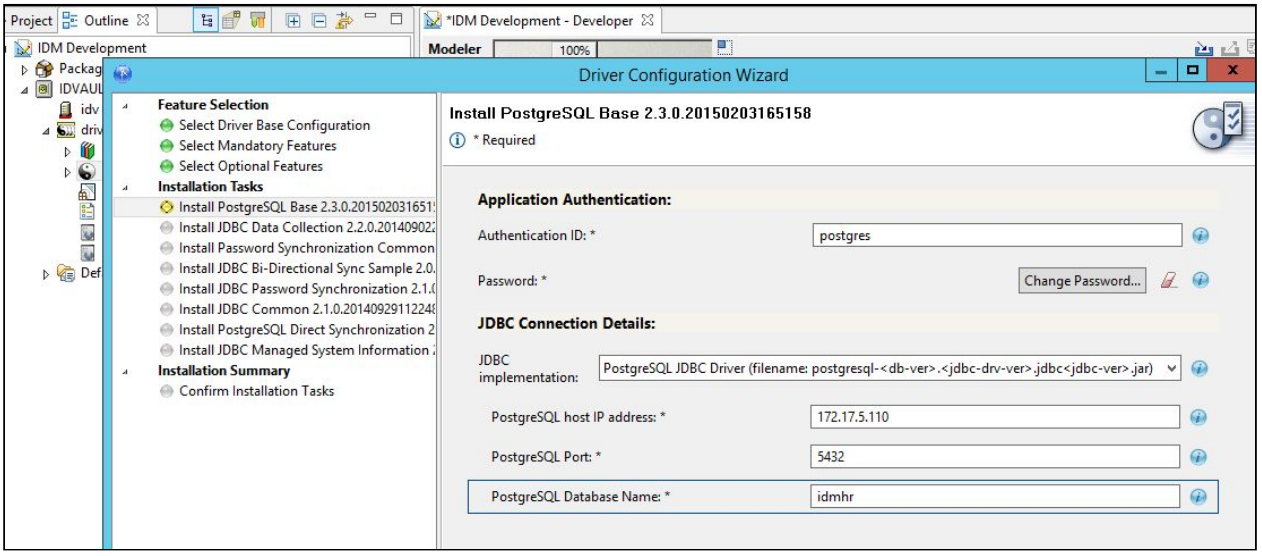


Figura 5.17: Parámetros inicial de BD

En la siguiente figura vemos que una vez instalado un conector, se muestra la conexión que hay entre dicho conector y el Identy Vault, esto significa que ya se encuentran integrados ambos sistemas. De ahora en mas solo queda configurar como se tratan los eventos que surgen en cada uno de ellos y qué operación se realiza ante dicho evento.

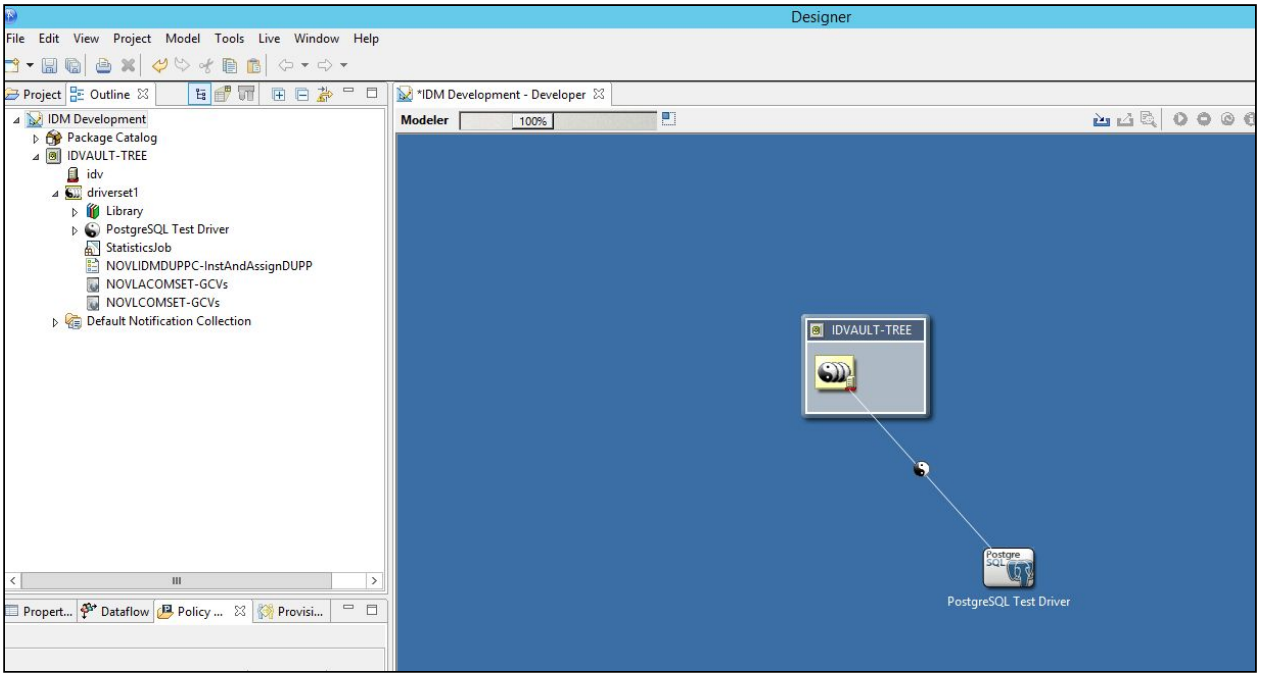


Figura 5.18: Driver Postgre conectado

Los pasos siguientes en la configuración que se deben realizar para efectivamente integrar este conector con el sistema de Identity Manager, por ejemplo: Mapear atributos del Identity Vault (que como dijimos con anterioridad es el repositorio de información de todo el sistema Identity Manager) con atributos de la base de datos de HR.
En la siguiente figura se muestra como se mapea a un nombre de tabla específico de usuarios llamada *hr_pers*.

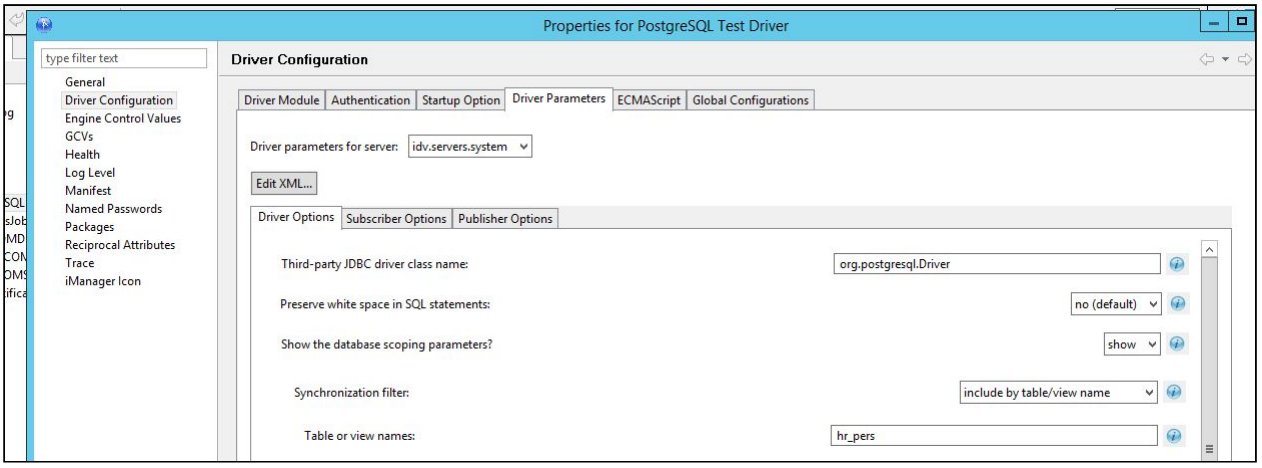
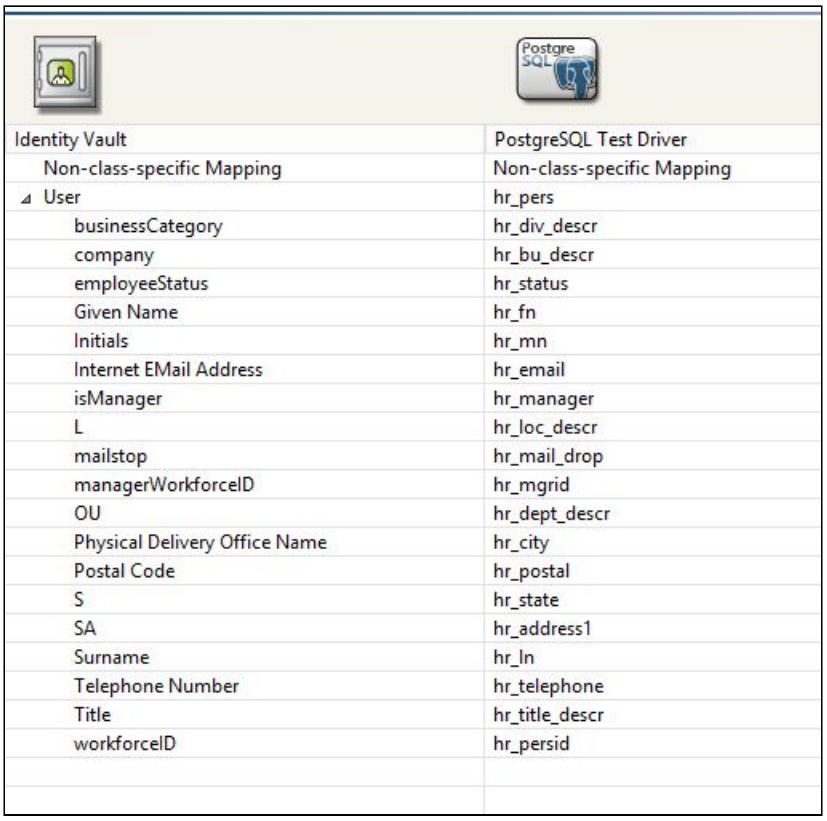


Figura 5.19: Mapeo de usuarios entre Identity Vault y BD

En la siguiente figura, se muestra como ejemplo los distintos mapeos de los atributos entre los diferentes sistemas Identity Vault y la base Postgre de HR:



Identity Vault	PostgreSQL Test Driver
Non-class-specific Mapping	Non-class-specific Mapping
◢ User	hr_pers
businessCategory	hr_div_descr
company	hr_bu_descr
employeeStatus	hr_status
Given Name	hr_fn
Initials	hr_mn
Internet EMail Address	hr_email
isManager	hr_manager
L	hr_loc_descr
mailstop	hr_mail_drop
managerWorkforceID	hr_mgrid
OU	hr_dept_descr
Physical Delivery Office Name	hr_city
Postal Code	hr_postal
S	hr_state
SA	hr_address1
Surname	hr_ln
Telephone Number	hr_telephone
Title	hr_title_descr
workforceID	hr_persid

Figura 5.20: mapeo entre sistema Identity Vault y Postgre HR

Una vez que se setean los mapeos entre el IDM y el sistema de base de datos a integrar, se pueden programar las acciones que se ejecutan ante un evento en particular. En la figura 5.21 vemos por ejemplo que ante ciertas condiciones (ej. si la operación es alta, si es un usuario, etc.), la acción a hacer es setear el password por default al usuario (en este caso “netiq000”).

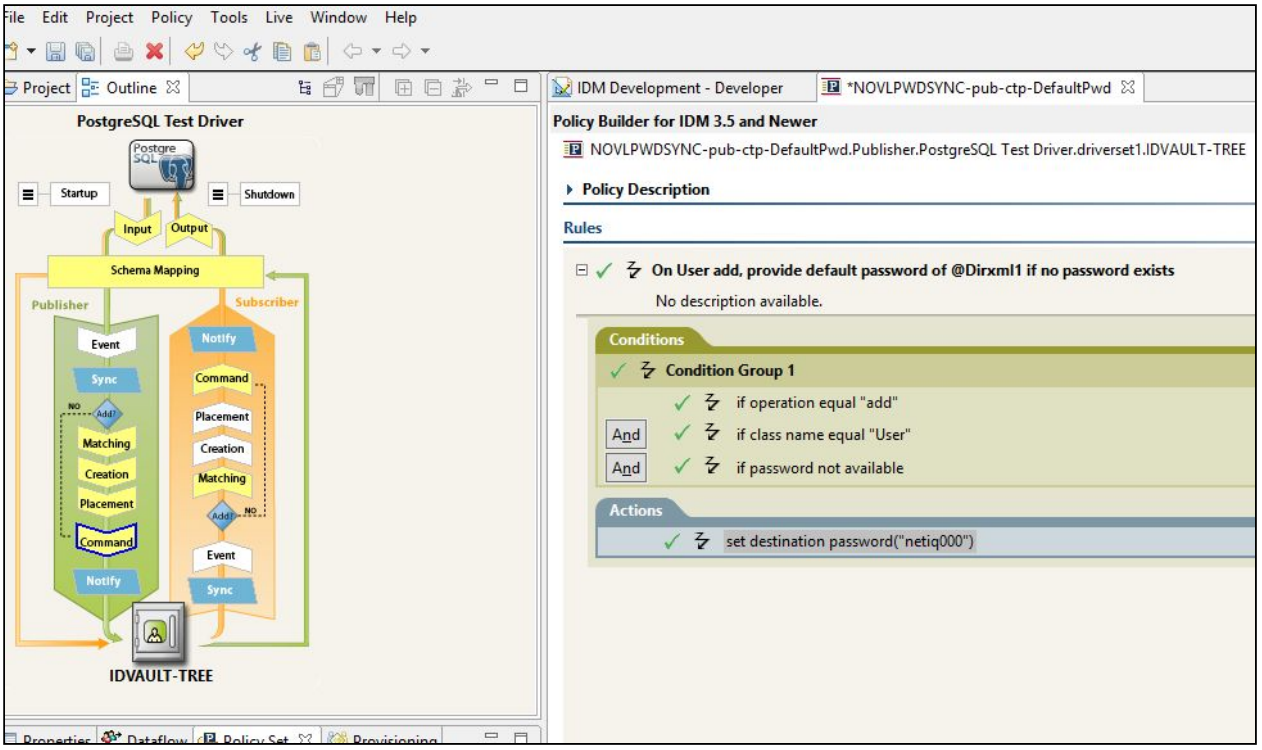


Figura 5.21: Programación de eventos

Luego de configurar el conector y programar los eventos que se realicen en la base de datos, en la herramienta de administración iManager podemos ver que una vez inicializado el conector, como se han poblado los usuarios en el repositorio de Identity Manager, con los usuarios guardados en la base de datos de HR Postgre, como se muestra en la figura 5.22:

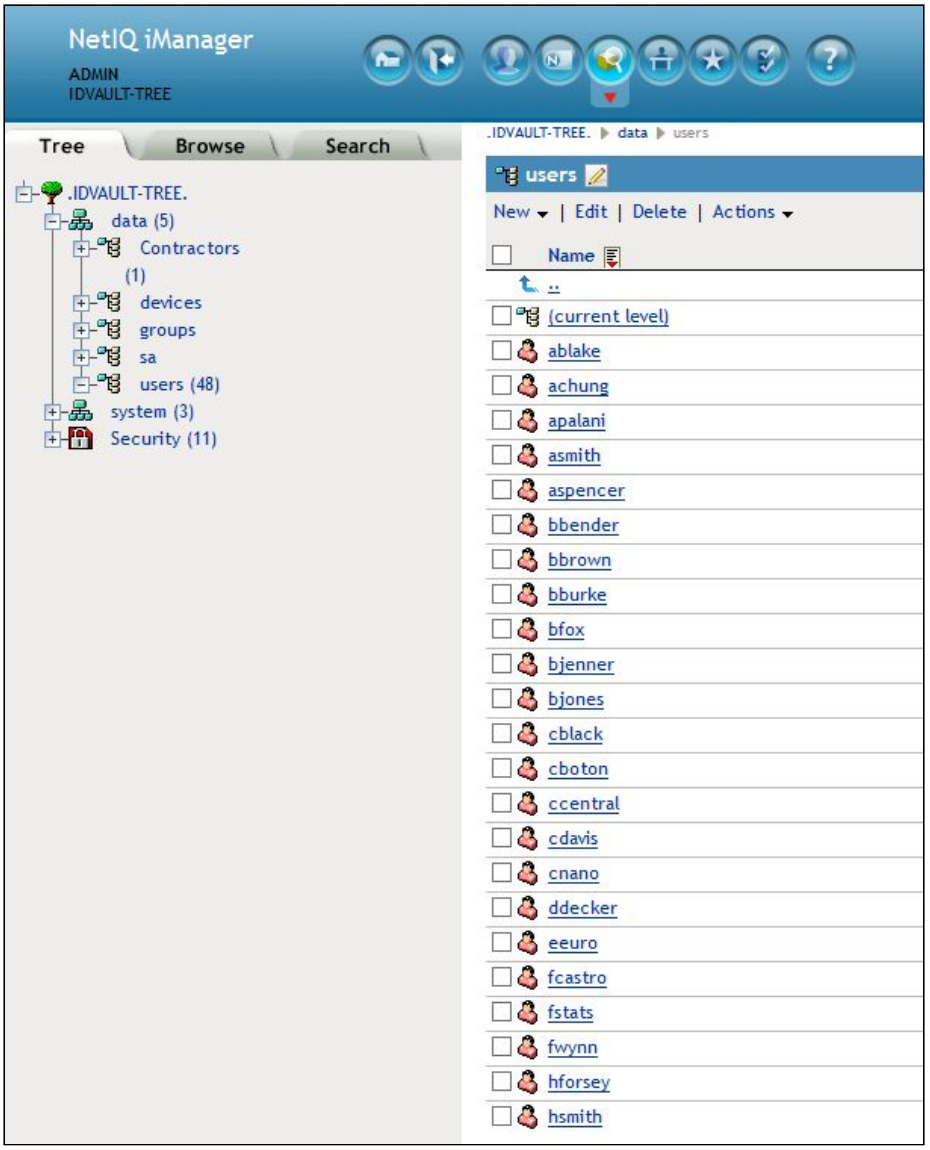


Figura 5.22: iManager usuarios agregados

Por último, una vez finalizado dicha configuración y programación del conector, desde la misma herramienta iManager vemos el estado del mismo, si funciona correctamente, pudiendo también detenerlo o inicializarlo según se requiera (figura 5.23).

