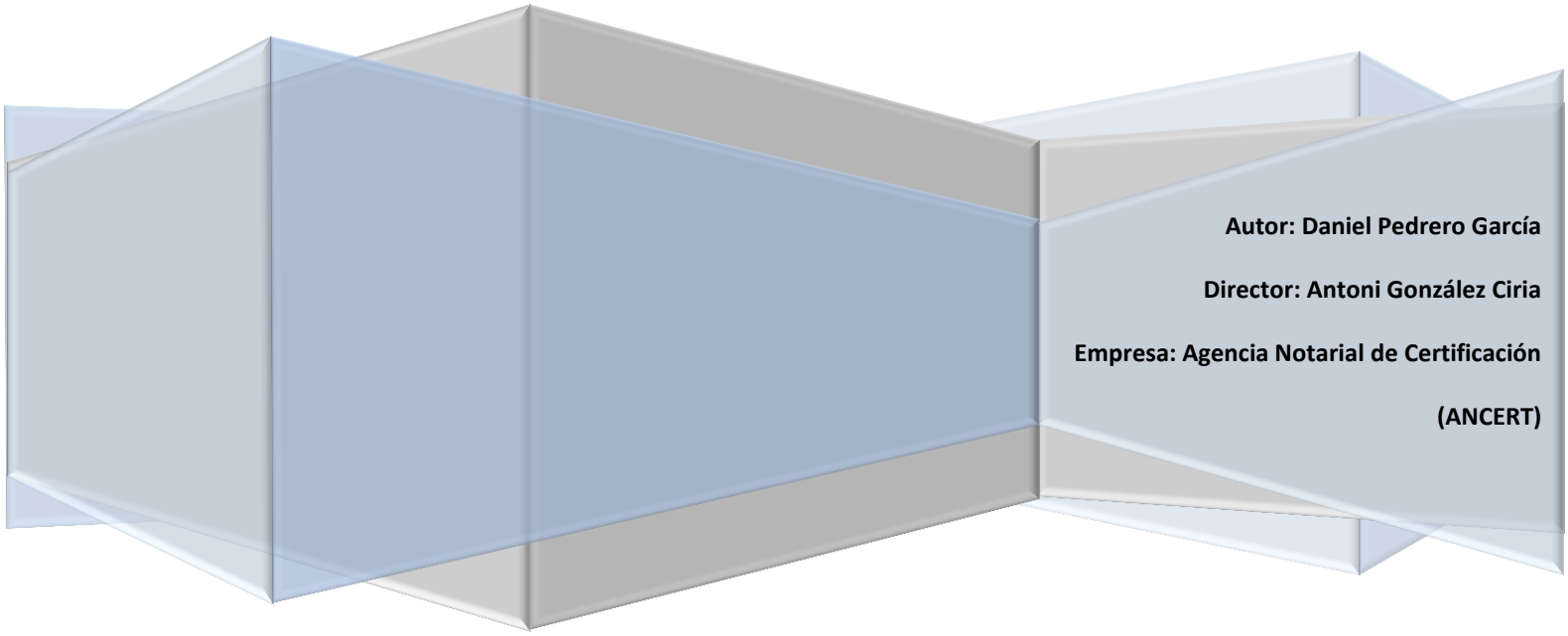
Universidad Oberta de Cataluña

Trabajo Final de Máster: Implantación de un mecanismo de Single Sign-On (SSO)

Máster Universitario de Seguridad de las Tecnologías de la Información y las Comunicaciones



Autor: Daniel Pedrero García

Director: Antoni González Ciria

Empresa: Agencia Notarial de Certificación (ANCERT)

Tabla de contenido

Resumen

Este proyecto es realizado como trabajo final de los estudios del Máster Universitario de Seguridad de Tecnologías de la Información y las Comunicaciones, impartido por la universidad Oberta de Cataluña en colaboración directa con ANCERT, la Agencia Notarial de Certificación. Este trabajo se centra en sistemas de autenticación y autorización de usuarios, más concretamente en la implantación de un mecanismo de Single Sign-On (SSO).

A lo largo de esta memoria se describirá detalladamente las distintas fases que se han afrontado a lo largo del proyecto, empezando desde la fase inicial de análisis y toma de requisitos hasta la implantación final de la solución elegida.