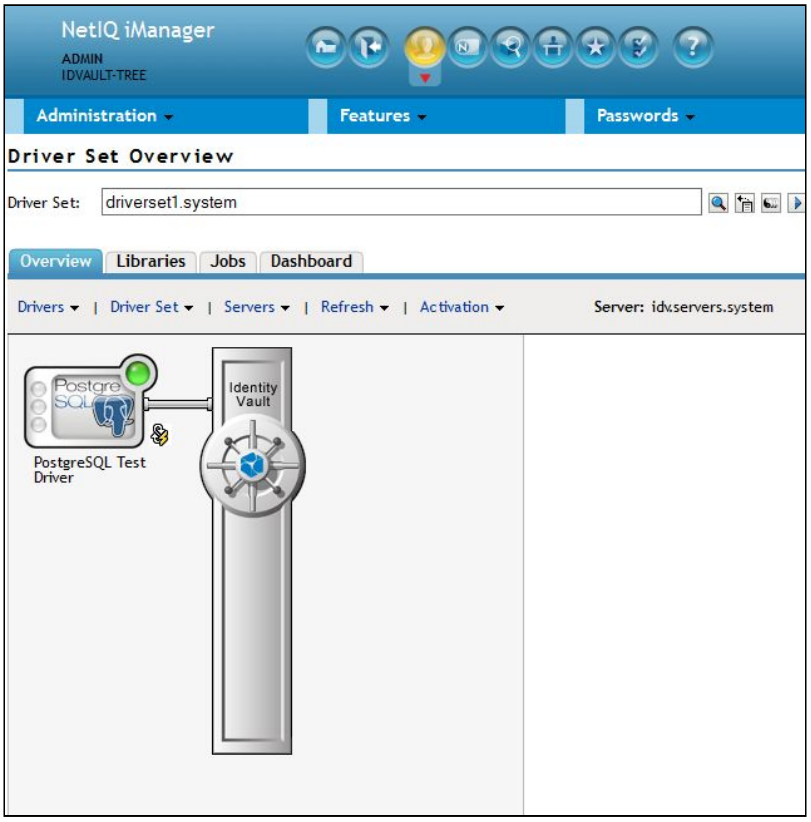


Figura 5.23: iManager conector funcionando.

5.4.2. Conector de plataforma Active Directory

El sistema de repositorio de usuarios Active Directory es por lo general uno de los más comunes repositorios donde se guarda y gestiona los usuarios y grupos.
Desde dicho sistema, se autentican varios sistemas, ya sean correo, permisos file servers, accesos a sistemas web, etc.
Es por eso que este conector es uno de los principales, ya que es el encargado de mantener sincronizados los datos entre el repositorio Active Directory y el IDM.
La integración con Active Directory, al ser un sistema de tipo Microsoft con drivers especiales, la integración se realiza mediante la utilización del componente "Remote Loader", el cual es el encargado de la transmisión de los eventos entre el Metadirectorio y el Active Directory, ejecutando el driver (ADDriver.dll) en forma local al Member Servers.
La instalación del conector Active Directory se hace de la misma manera que el mostrado para la base Postgre, eligiendo el componente desde los conectores disponibles en la herramienta de desarrollo Designer, como se ve en la figura 5.24:

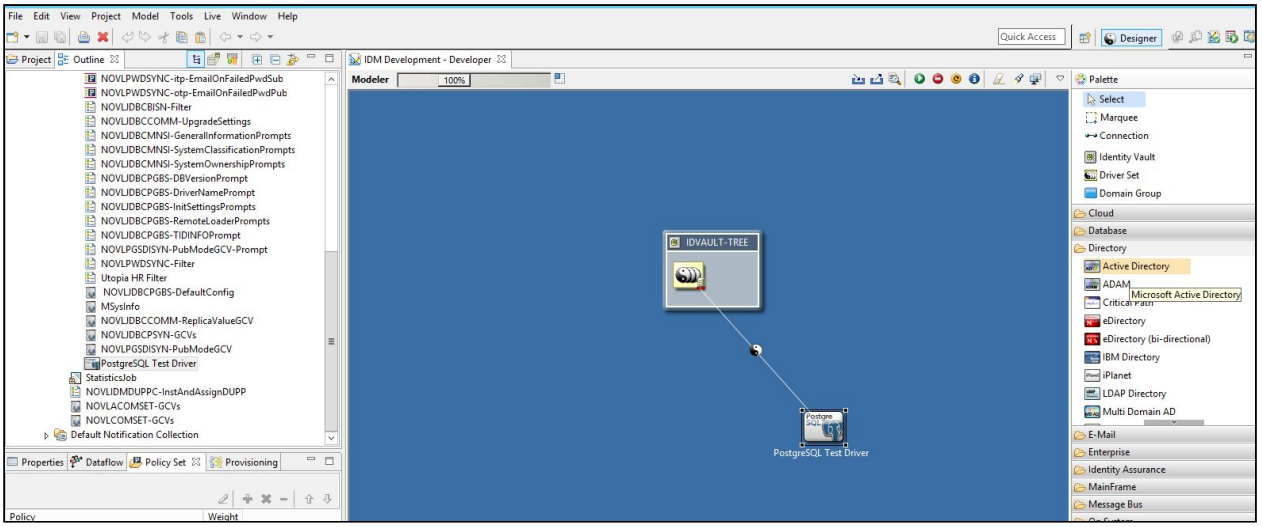


Figura 5.24: Selección de conector de Active Directory

En las siguientes figuras se muestran las pantallas iniciales de dicho conector, que en este caso particular como dijimos, utiliza el componente Remote Loader

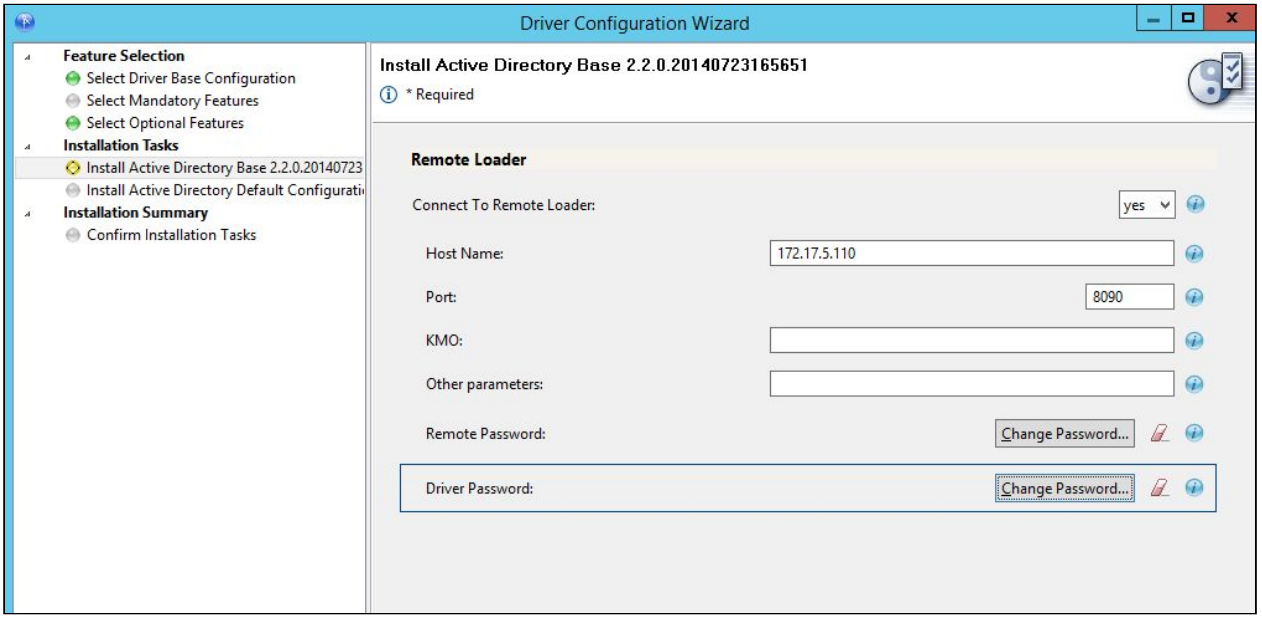


Figura 5.25: Configuración inicial de conector Active Directory

En la siguiente figura 5.26 vemos configuración relacionada con el nombre de dominio, la rama de los usuarios, etc. Esta configuración inicial es la básica y por lo general común a todos los conectores de integración.

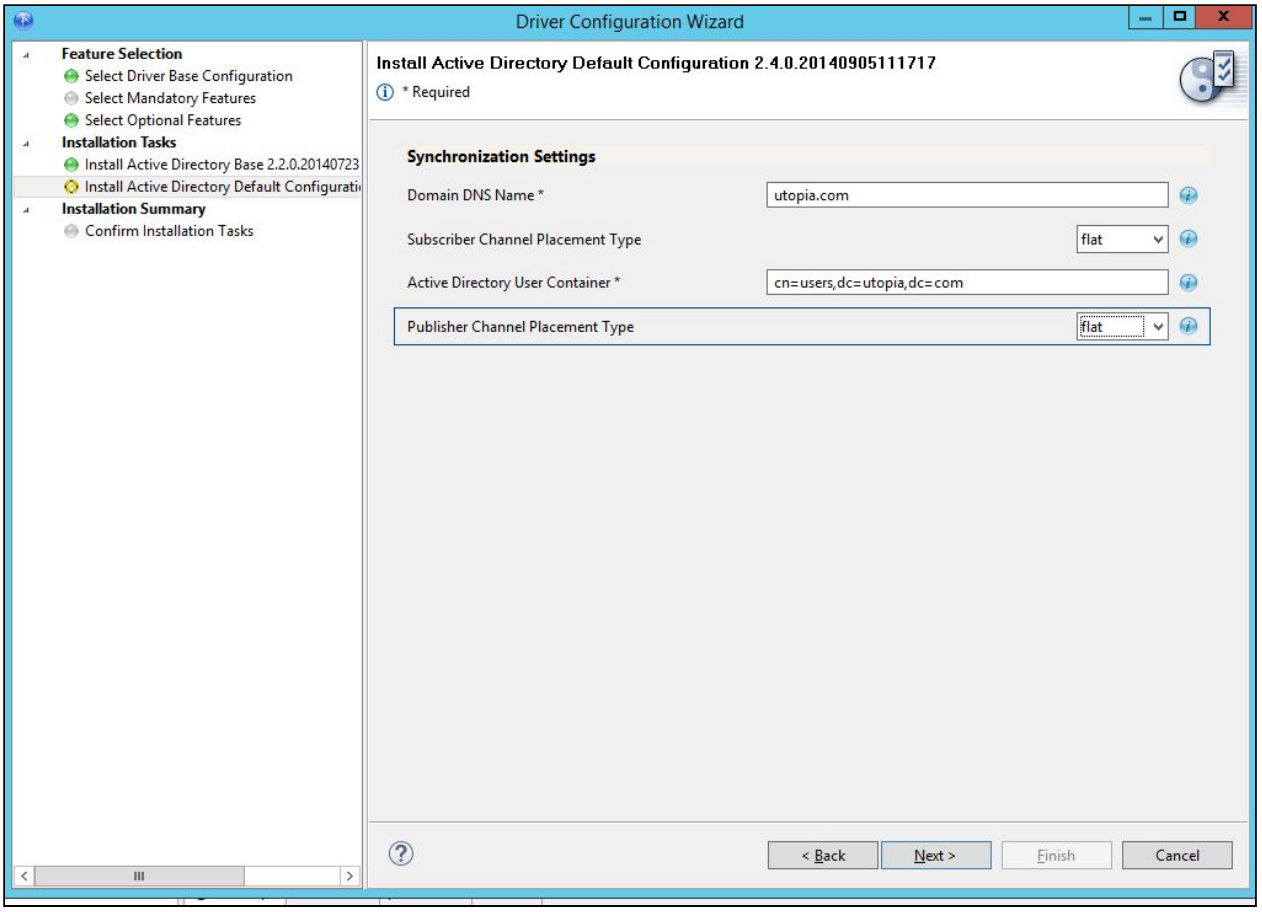


Figura 5.26: Configuración del conector Active Directory

Una vez instalado el conector, podemos apreciar dicho conector dentro del entorno de Identity Manager, y su conexión con el Identity Vault, como vemos en la figura 5.27:

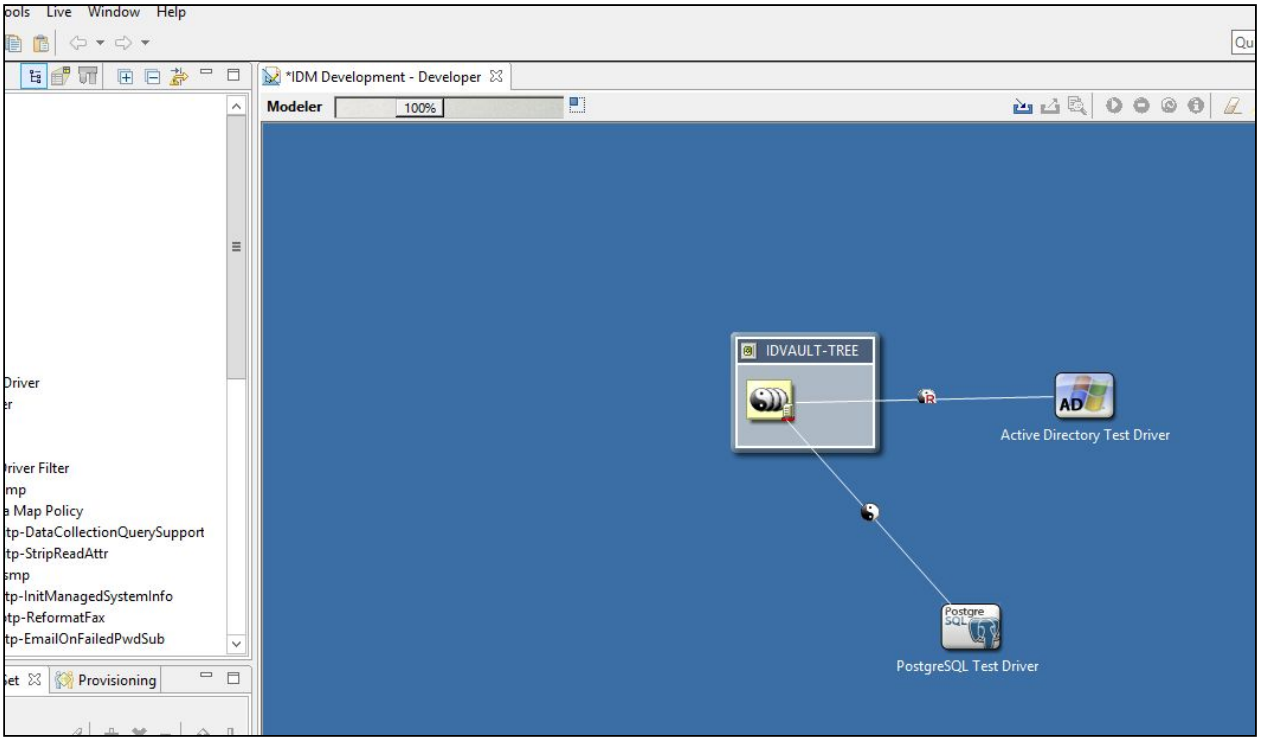


Figura 5.27: Conector de Active Directory integrado al sistema Identity

Una vez instalado el conector, se debe configurar el componente de Remote Loader. En este caso, dicho componente se instaló dentro del mismo servidor donde se encuentra el sistema Active Directory (puede ser instalado también en un servidor separado para evitar sobrecarga de procesamiento).

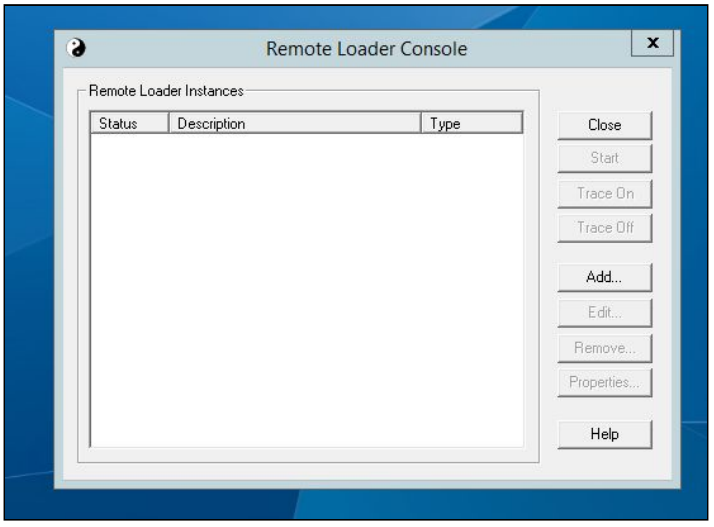


Figura 5.28: Componente remote loader

En la siguiente figura vemos la configuración del componente del remote loader, donde se configuran nombres, dirección IP del Metadirectorio con el que se conectara, drivers y archivos de configuración específicos, archivos de logs, etc.

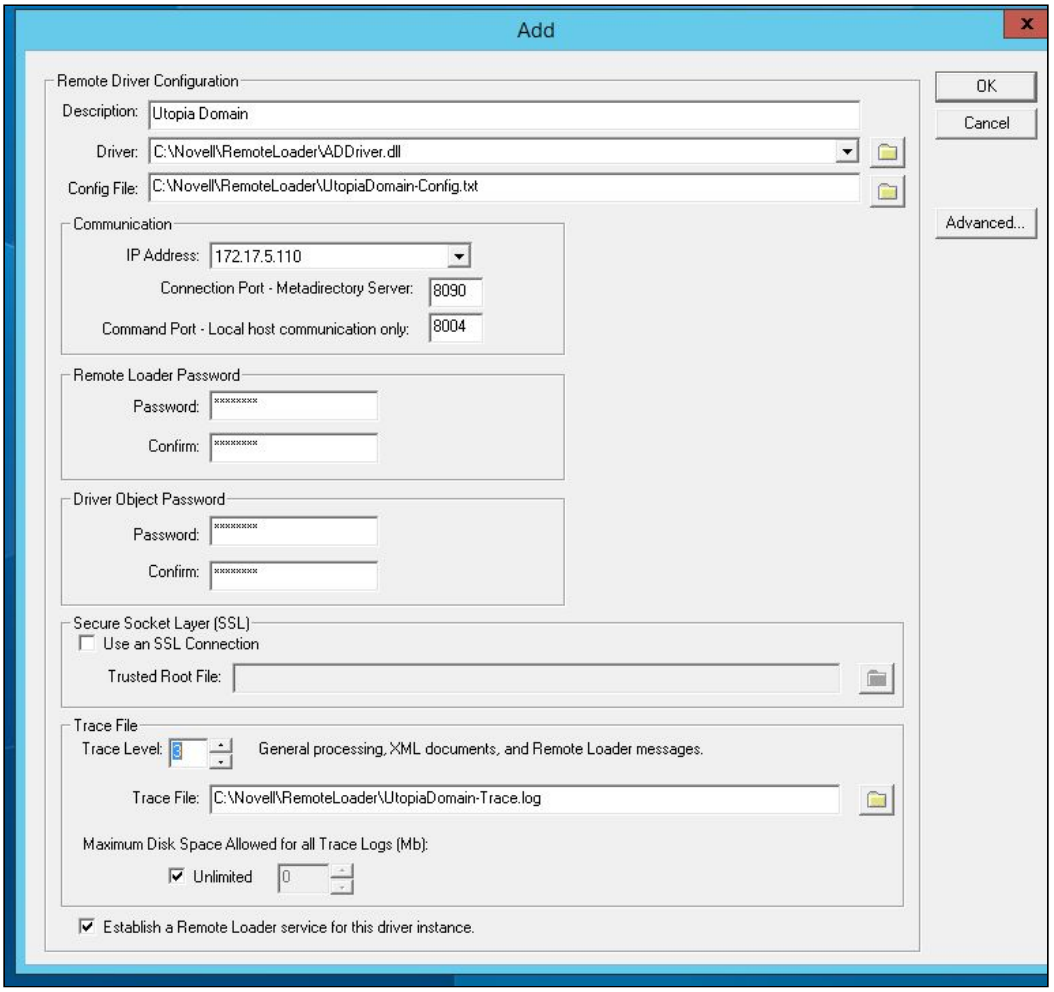


Figura 5.29: Configuración del componente Remote Loader

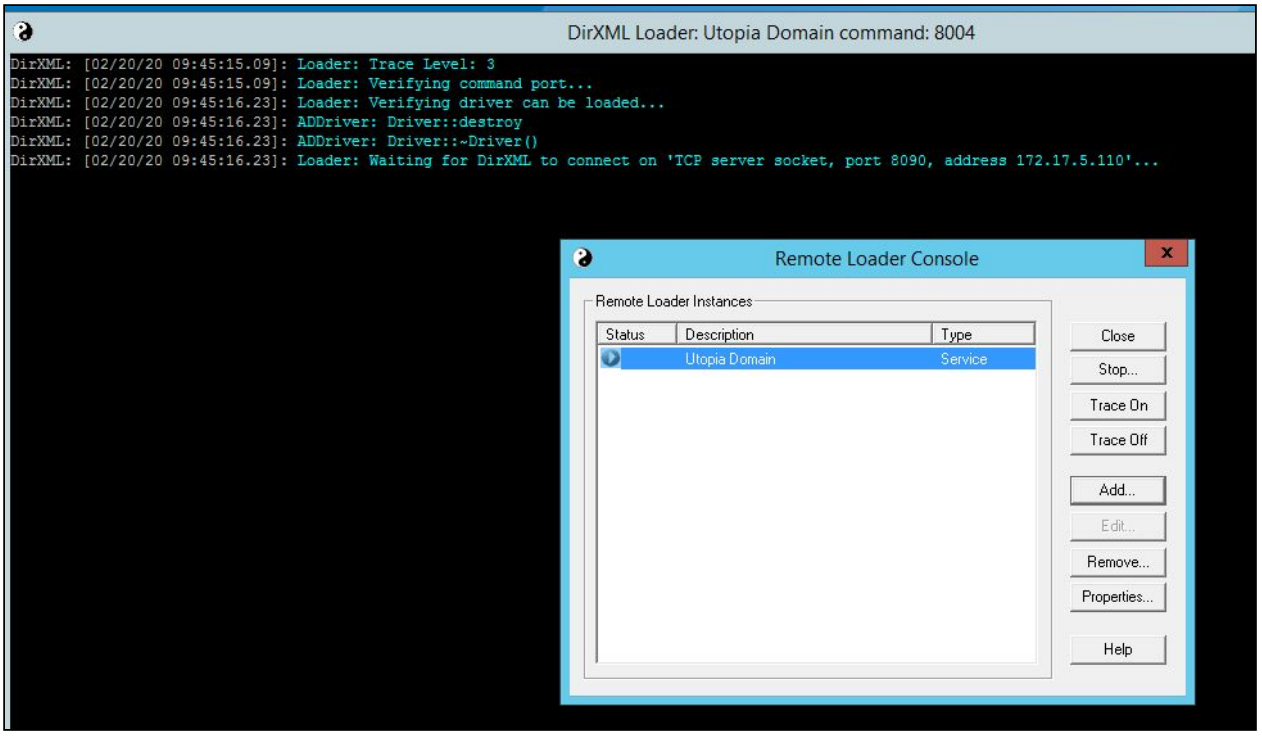


Figura 5.30: Remote Loader funcionando

Una vez instalado dicho conector, está integrado al sistema de Identity Vault.
Cuando por ejemplo, se de un alta de usuario nuevo en el sistema de Recursos Humanos, el mismo se verá reflejado tanto en el sistema de Active Directory, como dentro del sistema Identity Manager:

Por ejemplo si agregamos un usuario Sebastian Castro:

Figura 5.31: Usuario agregado en sistema de HR

Lo vemos agregado al repositorio de Active Directory como se aprecia en la figura 5.32:

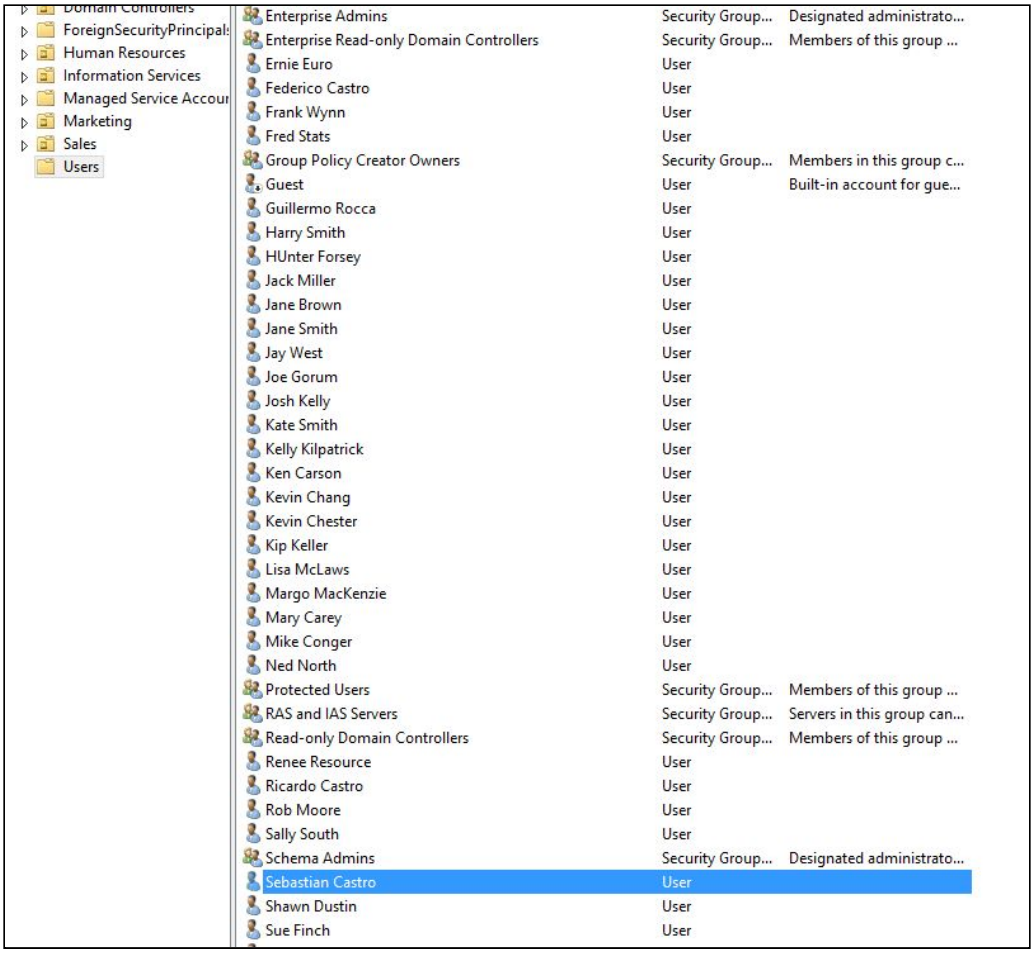


Figura 5.32: Usuario agregado en Active Directory

A su vez, si vamos al sistema de administración del IDM, iManager, podemos ver que el evento de alta de usuario ha sido procesado por el conector de Active Directory y dado de alta en el repositorio principal del IDM Identity Vault. (figura 5.33).

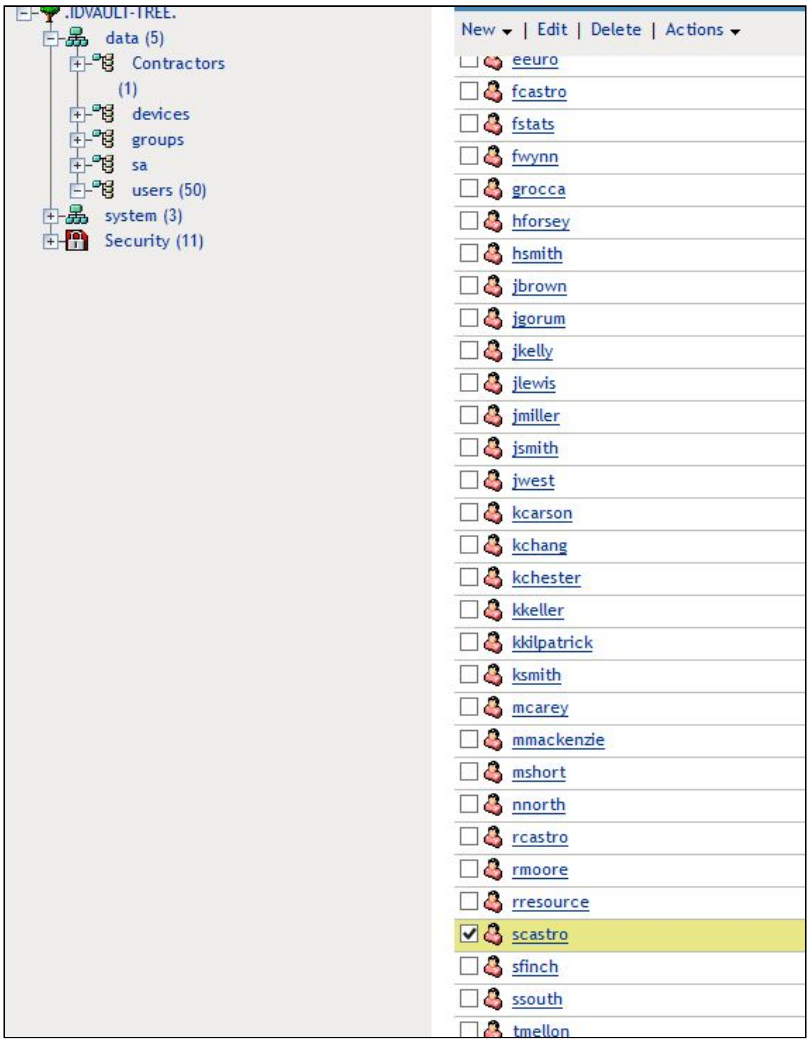


Figura 5.33: Usuario agregado en Identity Vault

Como vemos, lo que se mostró como ejemplo con la integración de estos dos sistemas, el externo de recursos humanos con su propia base de datos, como el interno al organismo de Active Directory, es que ante el alta (puede ser baja, modificación o cualquier evento que se quiera configurar) de un usuario en el sistema de recursos humanos, automáticamente se procese dicho evento y se da de alta en los sistemas de Active Directory interno como en el sistema principal que integra todas las identidades IDM.

Capítulo 6

Solución Access Manager a Implementar

En el siguiente capítulo se describe la solución elegida para llevar a cabo la protección de aplicaciones web y el acceso seguro a las mismas.
En un primer momento se describen las características particulares de la solución a implementar, detallando luego sus componentes y el funcionamiento general de toda la solución. Por último se detalla la arquitectura que posee mostrando cómo interactúan los diferentes componentes entre sí.

6.1. NetIQ Access Manager AM

La solución elegida por el organismo que es la encargada de la gestión de accesos a los sistemas informáticos es la de la empresa NetIQ, llamada Access Manager (AM por sus siglas en inglés) [14].
Dicha solución permite la administración de accesos a las aplicaciones y recursos web, proporcionando un inicio de sesión único y transparente para el usuario.
Para proporcionar acceso seguro desde cualquier ubicación o dispositivo, admite la autenticación de múltiples factores, el control de acceso basado en roles y el cifrado de datos.

6.2. Características principales:

Las principales características que se destacan de la solución Access Manager son las siguientes:

1. Proteger los recursos al proporcionar acceso

El propósito principal del sistema Access Manager es proteger los recursos web al permitir el acceso solo a los usuarios que se están autorizados, haciendo que únicamente los usuarios que están autorizados a usar los recursos protegidos tengan permiso de acceso, denegando a los usuarios no autorizados.

Figura 6.1:.Autorización de usuarios en NetIQ AM [17]

Este sistema asegura los recursos web de los usuarios malintencionados o hackers y amenazas de Internet, ya que las direcciones IP de los servidores que alojan los recursos protegidos están ocultas para los usuarios externos e internos.
La única forma de acceder a los recursos web es iniciando sesión en Access Manager con credenciales autorizadas.

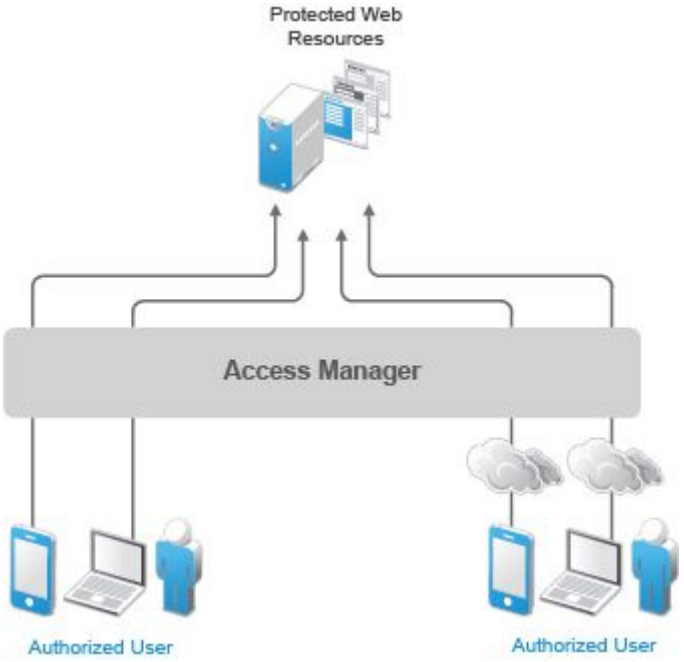


Figura 6.2: Autorización de usuarios en NetIQ AM [17]

2. Gestión de contraseñas con inicio de sesión único

La autenticación a través de Access Manager no solo establece la autenticación a las aplicaciones, sino que también puede otorgar autorización a esas mismas aplicaciones. Con el inicio de sesión único, los usuarios solo necesitan recordar una contraseña para acceder a todas las aplicaciones y recursos web que están autorizados a usar.

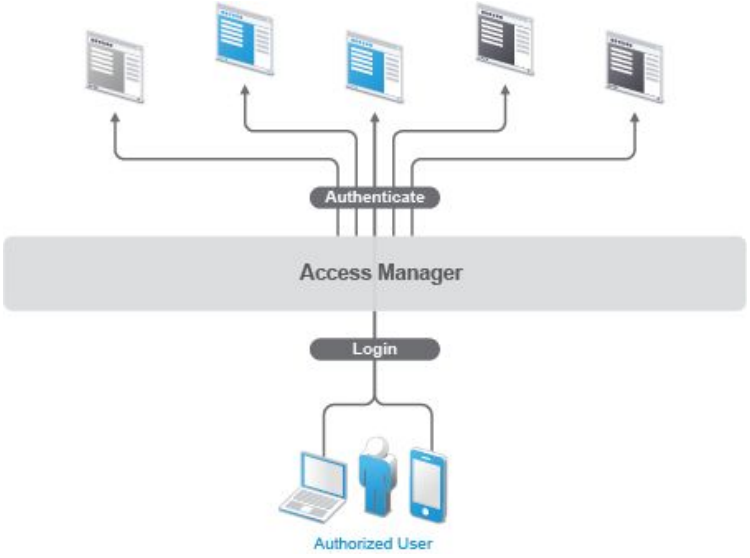


Figura 6.3: Autenticación en NetIQ AM [17]

3. Perfil de accesos por roles

Este sistema automatiza la concesión y revocación de acceso mediante el uso de roles y políticas establecidas. A los usuarios se les asignan roles que tienen políticas de acceso asociadas, y cada vez que un usuario se autentica a través de Access Manager, el acceso del usuario está determinado por las políticas asociadas con los roles del usuario.

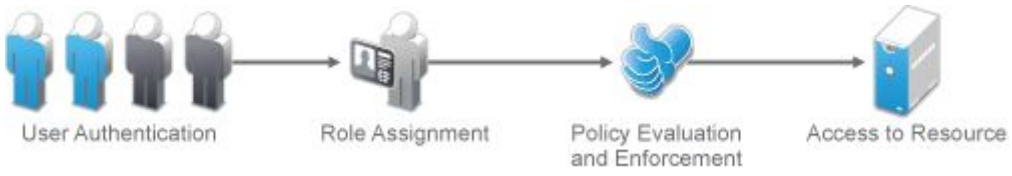


Figura 6.4: Roles y políticas de seguridad

6.3. Componentes y sus características

De la misma manera que una solución IDM, la solución de AM está comprendida por varios componentes y servicios que interactúan entre sí para permitir la gestión de accesos seguros y controlados.
Un sistema Access Manager se compone inicialmente por un componente de administración, y su funcionamiento básico se da a través de sus dos componentes principales: el Identity Servers y el Access Gateways, que proveen control de acceso para los distintos servicios web.
Los propósitos principales de un sistema Access Manager comprende en: Autenticación, Federación de Identidad (*Identity federation*), Autorización e Inyección de Identidad (*identity inyection*).

A continuación describiremos estos propósitos y las características y funcionamiento de cada uno de los componentes:

6.3.1. Consola de administración

La consola de administración es la herramienta central de configuración y administración del producto. Desde su panel de control permite evaluar el estado de todos los componentes de Access Manager y administrar todo el sistema.

Al iniciar en la consola de administración de Access Manager, podemos ver el panel inicial con los principales paneles de configuración:

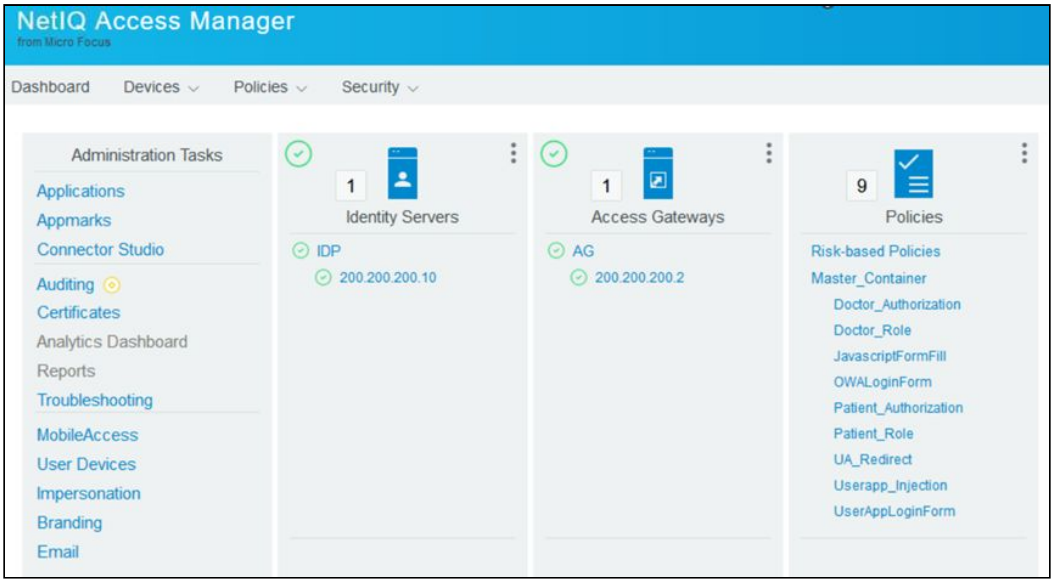


Figura 6.5. Consola de administracion Access Manager

Desde dicho panel se configuran principalmente los componentes principales de la solución, Identity Servers y Access Gateways.

En las siguientes figuras podemos observar la pantalla de configuración de ambos componentes, donde se crean nuevos, se manejan sus estados de inicio o detención de servicios, etc.