Más concretamente se describirá en qué consisten estos sistemas de SSO y por qué son tan importantes en la actualidad, se introducirán algunos conceptos teóricos necesarios para la correcta comprensión de este proyecto y se detallarán los aspectos más importantes de la instalación y configuración de la infraestructura física y lógica necesaria para la implantación de esta solución.

Abstract

This paper is a final work of the studies of the University Master of Security of Information and Communications Technologies. These studies are taken in Oberta University of Cataluña in collaboration with ANCERT company.

This paper is based on users authentication and authorization systems, specifically in Single Sign-On systems. In this paper, we describe all project phases since the analysis and requirements of the solution to the implementation of the final Project.

This work will respond to what are these SSO system, how works these implementations and why are they so important today. This paper introduce some theoretical concepts necessary for a correct understanding of this project, also it will detail the most important aspects of the installation and configuration process of the solution.

Introducción

En esta sección se describe uno de los elementos más importantes de cualquier gestión de proyectos, la planificación del proyecto. En este apartado, se describirá toda la información básica sobre el proyecto que se plantea en esta memoria:

- Partes implicadas en el proyecto.
- Descripción detallada del problema a resolver.
- Definición de objetivos.
- Descripción de la metodología utilizada.
- Definición hitos.
- Cronograma temporal de tareas.

Partes implicadas

Este proyecto es realizado por Daniel Pedrero García como trabajo de fin de máster de los estudios realizados en el máster universitario de seguridad de las tecnologías de la información y las comunicaciones impartido por la universidad Oberta de Cataluña y con la colaboración de la Agencia Notarial de Certificación (ANCERT).

Descripción del problema

Actualmente la tecnología está prácticamente al alcance de cualquiera, llegando a ser algo inherente al ser humano. La usamos en todos los aspectos de nuestra vida, desde la parte personal, como puede ser un medio de relaciones sociales, su uso en el hogar, en nuestras compras, los desplazamientos, como en nuestra vida profesional independientemente de que trabajemos o no en un sector tecnológico.

La tecnología está totalmente integrada en nuestras vidas, en un mundo globalizado, donde la información es el principal recurso y donde hacemos más uso de nuestra identidad digitalmente que presencial, identificándonos en multitud de aplicaciones, cada una de ellas con un método independiente de verificación de identidad, aumentando así la complejidad de gestión de las identidades y autorizaciones, creciendo exponencialmente conforme crece el número de usuarios.

En este punto, hay que tener en cuenta que, mientras más dependemos de la tecnología para identificarnos y para almacenar toda nuestra información personal, más prioridad hay que dar a la seguridad de la información digital, sin que esto incurra en una mayor complejidad para el usuario final.

Objetivos

Este proyecto se centra en los pilares básico de la seguridad de la información, como son:

- **La confidencialidad**: Se basa en la protección de la información frente a accesos no autorizados. Estos accesos son gestionados mediante la aplicación de políticas de seguridad, que permiten únicamente el acceso a los datos a los usuarios o sistemas que han superado el proceso de autenticación de identidad.

- **La disponibilidad**: Hace referencia a la capacidad de que la información esté disponible en todo momento. Para ello, se suele aplicar redundancia tanto en el hardware como en el software que proteja los sistemas ante caídas o saturaciones de los medios de acceso a la misma. No hay que olvidar las protecciones contra el borrado intencionado o involuntario de información.

- **La integridad**: Hace referencia a la inalterabilidad de la información, protegiéndola contra modificaciones no autorizadas o borrados parciales de los datos. Para ello es necesario identificar el propietario de los datos y los permisos asignados a cada usuario sobre ellos.

Para garantizar el cumplimiento de los principios de seguridad de la información que se han descrito, se propone la implantación de un único sistema de autenticación centralizado (SSO de su nombre en inglés, Single Sign On), orientado a aplicaciones corporativas, que se distribuya bajo licencia Open Source y que controle el acceso a diferentes aplicaciones sin necesidad de realizar diversos procesos locales de autenticación. En los siguientes apartados se describirá de manera detallada en qué consisten estos sistemas de autenticación, los tipos de soluciones que existen en el mercado y las ventajas que suponen su implantación en una empresa.