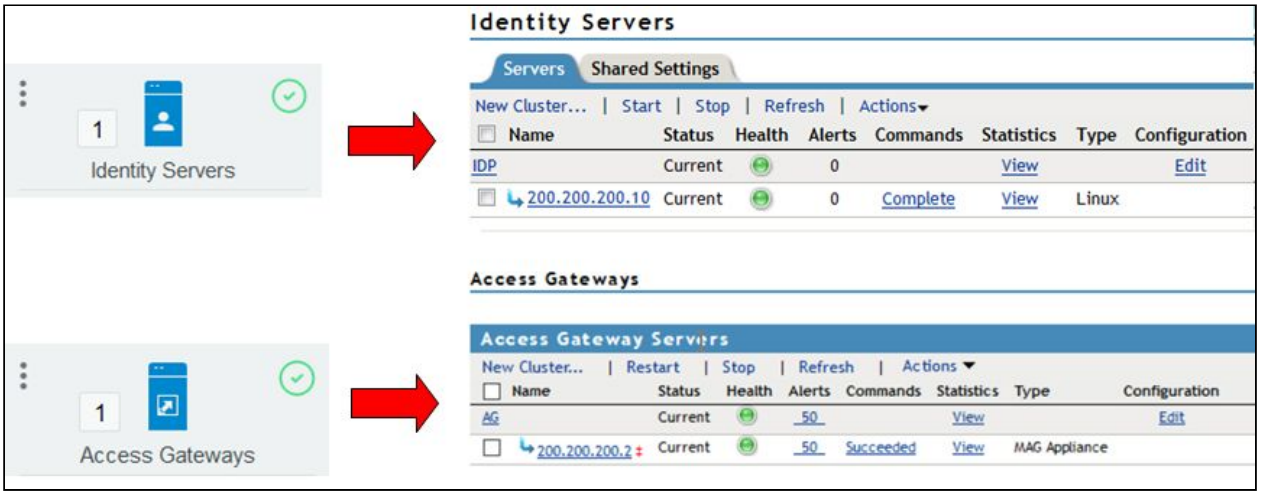


Figura 6.6. Panel informativo de los componentes principales

6.3.2. Identity Server

Este componente es el punto central de autenticación y acceso de identidad para todos los demás servicios dentro un sistema Access Manager. Es responsable de autenticar a los usuarios y distribuir información de roles para facilitar las decisiones de autorización.
El Identity Server siempre funciona como un proveedor de identidad y además puede configurarse para ejecutarse como un consumidor de identidad (también conocido como proveedor de servicios), mediante el uso de los protocolos de federación Liberty, SAML 1.1, SAML 2.0 o OAuth.
Como proveedor de identidad, Identity Server valida las autenticaciones contra el repositorio de usuarios de identidad que se haya definido, pudiendo ser este un repositorio de LDAP, Active Directory, u otro.

En una configuración de Access Manager, el componente de Identity Server es el responsable de administrar las siguientes tareas:

- Autenticación: verifica las identidades de los usuarios a través de varias formas de autenticación, tanto locales (proporcionadas por el usuario) como indirectas (suministradas por proveedores externos). La información de identidad puede ser algún atributo característico del usuario, como un rol, dirección de correo electrónico, nombre o descripción del trabajo. Los mecanismos de autenticación pueden ser nombre/password o más avanzados como la contraseña de un solo uso basada en el tiempo (TOTP *Time-Based One-Time Password*), certificados digitales, Kerberos, la autenticación federada con proveedores externos de

OAuth y también la autenticación basada en el riesgo (RBA *Risk Based Authentication*).

- Identity Stores: enlaces a las identidades de usuario almacenadas en directorios LDAP como pueden ser eDirectory, Microsoft Active Directory o Sun ONE Directory Server.

- Aprovisionamiento de cuentas: habilita el aprovisionamiento de cuentas del proveedor de servicios, creando automáticamente cuentas de usuario durante una solicitud de federación.

- Inicio de sesión único y cierre de sesión: permite a los usuarios iniciar sesión solo una vez para obtener acceso a múltiples aplicaciones y plataformas. El inicio de sesión único y el cierre de sesión único son las características principales de Access Manager.

- Manejo de Roles: Gestiona el control de acceso basado en roles, llamado RBAC (*Role Based Access Control*), proporcionando la asignación de permisos y accesos de los usuarios según su función o rol. El componente de Identity Server establece el conjunto activo de roles para cada nueva sesión del usuario cada vez que el mismo se autentica. Los roles establecidos se pueden usar en las políticas de autorización para formar la base para otorgar y restringir el acceso a recursos web particulares.

- Identity Federation: La federación de identidad o Identity Federation es la asociación de cuentas de usuario entre un Identity Provider (proveedor de la identidad) y un Service Provider (servidor de identidad). Para ello debe haber una relación de confianza entre el proveedor de la identidad (el identity provider) y el servicio que confía en dicho proveedor de la misma. Con la federación de identidad se reduce el costo que se adquiere al mantener la cuenta de usuarios, ya que múltiples organización no necesitan mantener independientemente información de las cuentas, como los password por ejemplo, y de parte de los usuarios es una mejora ya que no requiere de múltiples cuentas para acceder a distintos servicios.

6.3.3 Access Gateway

Un Access Gateway es el componente dentro de la solución de Access Manager que proporciona el acceso seguro a los servidores web existentes. Además, proporciona servicios de seguridad, como la autorización, inicio de sesión único y cifrado de datos, integrados con los servicios de identidad y las políticas de Access Manager.

Este componente de Access Gateway está diseñado para trabajar con el componente de Identity Server para habilitar el inicio de sesión único en servicios web a proteger. Entre

las funciones que puede realizar el componente de Access Gateway para permitir el inicio de sesión único se destacan:

- Identity Injection: El componente Access Gateway obtiene información de los usuarios de repositorio de usuarios (User Store, generalmente un sistema LDAP); usa es información para inyectar información dentro de headers HTML, querys o consultas SQL, o para headers de autenticación básica, y envía esa información hacia los web servers que tienen el servicio a acceder. Access Manager llama a esta tecnología como inyection de identidad o Identity Injection. El Web Server usa esa información para personalizar contenido o para ser usado como decisión de autorización adicional.
- Autorización: La autenticación es el proceso de determinar quien es un usuario, la Autorización es el proceso de determinar qué es lo que el usuario tiene permitido hacer o a que tiene permitido acceder.
  Las políticas de Autenticación son dinámicamente aplicadas y se aplican cuando un usuario intenta acceder a un recurso protegido.
- Relleno de formulario (*form fill*): esto permite rellenar automáticamente la información del formulario solicitado.

Además, este componente de Access Gateway también se puede configurar para almacenar en caché las páginas solicitadas. Cuando un usuario cumple con los requisitos de autenticación y autorización, se le envía la página desde la memoria caché en lugar de solicitarla al servidor web, lo que mejora el rendimiento de la entrega de contenido.

6.4. Arquitectura Física

A continuación se detalla la arquitectura típica de la solución de Access Manager donde se detallan los tres componentes principales antes descritos.

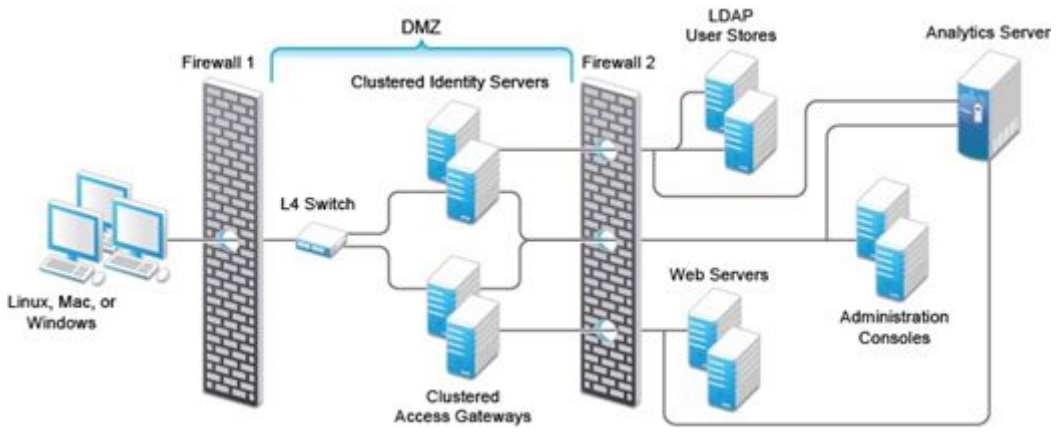


Figura 6.7: Arquitectura Física de Access Manager [18]

En el diagrama se observa que la arquitectura típica de un sistema Access Manager se instala y configura agrupando dentro de una zona asegurada por firewalls internet y externos (en este caso dentro de una DMZ o Demilitarized Zone), siendo protegidos en este caso tanto el componente de Identity Servers como el de Access Gateway.
En un otro sector de red interno o separado se encuentran los recursos web que se quiere acceder y proteger y el repositorio de los usuario o User Store. En este caso el componente de servidor LDAP User Stores, será el repositorio de Identidades de la solución de Identity Manager IDM.
En las comunicación o conexiones entre los servicios que componen la solución de Access Manager, un Identity Server se comunica con un repositorio de usuario que es de donde va a consumir la información de los mismos para la autenticación, y el sistema de Access Gateway que se comunica con los servidores web que protege.
Desde una consola de administración se controla y configura todo el sistema, teniendo comunicación, tanto con el Identity Server, como con el Access Gateway.

6.5. Funcionamiento de Access Manager

A continuación se muestra a modo de ejemplo en la figura 6.8 cómo interactúan los componentes y el flujo de procesos entre los mismos y que constituyen el funcionamiento básico de un sistema de Access Manager:

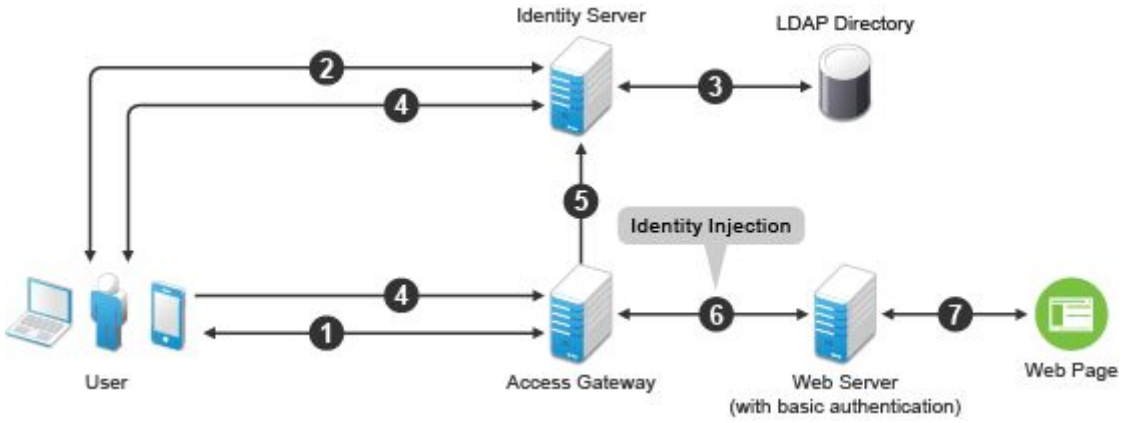


Figura 6.8: Flujo de comunicación de los componentes Access Manager [19]

1. El usuario envía una solicitud a Access Gateway para acceder a un recurso protegido.

2. El Access Gateway redirige al usuario al Identity Server, el cual verifica si el navegador que está realizando la petición ya tiene una sesión iniciada (mediante una cookie propia del Identity Service Provider exclusiva para este proceso).
   En caso de no tener sesión, le presenta al usuario un formulario para que ingrese las credenciales. En este caso se le solicitará el nombre de usuario y password en la página de login del componente de Identity Server.
3. El usuario ingresará las credenciales
4. El Identity Server verifica el nombre de usuario y la contraseña ingresado con el repositorio de usuarios LDAP que tenga definido.
5. En el caso de ser credenciales válidas, el Identity Server devuelve un token de acceso y se le enviará con un redirect hacia la aplicación a acceder.
6. El Access Gateway recupera las credenciales del usuario de Identity Server a través del canal de comunicación con el mismo.
7. Access Gateway inyecta la información básica de autenticación en el encabezado HTTP.
8. El servidor web valida la información de autenticación y devuelve la página web solicitada.

Capítulo 7

Implementación de la solución Access Manager

En este capítulo se explicará la implementación del sistema Access Manager, principalmente mostrando a través de figuras, los distintos pasos de configuración de los componentes principales, como son el Identity Server, Access Gateway y el Users Store o repositorio de usuarios.
Además se muestran como se integran las aplicaciones web y cómo se configuran los recursos que se quieren proteger de las mismas.
Por último se detalla cómo se aseguran los distintos componentes utilizando certificados digitales para encriptar la comunicación e información que se intercambia entre los mismos.

7. 1. Proceso de Instalación y de Configuración

Tanto el componente de Administration Console como el Identity Server pueden instalarse en un solo servidor, o en servidores separados donde se aloja cada componente; no siendo así el componente de Access Gateway, ya que este debe ser un servidor aparte separado de los demás componentes.
Este sistema de Access Gateway puede instalarse en forma de appliance (software que incluye todo el componente de Access Gateway, incluyendo su propio sistema operativo donde se ejecuta, dependencias, librerías y archivos de configuracion) o como un servicio aparte para poder instalarse dentro de un sistema operativo soportado previamente instalado.
Ambos tipos de gateways soportan las mismas funcionalidades básicas de su función, como la protección de recursos web, autorización, redundancia para proveer tolerancia a fallas, reescritura de URLs, etc.
La principal diferencia radica en el que en forma de appliance se obtiene una solución más robusta y confiable, estando la mayoría de las configuraciones del Access Gateway ya previamente seteadas para el correcto funcionamiento del mismo.
En el caso del organismo, se decidió la instalación de cada componente (Administration Control, Identity Server Provider y Access Gateway) se instalen en servidores separados; eligiendo para el Access Gateway la modalidad de appliance. (ANEXO: Diseño Físico de la Implementación).

7.1.1. Instalación del Administration Console y el Identity Server Provider

El software de instalación del producto elegido de la empresa NetIQ incluye tanto el instalador del componente de Administration Console (necesario para la configuración y manejo de los componentes) como el componente de Identity Server Provider IDP (Identity Server Provider encargado de la autenticación).

En la figura 7.1 se muestra el inicio de la instalación. Inicialmente se muestra los componentes a instalar, consola de administración y el identity server, pudiendo decidir cuál componente instalar.

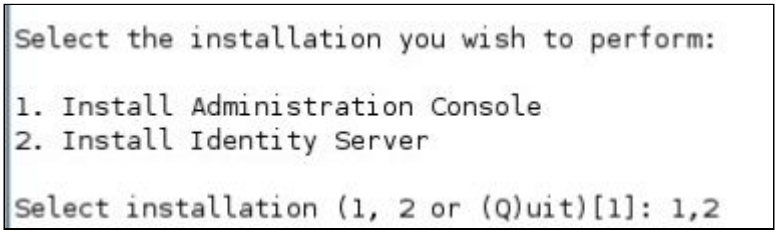


Figura 7.1: Selección de componentes a instalar

Ahí se seleccionan opciones como dirección ip del servidor IDP y de la consola Administrativa, password del usuario "admin", no requiriendo mucha más información, ya que el proceso de configuración se hará luego desde la consola administrativa.

7.1.2. Instalación de Access Gateway Appliance

Como se explico al principio, la instalación de Access Gateway se puede realizar a través de un servicio software a instalar en un sistemas operativo soportado previamente instalado, o sino mediante una appliance (distribución Linux que incluye el servicio de access gateway) que ya viene con todo lo requerido, sistema operativo y aplicación con sus servicios.

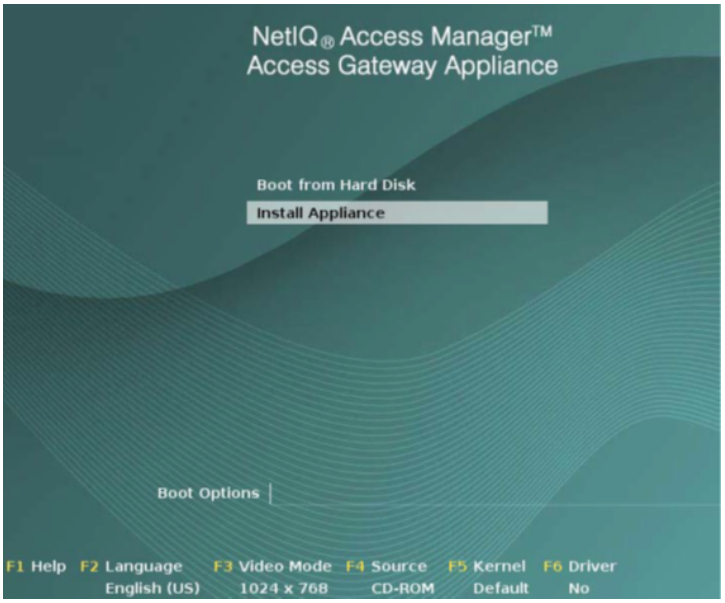


Figura 7.2: Booteo del instalador del appliance

En la primer ventana de configuración se deben ingresar los parámetros básicos de configuración de red, como nombre del host, IP address, dominio, etc.

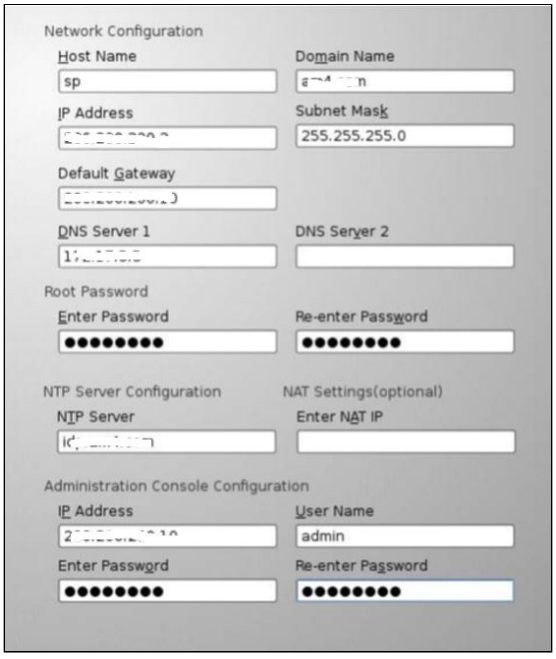


Figura 7.3: Pantalla de seteo de información básica inicial del Access Gateway

Una vez finalizada la instalación del Access Gateway, dentro de la consola de administración podemos chequear que el mismo se ha instalado correctamente y es reconocido dentro del sistema Access Manager:

Figura 7.4: Validación de la instalación del Access Gateway

Con esto ya quedan instalados y configurados inicialmente los parámetros básicos de red y conectividad los componentes de Access Manager. Ya luego a partir de aquí, como se detalla en las siguientes secciones de este capítulo, se comenzaron a configurar los aspectos más importantes y funcionales del sistema, siendo por ejemplo la configuración del Identity Service Provider (IDP), la configuración de proxies para la protección de recursos web, la configuración de certificados digitales y conexiones SSL para encriptar y asegurar las comunicaciones entre los distintos componentes, configuración de autorización, etc.