Metodología

Para el desarrollo de este proyecto no se cuenta con una implantación inicial, y por tanto, se deben realizar todas las fases necesarias para afrontarlo desde cero. Partiendo de la base de que este proyecto se centra en un caso más practico que teórico, se va a seguir una serie de etapas que se ejecutarán de manera secuencial o en cascada:

Análisis y toma de requisito

Durante esta etapa se evaluarán todas las medidas técnicas que sean necesarias para poder desplegar la solución propuesta. Por ejemplo, el despliegue de:

- Servidor DNS
- Servidor LDAP
- Servidor de Active directory
- Segmentación de red
- Servidor proxy
- Servidor de aplicaciones

Por otro lado, se definirán los requisitos necesarios para la elección del software adecuado en base a restricciones y funcionalidades como:

- Debe estar basada en código abierto.
- Permitir distintos tipos de autenticación.
- Permitir recuperar información del usuario autenticado.
- Número de usuarios concurrentes.
- Posibilidad de clusterizar la solución.

Diseño de la solución

Tras la toma de requisitos y análisis, se procederá con el diseño de la solución a implantar en base a todos los datos recogidos en la primera etapa del proyecto. En este caso concreto que no se dispone de un entorno de partida, se debe dimensionar el despliegue del mismo en base a las necesidades expuestas.

Implementación

Esta etapa se puede dividir en dos partes:

- Infraestructura: Despliegue del entorno necesario para la implantación de la solución de SSO.
- Software: Todas las configuraciones necesarias para el correcto funcionamiento del sistema de autenticación centralizada de usuarios.

Cronograma

Para la planificación de las distintas fases que se han mencionado en el apartado de metodología, se ha de tener en cuenta la duración del proyecto y los plazos de entrega marcados en el plan docente. Por tanto, tomando como base el cronograma que se ha definido para el TFM, utilizaremos los entregables de las pruebas de evaluación continua (PEC) como hitos del proyecto y definiremos el contenido de cada uno de ellos:

Se procede con la descomposición de cada hito en tareas:

Hito 1:

Este hito tiene como fecha de inicio el 06 de marzo de 2019 y fecha de entrega 02 de abril de 2019 y comprende las fases de análisis y diseño del proyecto:

Fase de análisis:

- Existencia de un entorno de partida
- Requisitos de infraestructuras
- Requisitos del aplicativo
- Funcionalidades de la solución
- Seguridad de los sistemas

Fase de diseño:

- Dimensionamiento de la solución
- Estructura del entorno de desarrollo
- Elección de la solución de SSO
- Aplicativos a integrar en la solución
- Políticas de seguridad a implementar

Hito 2:

Este hito tiene como fecha de inicio el 03 de abril de 2019 y fecha de entrega 30 de abril de 2019 y comprende las fases de implementación del proyecto:

Fase de implementación:

- Infraestructura
  El despliegue de la infraestructura se realizará mediante una capa de virtualización.
  - Despliegue de DMZ
    - Proxy de aplicaciones
    - Servidor de DNS
    - Configuración de red
    - Sistema firewall
  - Despliegue de LAN
    - Servidor de aplicaciones
    - Servidor de Active directory
    - Servidor de SSO
- Software
  - Configuración DMZ
    - Configuración de servicio DNS
    - Configuración de reglas de proxy
    - Configuración de política de red perimetral

- Configuración LAN
    - Configuración de Active directory /LDAP
    - Configuración de servidores web
    - Despliegue del servicio de SSO
    - Configuración de políticas de acceso
    - Securización de aplicativos corporativos

Hito 3:

Este hito tiene como fecha de inicio el 01 de mayo de 2019 y fecha de entrega 04 de junio de 2019 y se basa en la redacción de memoria del proyecto:

- Recopilación de información del proyecto
- Estructuración de la memoria
- Redacción final

Hito 4:

Este hito tiene como fecha de inicio el 05 de junio de 2019 y fecha de entrega 11 de junio de 2019 y se basa en la presentación en video del proyecto:

- Redacción de la presentación
- Grabación de la defensa

Hito 5:

Este hito tiene como fecha de inicio el 17 de junio de 2019 y fecha de entrega 21 de junio de 2019 y se basa en la defensa del proyecto.