7.2. Configuración de Access Manager

La configuración inicial de la solución Access Manager consistió en configurar los dos componentes principales: Identity Server y Access Gateway mediante la consola de administración.
Si bien la solución de Access Manager soporta múltiples mecanismos de autenticación, en el contexto del proyecto solo se configuró el mecanismo de autenticación mediante el ingreso de nombre de usuario y password en el formulario de login que presenta el componente de Identity Server al momento de que un usuario requiera el ingreso a un sistema web y no esté autenticado.
A su vez, debido a la criticidad de los componentes que componen el sistema Access Manager, una buena práctica a implementar en ambientes productivos y para poder tener alta disponibilidad una mejor calidad de servicio y redundancia, se implementaron los componentes tanto de Access Gateway como de Identity Server Provider en cluster (siendo un cluster un grupo de dos o más servidores conectados que son visto como un único servidor).

- *AG_CLUSTER*: este cluster de servicios es el dedicado a atender las peticiones recibidas por los equipos Access Gateways, los cuales acelerarán los aplicativos del organismo (el concepto de *acelerador* está asociado a una solución de Access Manager, en la cual un webserver es accedido a través del Access Gateway por los usuarios, sin llegar estos a tener una conexión de red con los mismos).

- *IDS_CLUSTER*: este cluster estará dedicado a atender las peticiones referidas a autenticación de los usuarios en la solución. Es el encargado de generar el inicio de sesión único (SSO Single Sign-On) entre el usuario y los aplicativos en cuestión.
  El cluster de identity servers se expone por protocolo seguro (https) bajo el siguiente nombre: *login.organismo.gov.ar*

7.2.1. Configuración del componente Identity Server

En este sección se muestra a modo de ejemplo la configuración realizada para este componente.
Después de la instalación, la configuración inicial del Identity Server, se requiere la siguiente información:

- El nombre DNS para Identity Server.
- La dirección IP de un directorio LDAP (repositorio de usuarios).
- El directorio LDAP se utiliza para autenticar a los usuarios.
- El certificado raíz de confianza del almacén de usuario se importa para proporcionar una comunicación segura entre el Servidor de Identidad y el almacén de usuario.
- El nombre y la contraseña distinguidos del administrador de la tienda de usuarios LDAP.

En la figura 7.5 se muestra la pantalla inicial de configuración del componente Identity Server, desde donde se configuran todos los parámetros requeridos.

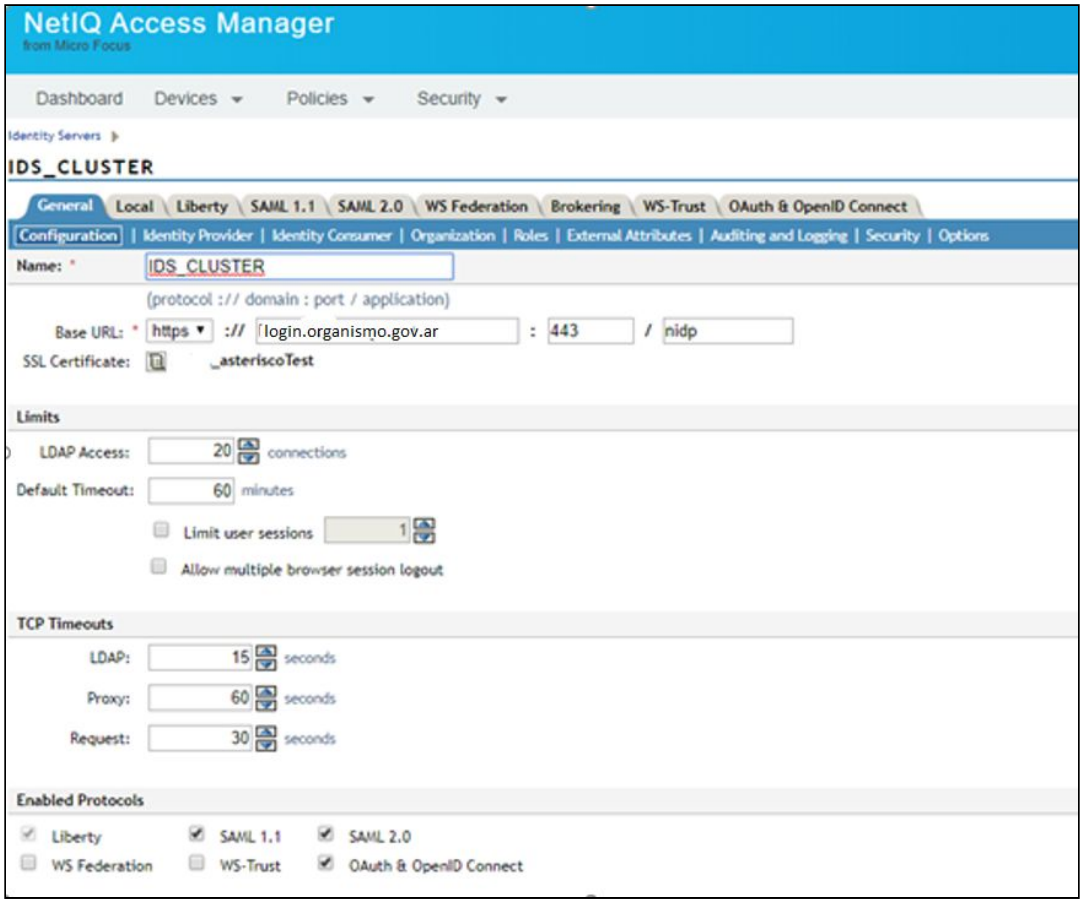


Figura 7.5: Configuración general de Access Manager

A su vez también se configura desde esta pantalla principal General, el url base de login de usuario, los protocolos de federación que están habilitados (en este caso SAML, Oauth y OpenID Connect).

7.2.2. Repositorio de Usuarios

El repositorio de usuarios configurado en el componente de Identity Server es únicamente el repositorio de LDAP de la solución de Identidades, llamado dentro del documento como Metadirectorio (o User Store).
Este repositorio permite la autenticación de los usuarios internos y externos. Para la comunicación se utiliza una cuenta de servicio del repositorio LDAP.
En la figura 7.6 se muestra la configuración del repositorio de usuarios, en el caso del organismo el sistema LDAP eDirectory.

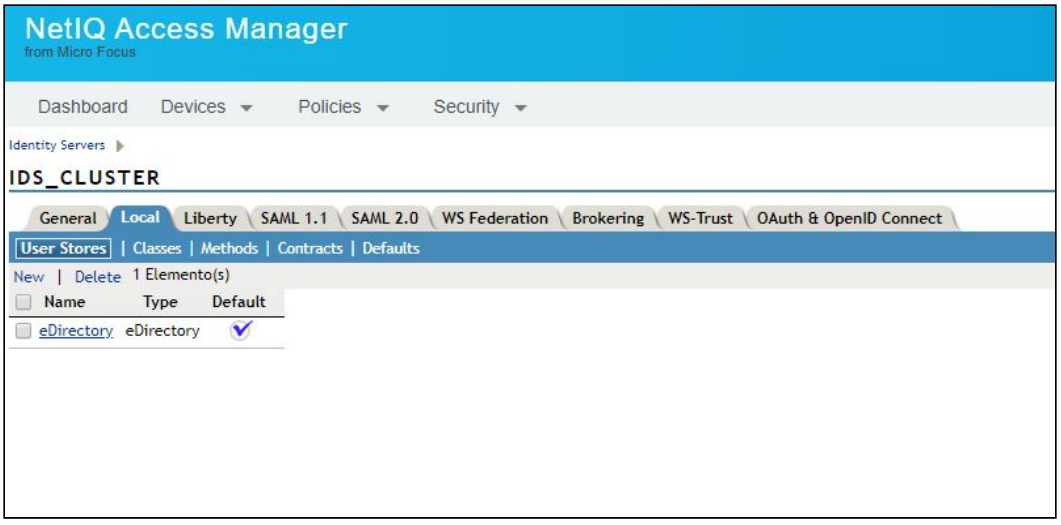


Figura 7.6: Configuración inicial de directorio LDAP

En la figura 7.7 se puede observar la pantalla de configuración de dicho componente, con los parametros especificos.
Lo que se requiere es una la dirección IP del servicio de LDAP a configurar, puerto de conexión (sea SSL o no), rama de búsqueda inicial o contexto de búsqueda, usuario administrador del sistema Ldap.

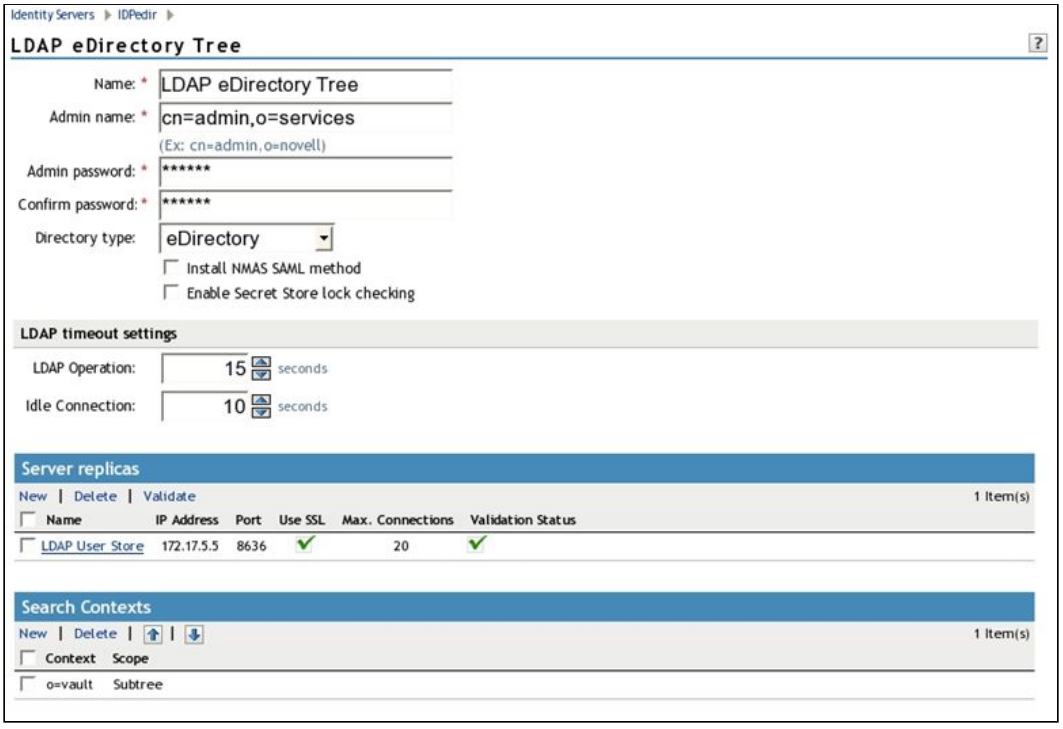


Figura 7.7: Configuración de repositorio LDAP

También, en esta sección de configuración del componente de Identity Server Provider, se encuentra la pestaña de “OAuth & OpenID Connect”, que es donde se setean las

aplicaciones que están registradas para la autenticación por federación; pero esta configuración se detalla en el apartado de “Integración de aplicaciones por federación”.

7.2.3. Configuración de Access Gateway

Como hemos explicado, un Access Gateway proporciona acceso seguro a los servidores Web existentes basados en HTTP. Este proporciona los servicios de seguridad típicos (autorización, inicio de sesión único y cifrado de datos) está integrado con los servicios de identidad y políticas de Access Manager. La configuración inicial de un sistema Access Gateway comprendió en la configuración de un proxy reverso, actuando como intermediario entre los requerimiento realizados por los navegadores y las aplicaciones que brindan los servicios.
Como se explicó en el capítulo 3.2, un proxy reverso actúa como el front end de los servidores web en la red DMZ o en la intranet y a su vez, permite acelerar las aplicaciones web, descargando las solicitudes más frecuentes, liberando así ancho de banda y conexiones con el servidor web.
También aumenta la seguridad porque las direcciones IP y los nombres DNS de sus servidores web están ocultos de Internet.
En la figura 7.10 se muestra un ejemplo de ventana de generación de un proxy reverso (*Reverse Proxy*). Aquí entre la información que se debe agregar es si se utiliza comunicación segura entre el Access Gateway y el cliente Browser, los puertos que escucha, tanto en plano o inseguro como el puerto seguro.

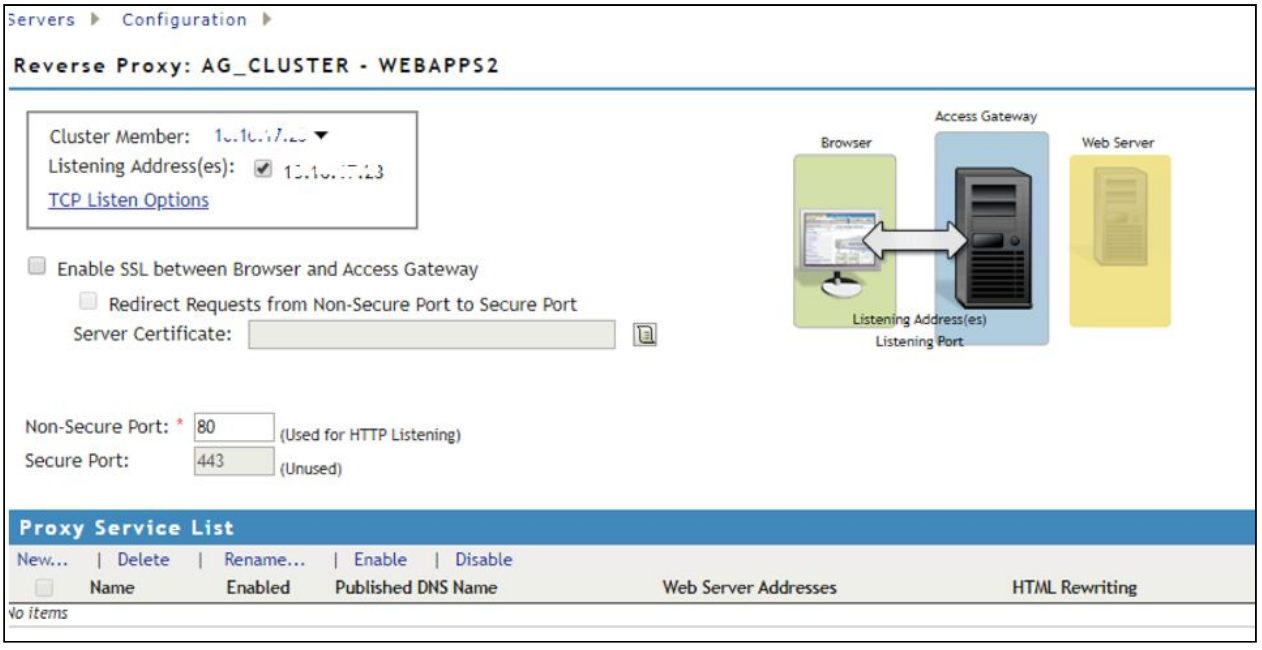


Figura 7.10: Creación de un Proxy

Otra de las opciones importantes a configurar es el proveedor de identidad con el que se comunicara para autenticar el Access Gateway, en este caso es el Identity Server previamente instalado y configurado.

Figura 7.11 : Selección de Identity Server dentro del Proxy Reverso

Con esto estará configurado el proxy reverso a utilizar únicamente, luego se deberá configurar las distintas aplicaciones que se quieren acelerar y proteger por este proxy; siendo lo mismo explicado en la próxima sección de las aplicaciones a integrar.

7.3. Integración con las Aplicaciones

La integración de las aplicaciones se decidió que sea un esquema mixto, es decir, las aplicaciones se configuraron para estar aceleradas por medio del Access Gateway a través de un proxy reverso y a su vez mediante federación con la utilización del protocolo OAuth contra el componente de Identity Server.
Con este enfoque la primer capa de protección la realiza la plataforma Access Gateway (modo proxy reverso) y en segundo lugar mediante el proceso de federación contra el Identity Server.

7.3.1. Integración por proxy reverso

Como se explicó en el apartado anterior, un proxy reverso puede ser configurado para proteger uno o más servicios proxy.
Inicialmente se definieron en cada aplicación web a proteger los PATHs que requieren autenticación (formulario de usuario y password), los paths que son públicos y si exponen API se definió la protección por medio de protocolo de federación OAuth. Para dar un ejemplo, en caso de un aplicativo ejemplo que denominamos “consulta” , un acelerador proxy para esa aplicación tendría la siguiente configuración:

Nombre del Acelerador: Consulta
URL con que se expone la Aplicación: consulta.organismo.gov.ar
Nombre de host enviado al webserver: consulta.organismo.gov.ar
Protección: PATH: /consulta/*

Autenticación: Formulario de → usuario y password

PATH: /consulta/api/*
Autenticación: OAuth Token

PATH: /consulta/public/*
Autenticación: Público

En este escenario la aplicación integrada en modo proxy, si el usuario accede a una página que requiere autenticación, el Access Gateway realizará un redirect al componente de Identity Server para que le solicite el login. Por el contrario si se corresponde a una llamada API protegido por medio de OAuth, el componente de Access Gateway en caso de no recibir un token OAuth válido retornará un HTTP code 401 Forbidden.
A continuación se detalla a modo de ejemplo como fue el proceso de integración de las aplicaciones web del organismo por proxy reverso.
Por cada aplicación a integrar al Proxy Reverso para asegurar y acelerar, se especificaron la siguiente información:

- Proxy service: donde se establece el nombre para identificar el el proxy
- Web Server: el servidor Web donde se encuentra la aplicación
- HTML Rewriting: parte de código HTML se reescribe por otro
- Protected Resources: que parte de la aplicación o Path se protege con autenticación

En las figuras a continuación vemos las pestañas de configuración necesarios.
Por ejemplo, vemos en la figura 7.12 vemos como es la ventana inicial de configuración donde se crea el servicio proxy para la aplicación que se quiera acelerar, donde por ejemplo se especifica el nombre público de la aplicación:

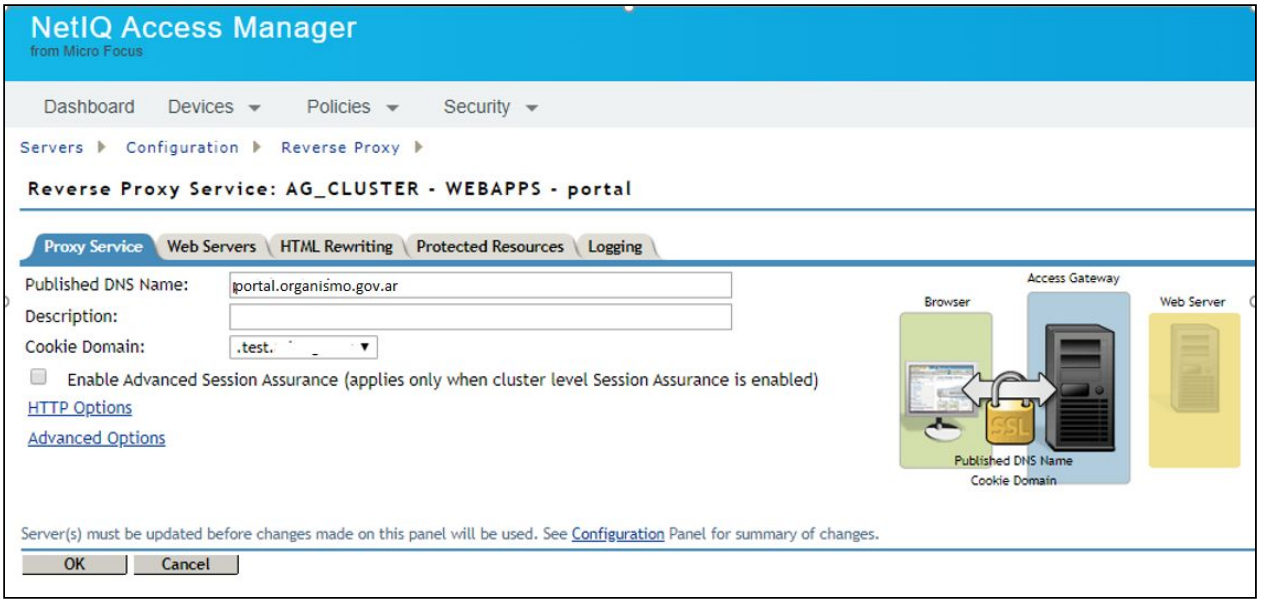


Figura 7.12: Generación de un Proxy Reverso

En la figura 7.13 vemos la parte de la configuración del servidor web donde se aloja la aplicación en cuestión y donde el Access Gateway redirecciona el acceso.