- Defensa del proyecto de forma telemática ante un tribunal.

Fundamentos teóricos

Sistemas de virtualización

A grandes rasgos la virtualización consiste en la emulación mediante software del funcionamiento de una infraestructura de servidores real, proporcionando un entorno de ejecución idéntico al físico.

Un entorno virtualizado permitirá ejecutar diversos sistemas operativos en un único servidor físico. Cada sistema operativo reside en un contenedor de software totalmente independiente, comúnmente denominado máquina virtual (VM). Sin embargo, el pool de recursos usado por estas máquinas virtuales es compartido, es decir, todas las máquinas virtuales comparten la misma memoria, CPU, almacenamiento y el resto de recursos disponibles del servidor físico.

Características

La virtualización se caracteriza por proporcionar:

- **Encapsulación**: Paquete de software que incluye todo el hardware virtual, sistema operativo y aplicaciones necesarias.
- **Aislamiento**: Aunque las máquinas virtuales comparten los recursos del servidor físico en el que residen, están totalmente aisladas como si se trataran de máquinas independientes.
- **Compatibilidad**: Una máquina virtual consta de los mismo componentes qué una física por tanto es totalmente compatible con los sistemas operativos y aplicaciones.
- **Independencia del hardware**: Las máquinas virtuales son completamente independientes del hardware físico del que disponen.
-

Ventajas

La virtualización de sistemas proporciona un gran número de ventajas respecto a las soluciones físicas tradicionales, como puede ser:

- Proporciona alta disponibilidad de las máquinas virtuales y por tanto de las aplicaciones, asegurando que los servicios permanezcan operativos reduciendo drásticamente el tiempo de inactividad de los sistemas debido a un fallo físico del servidor o mantenimientos planificados.
- Gestión centralizada y ágil de toda la infraestructura virtual. Reduciendo costes de aprovisionamiento y mantenimiento.
- Supervisión constante de las máquinas físicas y virtuales.
- Consolidación de recursos.
- Automatización de la gestión dela infraestructura dontándola de mayor **rendimiento, escalabilidad y disponibilidad.**
- Reducción de costes en adquisición de infraestructura.
- Reducción de gastos energéticos.

Sistemas de Single Sign-On.

Definición

Los sistemas de Single Sign-On (SSO) permiten la centralización de los distintos procesos de autenticación local en una única instancia de identificación de los usuarios. Como su nombre indica es un inicio de sesión único, permitiendo hacer uso de los distintos servicios protegidos por este tipo de soluciones sin necesidad de afrontar varios procesos de validación de la identidad del usuario.

Los sistemas de Single Sign-On nos permiten simplificar drásticamente los procesos de autenticación de los accesos a recursos, servicios y aplicaciones que debemos gestionar a diario. Este tipo de sistemas permiten tener una gestión simplificada y un mayor control de todos los procesos de validación de identidad de los usuarios, pudiendo llegar a permitir el uso de varios tipos de autenticación en función de la sensibilidad del acceso solicitado, incluso el uso de sistemas de múltiple factor de Autenticación (MFA), gestión de sesiones, entre otras funcionalidades que comentaremos más adelante.

Los sistemas de Single Sign-On no solo facilitan el proceso de gestión para el personal TI, sino que también ayuda enormemente a los usuarios en el uso de las aplicaciones personales o corporativas que usan en su día a día. Estos sistemas permiten que con una única instancia de validación de identidad el usuario pueda hacer uso de sus aplicaciones a las que tienen acceso, haciendo que la experiencia del usuario sea más cómoda y ágil.

Tipos de soluciones

Una vez definido a grandes rasgos lo que es un sistema de SSO, vamos a indicar los diferentes tipos de SSO que se pueden usar en función de las necesidades de cada caso:

- **Enterprise Single Sign-On (E-SSO)**: Estos sistemas también son conocidos como legacy SSO y son usados como sistemas de autenticación primaria, permitiendo la interacción con otros sistemas que permitan deshabilitar la interfaz de autenticación de usuarios. Este tipo de sistemas interceptan las peticiones de autenticación con el fin de autocompletar esta información de forma automática.