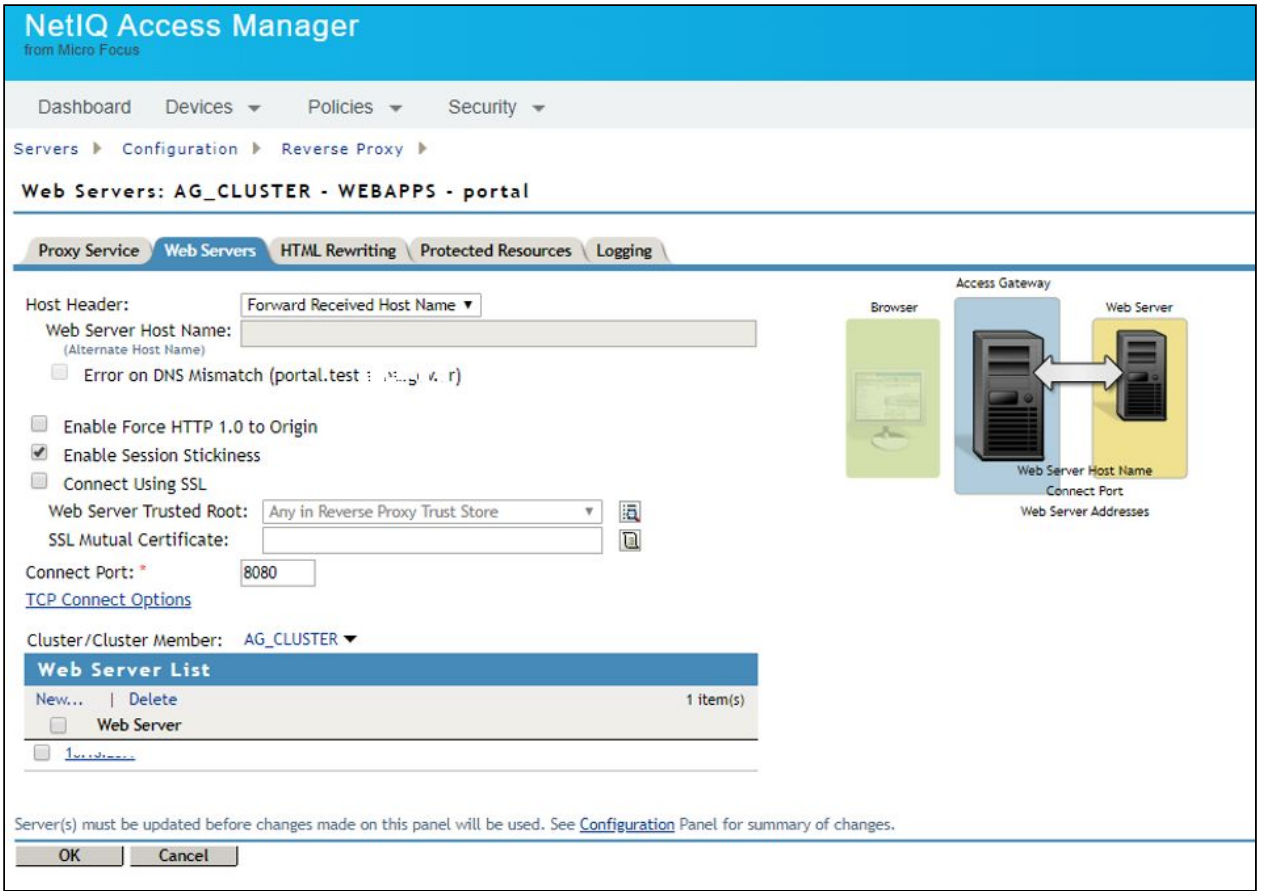


Figura 7.13: Pestana Web Server en generación de un Proxy Reverso

Dentro de las opciones para generación de un proxy, una de las principales es la de protección de recursos.
Una configuración de recursos protegidos especifica los directorios en el servidor Web que desea proteger (parte pública y parte privada)
Particularmente lo que se especifica es qué parte o sector de la aplicación web son públicas por un lado, sin ningún tipo de control en su acceso y cuáles son privadas. Se especifican para ello los diferentes paths o carpetas que serán protegidas. En la figura 7.14 vemos un ejemplo de esta configuración de protección de recurso para una aplicación ejemplo:

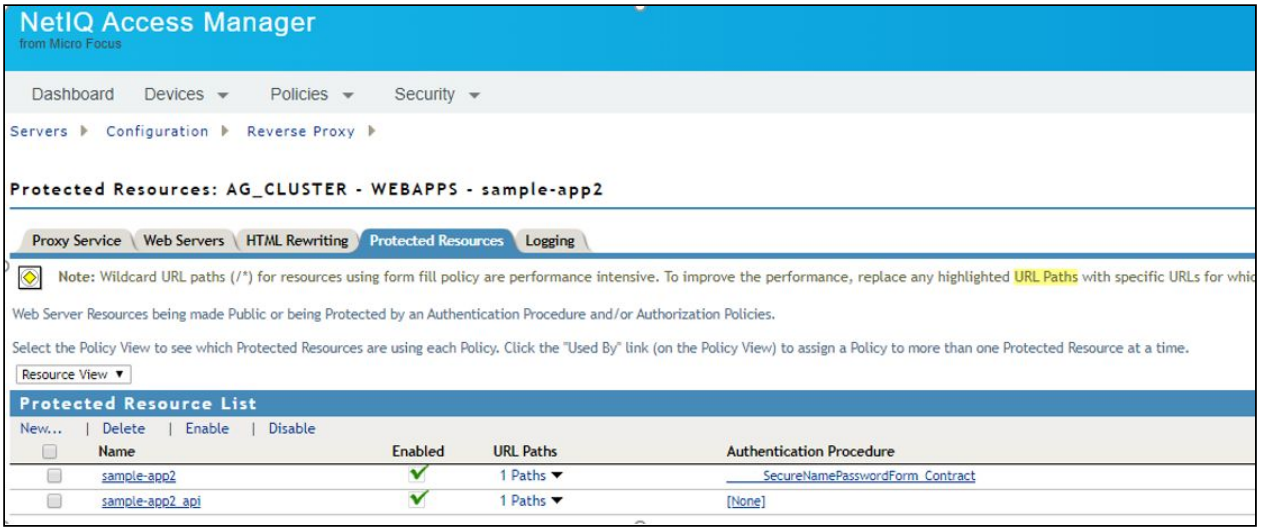


Figura 7.14: Pestaña de configuración de recurso a proteger

Aquí dentro de "Authentication Procedure" podemos seleccionar la forma de autenticación, en este caso se selecciona la autenticación vía formulario usuario/password.

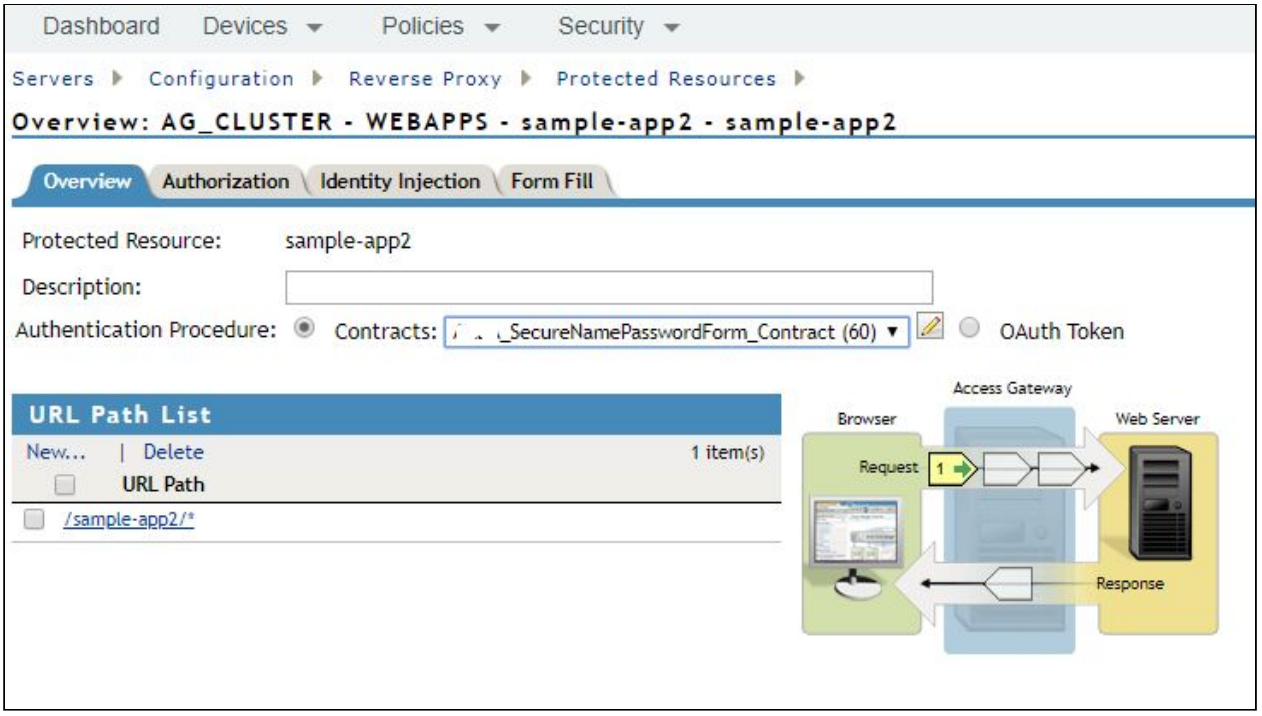


Figura 7.15: Pestaña Protección de Recurso : Authentication Procedure

Por último en la figura 7.16 vemos un ejemplo del listado de las aplicaciones integradas a través de proxy reverso que se han integrado para el proyecto de esta tesina..

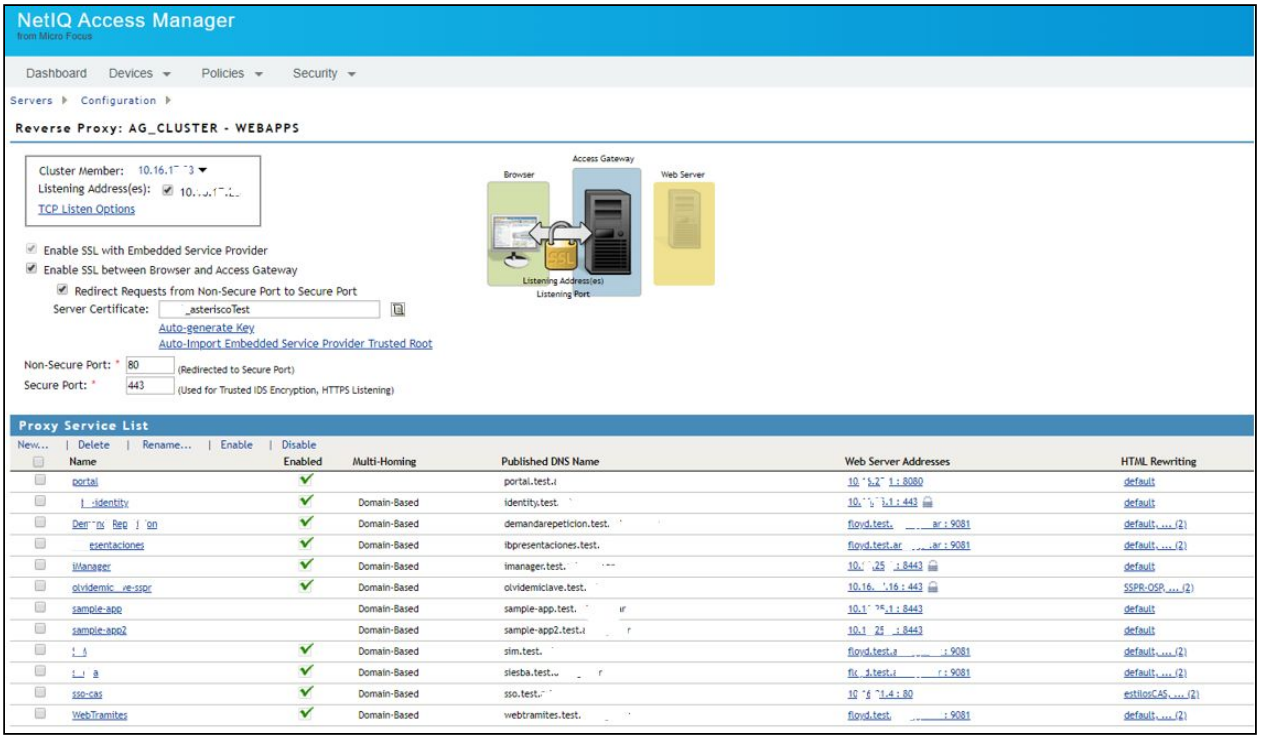


Figura 7.15: Listado de aplicaciones aceleradas por proxy

7.3.2. Integración por federación OAuth

En este tipo de integración se realiza la Federación de Identidades, tomando el Access Manager el rol de Identity Server. De esta manera los aplicativos delegan el proceso de autenticación contra el Identity Server y luego validan que el proceso se haya realizado de forma correcta mediante la utilización de Tokens generado por el Identity Server y entregados por el User Agent a la aplicación. La federación de las aplicaciones será mediante protocolo OAuth/OpenID Connect.

En la figura 7.16 se muestra como es la configuracion para poder integrar la aplicación por medio de OAuth/OpenID. Primero debe estar seteado dicho protocolos de federación, en este caso aparecen seteados además de OAuth & OpenID Connect los protocolos de SAML.

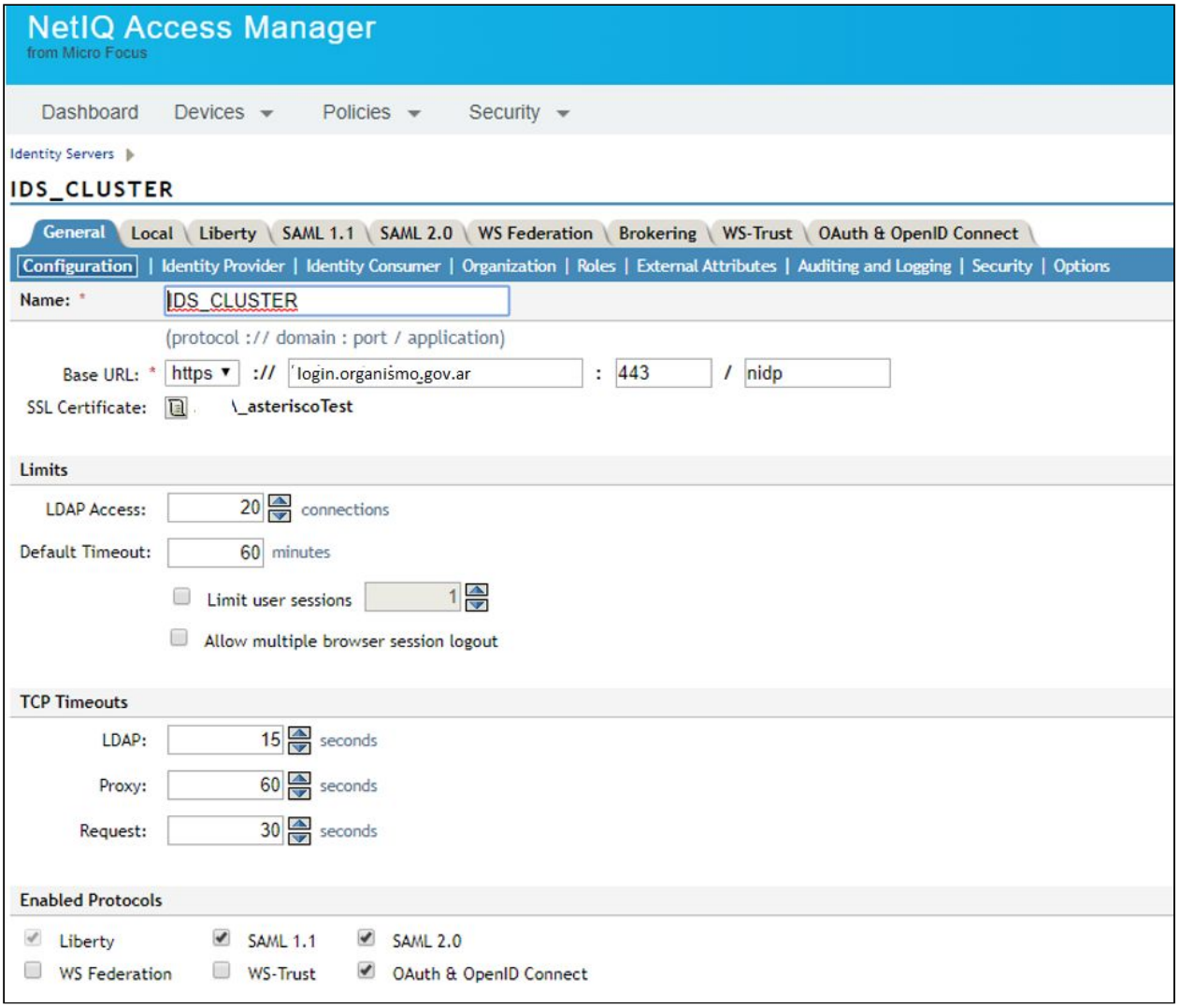


Figura 7.16: Habilitación de protocolos de federación

Después de tener la habilitación de dichos protocolos de federación, en la pestaña OAuth & OpenID Connect se debe registrar la nueva aplicación a federar.
En la figura 7.17 se muestra la configuración necesaria para poder registrar una aplicaciones OAuth. En primer lugar, la aplicación deberá estar registrada en Access Manager con los siguientes datos (se marcan los relevantes):

- Client ID: Identificador de la aplicación que realiza la solicitud
- Client Type: Todas son Web Based
- Callback URL: Ruta a la que debe redirigir al usuario una vez autenticado

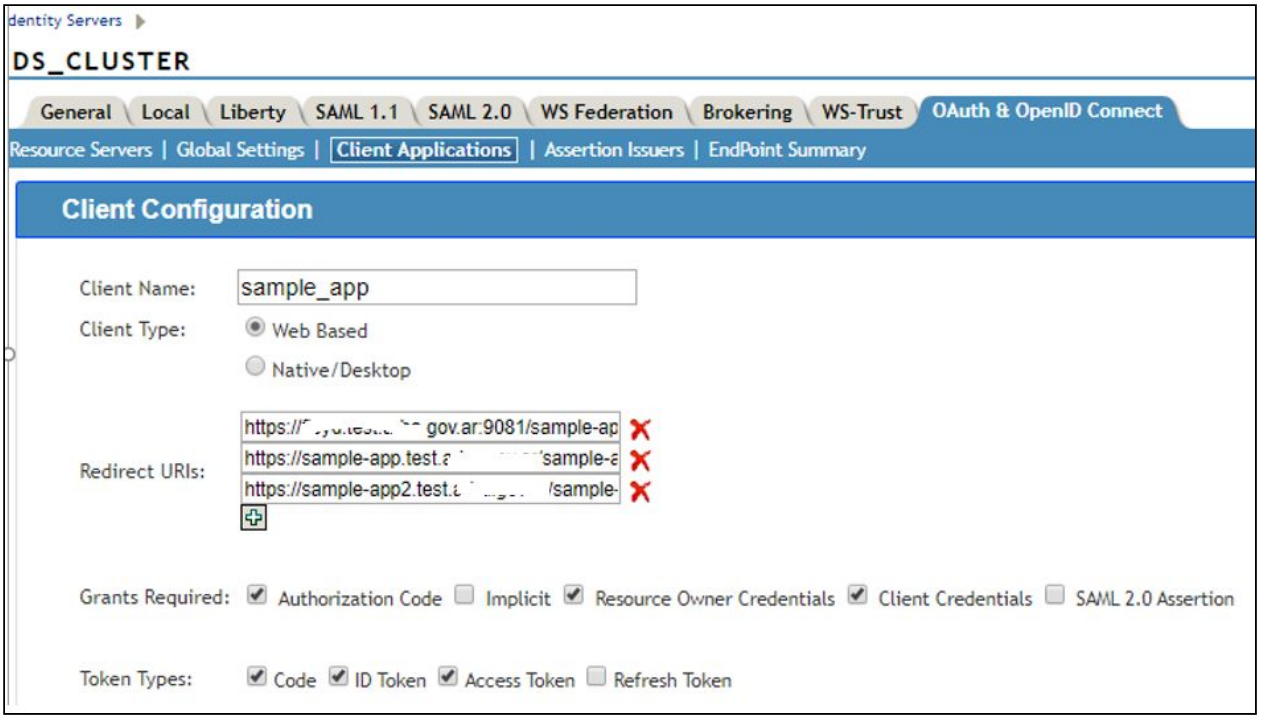


Figura 7.17: Seccion OAuth & OpenID Connect - Client Application

En la figura 7.18 vemos un listado de las aplicaciones ya registradas.