- **Web Single Sign-On (Web-SSO):** Estos sistemas se centran únicamente en recursos y aplicaciones que son accedidas mediante vía web. En este caso, es habitual el uso de servidores proxy donde se centralizan los servicios web, donde son capturadas todas las peticiones de autenticación, redireccionadas al sistema de SSO y una vez validadas devueltas al recurso solicitado.

- **Kerberos:** sistema de autenticación externa ampliamente extendido. Durante el proceso de autenticación contra un servidor kerberos, se realiza la asignación de un tiquet, el cual será usado posteriormente por las distintitas aplicaciones y servicios para su identificación.

- **Identidad federada**: Se basa en el uso de estándares, permitiendo a las empresas compartir información sobre gestión de la identidad para realizar la validación del usuario sin tener que identificarse en ambas soluciones, ni compartir ningún tipo de información privilegiada. En este tipo de sistemas, los usuarios pueden validarse de forma única entre diversas soluciones, las cuales no tienen por qué estar en la misma red ni basarse en la misma tecnología.

- **Open ID:** En este tipo de SSO la identidad del usuario es compilada en una URL siendo accesible por las diversas aplicaciones o servicios que requieran validad la identidad del usuario. Esta solución es distribuida y descentralizada y los recursos protegidos solo requieren del identificador del usuario asociado al servicio de OpenID.

Fortalezas de la solución

Como se ha comentado con anterioridad, la implantación de sistemas de Single Sign-On facilita las labores de gestión de los procesos de verificación de la identidad, teniendo multitud de ventajas como:

- Gestión centralizada de multitud de procesos de validación de usuarios.

- Reducción de personal y tiempo de dedicación a la gestión de usuarios. Teniendo un menor número de procesos de autenticación, y por tanto, un menor número de incidencias y un menor número de bases de datos que gestionar.

- Permite tener un mayor nivel de seguridad, gestión centralizada de políticas de seguridad, pudiendo implantar sistemas más estrictos de autenticación en función de la sensibilidad del recurso o aplicación. Además de una reducción importante de la posibilidad de fallos de seguridad por factor humano.

- Mejora de la experiencia del usuario durante el proceso de autenticación en las herramientas corporativas o personales. Mediante una única fase de validación global de la identidad de usuario, podrá acceder a todos los sistemas sobre los que tiene autorización, reduciendo así el número de credenciales que debe gestionar.

Riesgos de la solución

Como se ha comentado, los sistemas de Single Sign-On se focalizan en el proceso por el cual se identifica digitalmente a cada persona de manera centralizada, permitiendo el acceso a diversas aplicaciones mediante un único proceso de autenticación. Este planteamiento conlleva un riesgo muy evidente, si un usuario malintencionado descubre el secreto con el que el usuario legítimo valida su identidad, digamos por ejemplo una contraseña, tendrá acceso a todas las aplicaciones que estén bajo el control del sistema de SSO, con el nivel de privilegio que se haya concedido al usuario en cada una de ellas. Como medida complementaria para evitar este problema se podría implantar un sistema de múltiple factor de autenticación (MFA) que muchos sistemas de SSO incluyes como módulos dentro de la solución.

Soluciones disponibles

Evidentemente existen multitud de soluciones empresariales de Single Sign-On en el mercado, algunas de las más destacadas pueden ser:

- Okta
- LastPass
- One Login
- Ldaptive
- CAS
- OpenAM
- Microsoft Azure AD
- RSA SecurID

Estas son algunas de las soluciones disponibles pero existen muchas más soluciones, algunas basadas en código abierto y otras versiones Enterprise que requieren de adquisición de licencia. Para la elaboración de este proyecto es requisito indispensable que la solución elegida se base en código abierto, entre otros requisitos.

Análisis de la solución

En este apartado se evaluarán los requisitos de hardware y software necesarios para la implantación de la solución y se valorarán las soluciones disponibles que cumplan con todas las características necesarias y se estimarán los recursos que serán necesarios como mínimo para poder dimensionar el entorno de implantación.