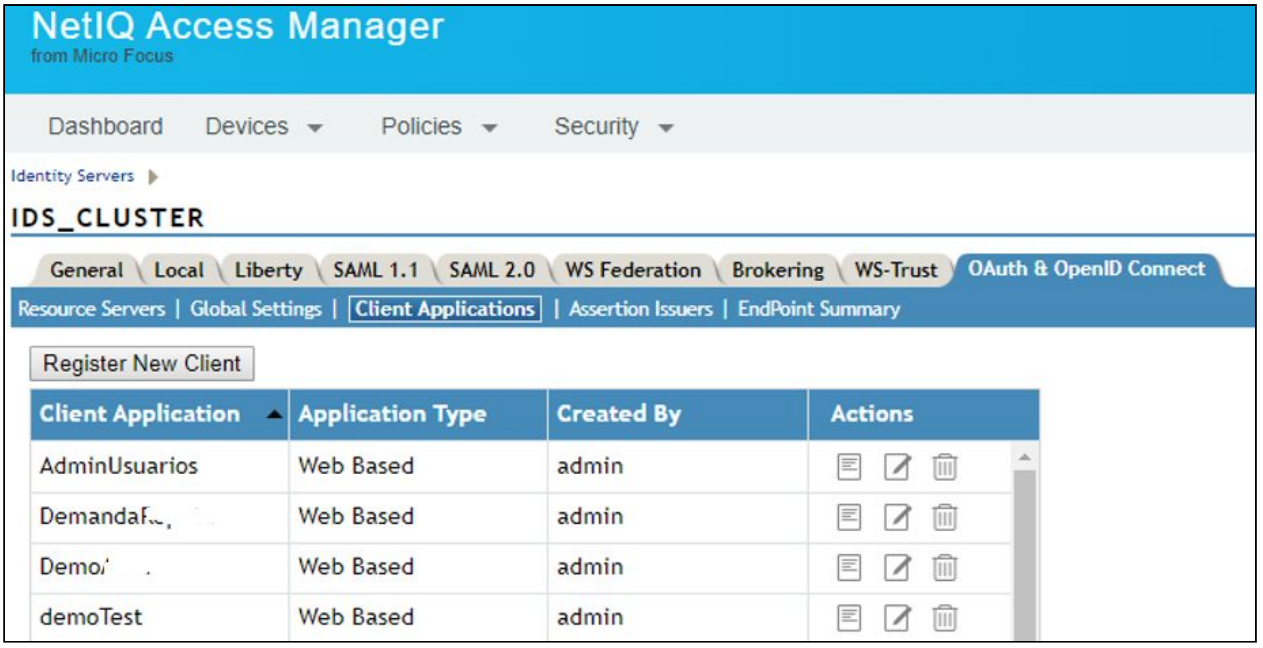


Figura 7.18: Aplicaciones registradas

7.4. Asegurando la Comunicación de los componentes con certificados

Por otro lado una de las características principales de una solución de Access Manager, consiste en la securización de las comunicaciones de las aplicaciones integradas mediante la utilización de Certificados Digitales. Esta securización será dada para cada uno de los aplicativos en cuestión que serán Acelerados.

- *Identity Server*: Utiliza certificados y almacenes de confianza para proporcionar autenticación segura al Identity Server y habilitar el contenido cifrado del portal del Identity Server, a través de HTTPS.

- *Access Gateway*: Utiliza certificados de servidor y raíces de confianza para proteger los servidores Web, proporcionar un inicio de sesión único y habilitar las funciones de confidencialidad de datos del producto, como el cifrado.

En la siguiente figura 7.19 se describen los canales de comunicación entre los diferentes componentes de Access Manager. La configuración de estos canales seguros pueden realizarse en su totalidad (lo recomendado en ambientes productivos), o elegir cuáles conexiones se realizarán seguras y cuáles no. En el proyecto para esta tesina se configuró todos los canales de comunicación como seguros.

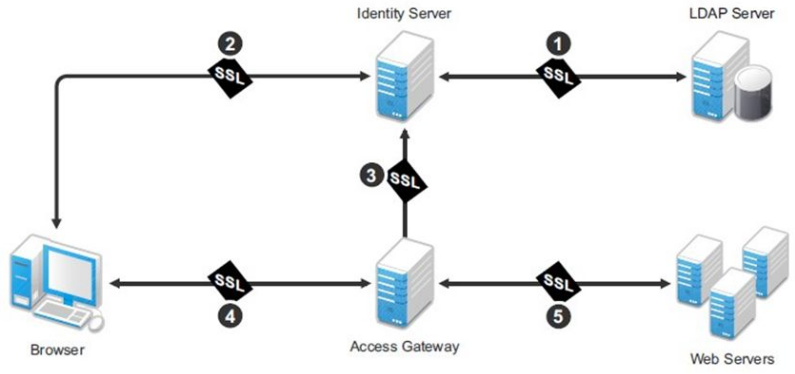


Figura 7.19: canales de comunicación ssl

1. Habilitación de SSL entre el cliente browser, Identity Server y Access Gateway (canales 2, 3, 4)

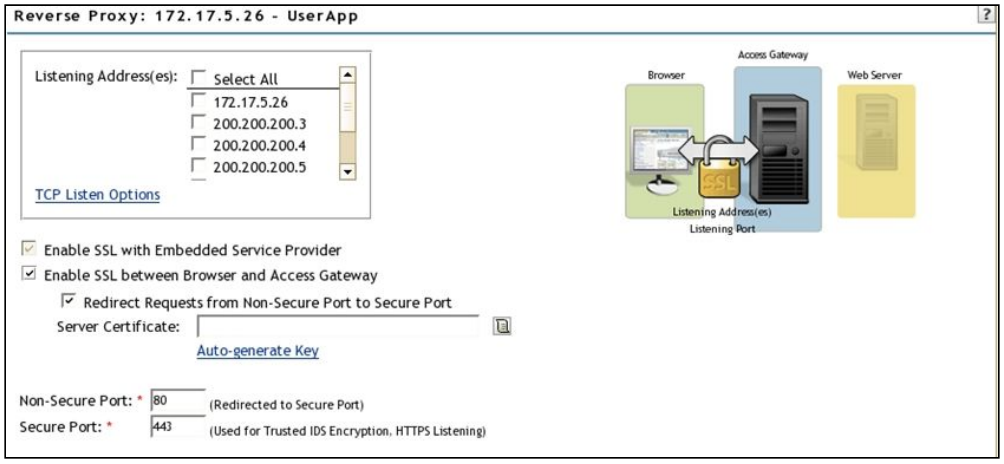


Figura 7.20: Selección de certificado digital para SSL entre Browser y Access Gateway

2. Habilitación de SSL entre Access Gateway y el Web Servers (canal 5)

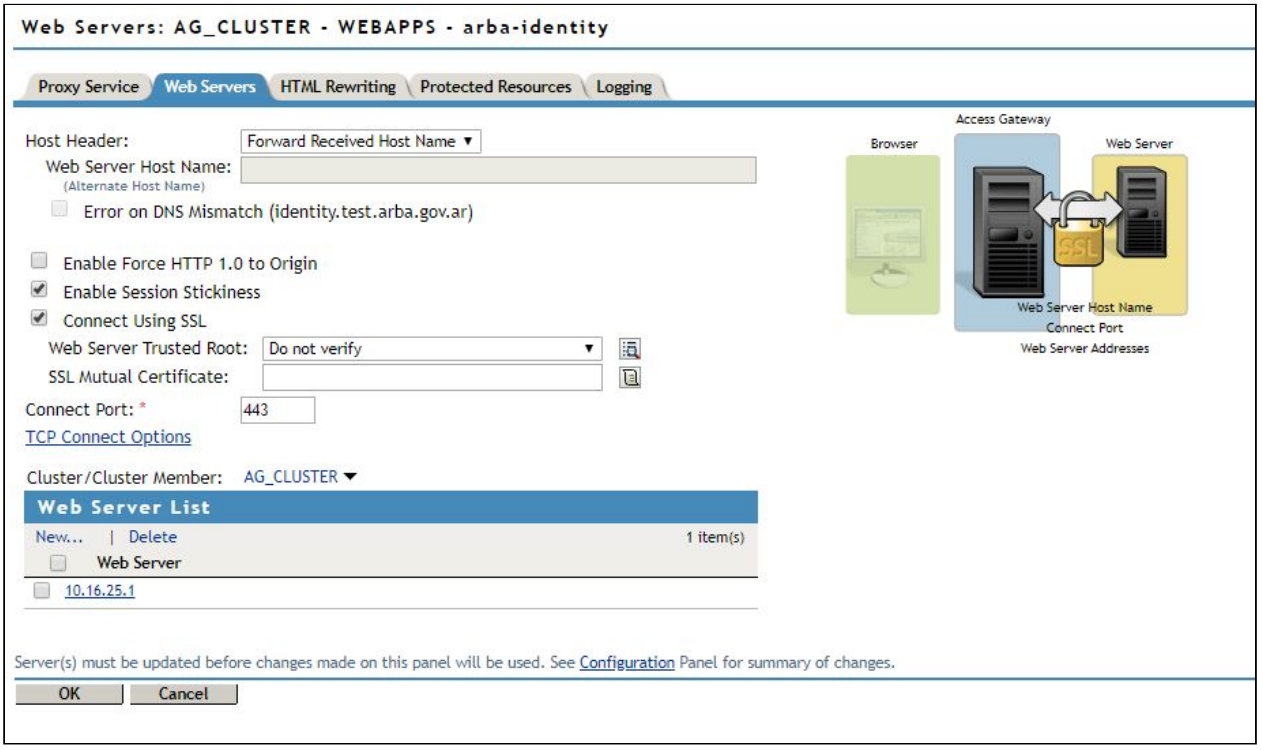


Figura 7.21: Selección de certificado digital para SSL entre Access Gateway y Web Server

Capítulo 8

Eventos de Seguridad

Como parte final de la solución de gestión de identidades y accesos implementada en el organismo, se instalo y configuro un sistema de repositorio de eventos de seguridad que procese y almacene los eventos que ocurran en dicha implementación.
Este solucion de eventos, es un sistema de logs centralizado que correlacione y normalice los diferentes eventos que generen los componentes de IAM en el organismo y que permita la generación de alarmas, reportes e información estadística del funcionamiento total.
Para ello se instalo y configuro la plataforma de recolección y correlación de eventos de seguridad del tipo SIEM (Security Information and Event Management)[20], mediante el producto también de la empresa NetIQ Sentinel.

La plataforma se configuró para la recepción de eventos los macro componentes auditados se mencionan a continuación:

- Repositorios de Identidades (eDirectory)
- Identity Manager
- Identity Applications
- Access Manager

8.1. Instalación del SIEM y configuración de colectores de logs

Se muestra a continuación el proceso realizado para la instalación de dicho producto SIEM y la integración de logs a auditar de las distintas plataformas.
El proceso de instalación del producto es mediante la ejecución de un script en Linux como se muestra en la figura 8.1

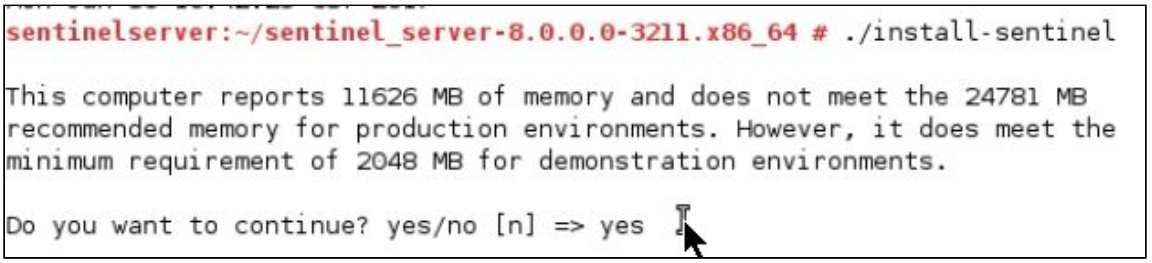


Figura 8.1: Instalación de Sentinel

Como información requerida se solicitan los parámetros típicos de una configuración de red: nombre de servidor DNS, dirección IP, puerta de enlace, usuario administrador , etc.

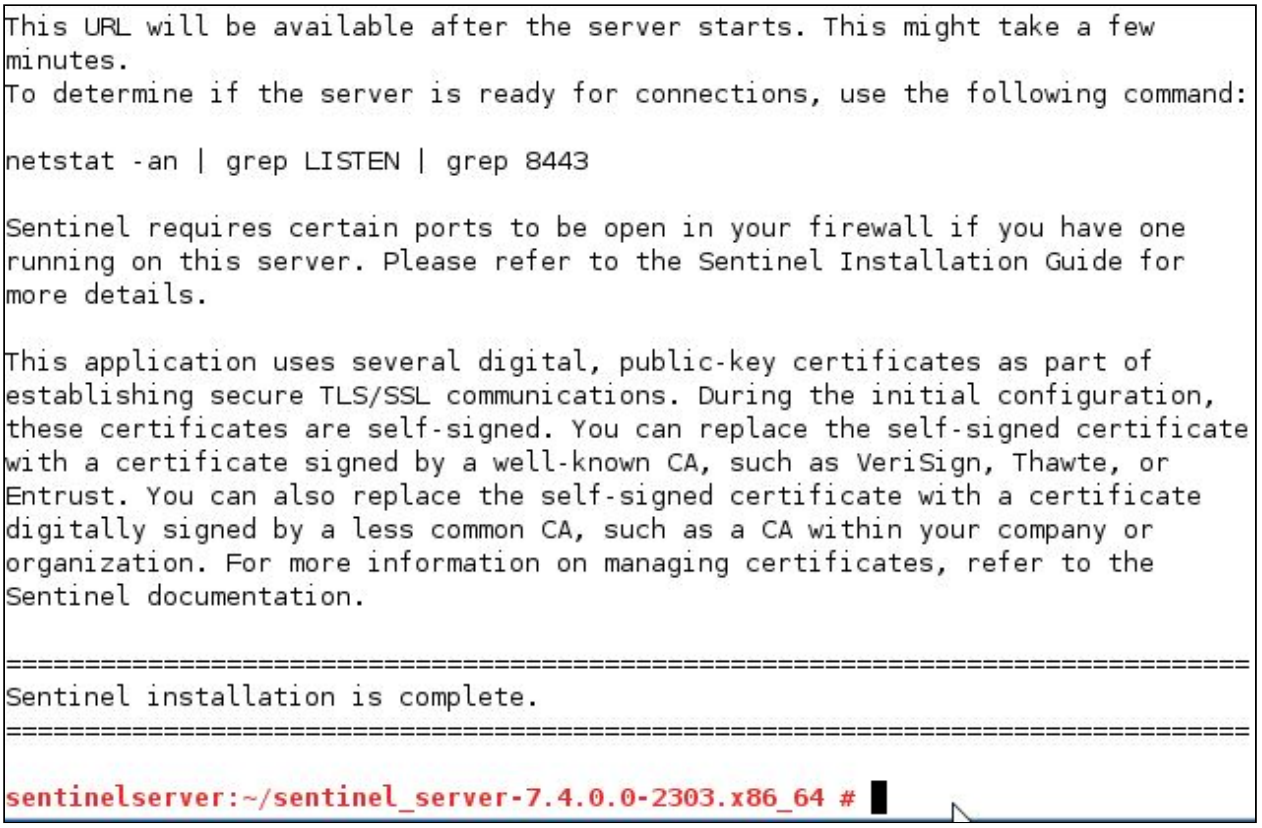


Figura 8.2: Finalización de proceso de instalación

Sentinel posee una administración web, que inicialmente muestra el logueo, con el que se ingresa con el usuario administración creado en al instalación del mismo

Figura 8.3: Inicio de login en Sentinel

Se muestra a continuación en la figura 8.4 la imagen inicial del servidor de logs, sin ningun evento reportado.
En el proyecto de Identity & Access Manager, los eventos son reportados al SIEM via Syslog, pudiendo luego este a través de un conector específico, poder procesar dichos eventos a auditar.

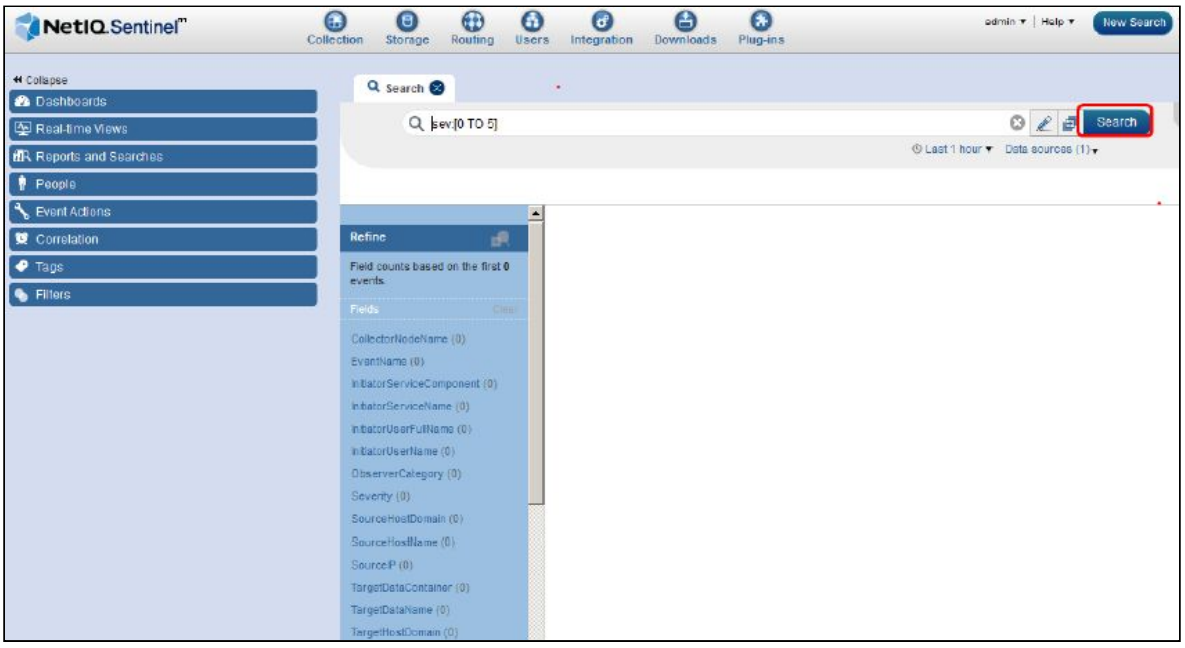


Figura 8.4: Pantalla inicial de Sentinel

Para que el SIEM procese y entienda dichos eventos generados en los distintos componentes de toda la solución de Identity & Access Management, deben ser agregador conectores específicos de cada plataforma, ya que con dicho conector tiene reglas específicas de parseo de logs.
En la figura 8.5 se muestra por ejemplo la agregación de un conector de Identity Manager

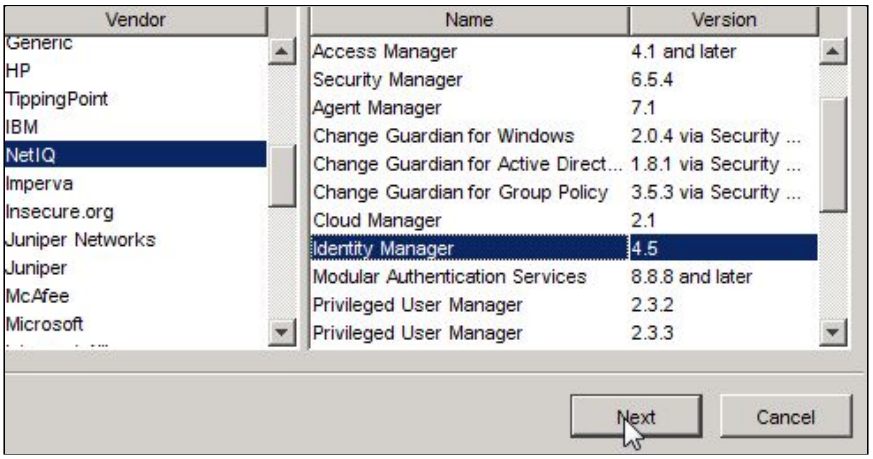


Figura 8.5: Conector de Identity Manager

Para el proyecto se instalaron los conectores necesarios tanto de la plataforma de Identity Manager, la de Access Manager y la del Metadirectorio LDAP eDirectory.
En la figura 8.6 se observa un ejemplo de los distintos conectores funcionando

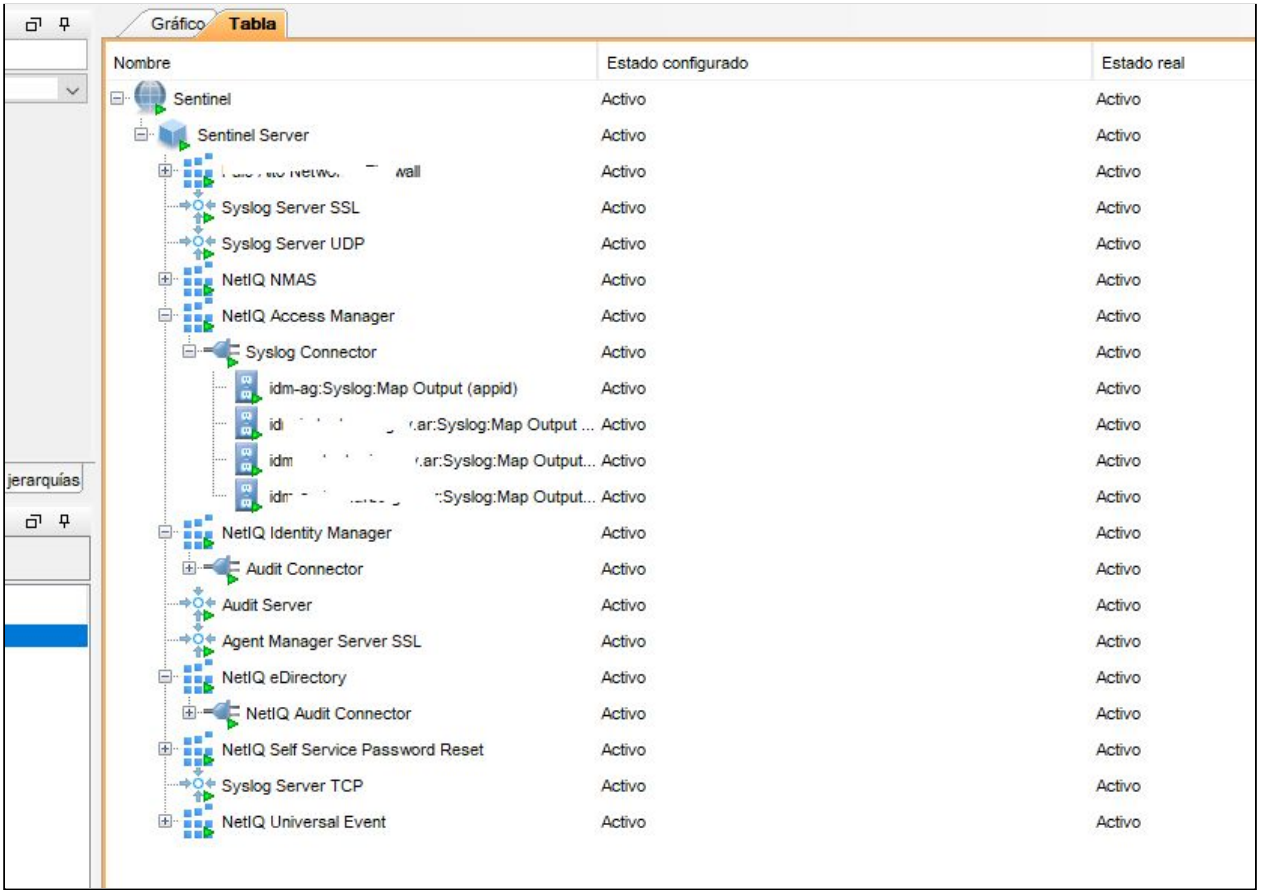


Figura 8.6: Conectores configurados en SIEM

Capítulo 9

Conclusiones y trabajos futuros

En el siguiente capítulo se describirán las conclusiones sobre el trabajo realizado y expuesto en esta tesina, como también los trabajos futuros que quedaron por implementar dentro del organismo.

9.1. Conclusiones

Entre las conclusiones que se pueden sacar sobre la implementación de este tipo de soluciones se destaca la mejora sustancial obtenida en la gestión de accesos a los sistemas informáticos y en los repositorios de información digital que se administra.
A su vez se logra asegurar un manejo transparente, seguro, auditable y eficaz del ciclo de vida de la identidad de los usuarios.
La correcta gestión del ciclo de vida de la identidad de usuario genera un impacto positivo en la disminución de costos administrativos, reduciendo la complejidad y el tiempo requerido en la administración de cuentas de usuarios, maximizando la continuidad y productividad operativa del organismo.
Otra de las consideración a resaltar, es que con esta implementación se cumple con las normativas vigentes en materia de Control de Accesos según se establece en la Política de Seguridad de la Información con la que debería contar el Organismo, en el marco de las buenas prácticas y los estándares de los Sistemas de Gestión de Seguridad de la Información (SGSI).
Finalmente, podemos destacar que se logra una considerable mejora en la calidad del servicio, reduciendo el tiempo de desarrollo y puesta en producción de nuevos servicios (no se tiene que desarrollar un nuevo método de acceso y autenticación cada vez que se desarrolle una aplicación).

9.2 Trabajos futuros

Como etapa final del proyecto de administración de accesos e identidades, uno de los accesos y control de usuarios mas importante y crítico es el de accesos como usuario privilegiado (llamado *root o superusuario* en ambientes Unix o *Administrator* en ambientes Windows) a los diferentes servidores de una infraestructura informática de un organismo que posea estas plataformas.
El principal inconveniente en ambientes tecnológicos de gran envergadura es la imposibilidad de mantener secreta y seguro dichos accesos y claves a los diferentes

servidores, ya que esta clave y acceso debe ser generalmente compartido por varios administradores o sectores dentro del organismo; creando así una brecha de seguridad muy importante.
Como parte de la solución de accesos administrados en servidores, en el caso de NetIQ, posee una solución del tipo Privileged Account Manager (PAM por sus siglas en inglés)[21], que permitirá al organismo que lo implemente, controlar y monitorear el acceso administrativo a sus servidores, dispositivos de red y bases de datos.
Dicho producto permitirá que los diferentes administradores de los servidores del organismo tengan permitido el acceso controlado a los sistemas sin exponer las credenciales administrativas a de sistemas, ya que proporciona una gestión de identidad privilegiada completa para ser usada durante un tiempo límite determinado.
Este sistema funciona guardando las credenciales del administrador de cualquier sistema ya sea Windows, Linux, aplicación, base de datos o hipervisores en una repositorio propio de credenciales privilegiada.
De esta forma cuando un usuario que sea administrador de sistemas necesite realizar alguna actividad en un servidor en particular, iniciará sesión con sus propias credenciales de usuario, y el sistema PAM verificará la política definida para acceder a esa sesión en particular. Luego, según la política, ingresa las credenciales del superusuario o root, lo que permite al usuario iniciar sesión con el administrador o las credenciales del superusuario.
Esta capacidad es útil cuando las credenciales de la cuenta privilegiada se comparten con más de un usuario, o en el caso del organismo, por más de un Departamento técnico.
Independientemente de la instalación de dicho producto, lo que se requiere como tarea principal es hacer un análisis de los actuales accesos privilegiados a los diferentes servidores que se posean en el organismo, los tipos de accesos que se permiten y los usuarios involucrados en dicho proceso.

Una vez implementado, este sistema de acceso privilegiado, permitirá por ejemplo:

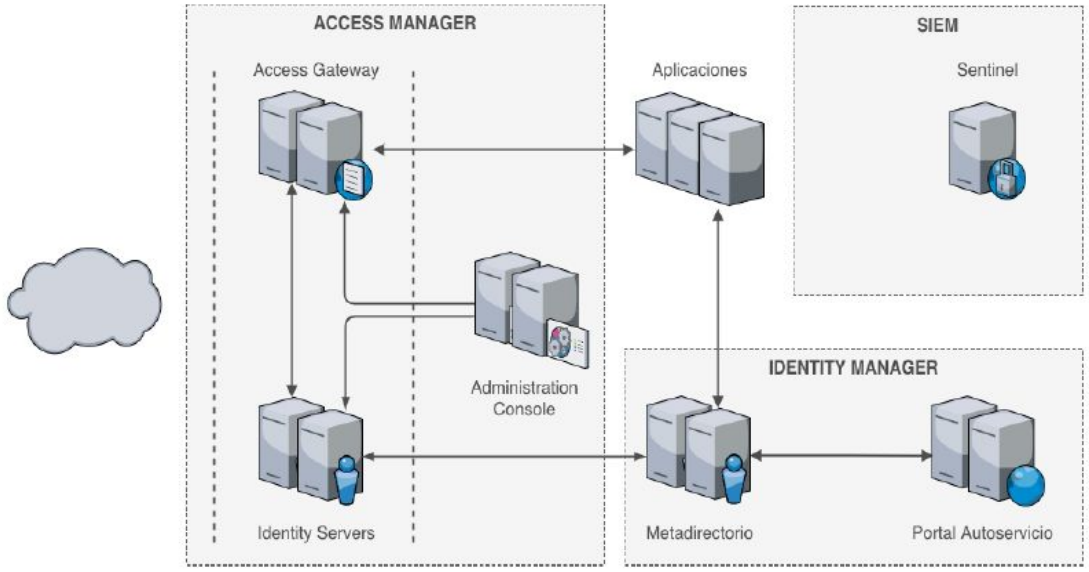
- Manejo de cuentas privilegiadas.
- Controlar el acceso administrador a los sistemas Linux, Unix, WIndows , base de datos y servidores de aplicaciones
- Manejo de políticas basadas en roles
- Monitoreo en tiempo real de actividades de un usuario que usa una cuenta privilegiada.
- La grabación en video de la sesión
- Manejo de claves SSH u otro tipo de claves
- Restricción del acceso al usuario según el tipo de administrador que sea.
- Integración con Identity Manager
- Integración con Access Manager

ANEXO: Diseño Físico de la Implementación

Para la implementación en el organismo se establecieron dos ambientes principales, el ambiente de producción (principal y redundante en servidores y servicios) para soporta toda la infraestructura IAM; y el ambiente de testing que permite las diferentes pruebas y testeos de nuevas características desarrolladas, pruebas de actualizaciones de nuevas versiones, parches de seguridad, etc.

Ambiente de Producción:

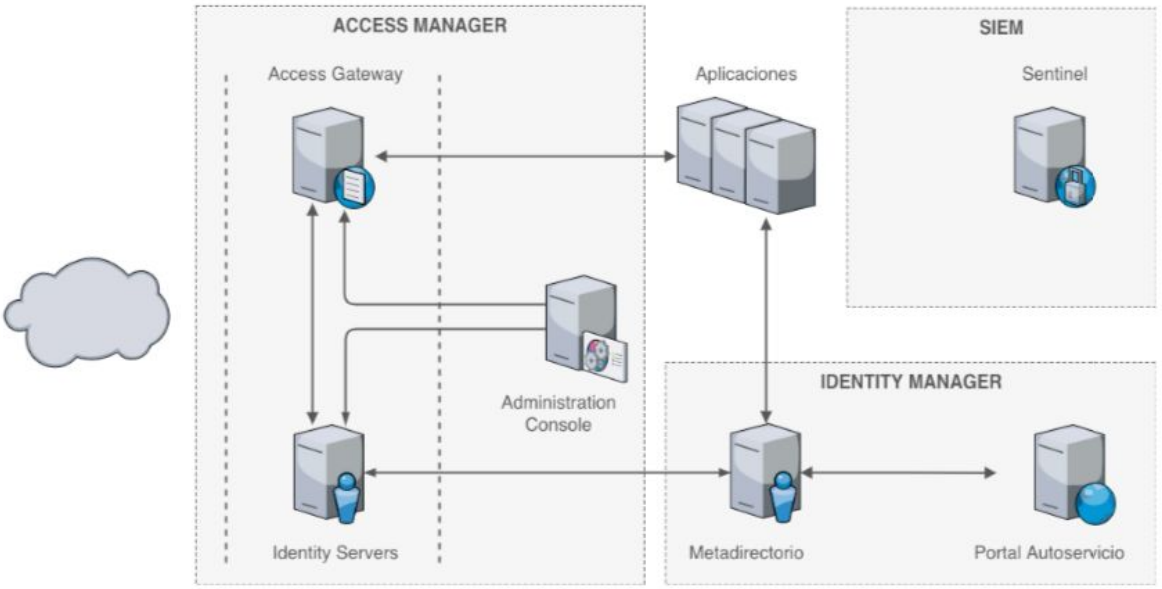
El modelo de diseño física está desarrollado sobre tres servicios lógicos, distribuidos en once máquinas físicas. Esta arquitectura puede estar centralizada o distribuida en forma física, de acuerdo a las necesidades del organismo.
En el caso puntual del ambiente de producción, se puso foco en la alta disponibilidad de la solución para el Metadirectorio, el Portal de Autoservicio y todos los componentes del Access Manager debido a su criticidad para el negocio.
Para el caso de la plataforma de auditoria, considerando que la arquitectura de los eventos manejados por los distintos componentes es del tipo store-and forward, no se considera alta disponibilidad dado que ante una pérdida del servicio, los eventos no recibidos y almacenados en la base de datos, permanecen en la fuente de origen hasta que se restablezca la solución.



Para la sincronización de eventos desde el Metadirectorio hacia la plataforma de Active Directory y creación de cuentas en el sistema de correo electrónico Exchange se requiere la instalación del componente de Remote Loader. Este agente será instalado en un servidor del tipo Windows aparte.

Ambiente de Test

El objetivo de contar con un ambiente de test, es tener un entorno aislado del de desarrollo, y que simule un entorno real pero sin el riesgo de afectar el entorno productivo ni la operación de la organización, en el cual se puedan realizar todas las pruebas definidas en la metodología previo a los pasos a producción.
En este sentido resulta fundamental que este entorno refleje en la mayor medida posible las características lógicas de de producción.
La arquitectura de este entorno es similar a la de producción con menor capacidad de hardware (por ej. En este entorno no se cuenta con réplica y/o redundancia de servidores).



Referencias Bibliográficas

[1] https://es.wiktionary.org/wiki/identidad
[2] Enterprise Identity Management, D. Royer.
[3] Identity Management: Concepts, Technologies and Systems, E. Bertino and K. Takahashi.
[4] ISO27000, Information technology - Security techniques - Information security management systems.
[5] Digital Identity, P. J. Windley.
[6] Gestión de Identidades y Control de Acceso desde una perspectiva organizacional, Montoya S., Restrepo R. 2012
[7] https://searchdatacenter.techtarget.com/es/definicion/IAM-o-Sistema-de-gestion-de-accesos-e-identidades
[8] Designing an IAM Framework with Oracle Identity and Access Management. McGraw Hill. J. Scheidel. 2010.
[9] Kerberos: An Authentication Service for Computer Networks, B. C. Neuman and T. Ts'o.
[10] Understanding LDAP Design and Implementation, 2nd edition ed., IBM Redbooks, 2004, S. Tuttle, A. Ehlenberger, R. Gorthi, J. Leiserson, R. Macbeth, N. Owen, S. Ranahandola, M. Storrs and C. Yang
[11] Managing Enterprise Complexity: The Use of Identity Management Architecture to control Enterprises Resources; Peter White
[12] Identity Manager v4.7: https://www.netiq.com/documentation/identity-manager-47
[13] eDirectory v9.1: https://www.netiq.com/documentation/edirectory-91
[14] Access Manager v4.4: https://www.netiq.com/documentation/access-manager-44
[15] iManager v3.1 https://www.netiq.com/documentation/imanager-31
[16] Quick Start Guide for Installing NetIQ Identity Manager 4.7.pdf
[17] NetIQ Access Manager 4.4 Administration Guide.Seccion How Access Manager Solves Business
Challenges
[18] NetIQ Access Manager 4.4 Installation and Upgrade Guide. Seccion Deployment Models
[19] NetIQ Access Manager 4.4 Administration Guide. Seccion Understanding Access Manager Flow
[20] NetIQ Sentinel SIEM
https://www.microfocus.com/es-es/products/netiq-sentinel/overview
[21] NetIQ Privileged Account Manager
https://www.netiq.com/documentation/privileged-account-manager-37/

[22] NetIQ Designer
https://www.netiq.com/documentation/idm402/designer_intro/data/front.html