Requisitos de la solución

Como ya se ha explicado con anterioridad, las implantaciones de una solución de Single Sign-On (SSO) tienen asociadas una serie de necesidades implícitas por el tipo de implantación que se plantea en este proyecto. Estas necesidades se definirán a continuación:

- La solución propuesta debe basarse en código abierto.
- La autenticación de usuarios debe permitir como mínimo:
    - Autenticación tradicional por usuario y contraseña.
    - Autenticación mediante certificado digital.
- Diferenciación entre mecanismos de autenticación utilizados.
- Debe permitir definir una capa de proxy situada en segmentos de red distintos.
- Debe permitir escalado automático de privilegios.
- Debe permitir recuperar información relativa al usuario autenticado.

Respecto al entorno donde se va a desplegar la solución de SSO, se requiere como mínimo la implantación de los siguientes sistemas virtuales:

- Segmentación de red virtual
    - Definición de una red de área local (LAN)
    - Definición de una zona desmilitarizada (DMZ)
- Sistemas virtualizados
    - Servidor de Active Directory
    - Servidor de DNS
    - Servidor de aplicaciones
    - Servidor proxy
    - Sistemas cortafuegos

Como se puede comprobar, se requiere la segmentación de la red como medida de seguridad, aislando el servidor de aplicaciones situado en la LAN de accesos directos desde el exterior, forzando que este proceso se realice mediante un servidor proxy situado en la DMZ.

Análisis del producto

En base a los requisitos expuestos, se realiza el análisis de diversas aplicaciones que existentes en el mercado y se opta por una implantación de un sistema de Single Sign-On basada en una aplicación basada en código abierto llamada Open Access Management (OpenAM), la cual, cumple ampliamente con los requisitos necesarios para la implantación de la solución.

OpenAM es una solución que se distribuye bajo licencia de código abierto (Community) pero que también cuenta con una parte comercial. Esta versión Community nos permite, a grandes rasgos, la gestión centralizada de accesos a recursos en red generando un entorno único de validación de usuarios, por tanto, nos permite la implantación de una solución de SSO. Para ello, OpenAM centraliza los siguientes procesos:

- **Autenticación**: Proceso por el cual se verifica la identidad del usuario que requiere el acceso.
- **Autorización:** Proceso por el cual se verifica que el usuario autenticado (ya identificado) tiene los privilegios suficientes para realizar las acciones solicitadas sobre el recurso en cuestión.

La implantación de estos procesos es llevada a cabo mediante el despliegue de los módulos necesarios en casa caso. En función de la infraestructura de la que se disponga y las necesidades de seguridad de la empresa se puede llegar a encadenar procesos de autenticación para acceder a los recursos más sensibles.

Funcionalidades del aplicativo

Una vez definido el tipo de solución a afrontar, se procede a concretar las características por las que se decide su implantación para el despliegue de este proyecto:

- Autenticación
    - Permite interconectar distintos nodos de autenticación proporcionando varios servicios para ello.
    - Permite validación de usuarios de forma local y se puede integra con LDAP y Active Directory.
    - Permite validación de usuario mediante certificado digital.
    - Permite gestionar sesiones, permitiendo identificar al usuario durante su actividad en los recursos protegidos.
    - Permite definir niveles de autenticación a cada módulo en función de la confidencialidad del recurso.
    - Permite la implantación de múltiple factor de autenticación.
- Autorización
  Las autorizaciones de los usuarios se gestionan mediante políticas de seguridad donde se puede definir:
    - Las acciones que el usuario puede ejecutar sobre el recurso solicitado.
    - Limitaciones sobre el entorno como:
        - Horario laboral
        - IP origen

- Permite importar/exportar política XACML 3.0
- Permite definir grupo de políticas.

Requisitos del aplicativo

Una vez definida las características del aplicativo que se va a utilizar, se determinan las dependencias que son necesarias para su despliegue:

- Es una solución basada en Java y por tanto requiere de Java Development Kit
- Requiere de servidor web Apache
- Requiere instalación de Tomcat

Por último, Es necesario dimensionar correctamente la solución para poder proceder con un diseño correcto de la infraestructura sobre la que va a funcionar el sistema de SSO. Es muy importante saber de antemano:

- Número de usuarios que harán uso de la solución.
- Qué recursos se van a proteger.
- Medidas de seguridad perimetral que se van a implantar.
- Tipos de autenticación a usar.
- Niveles de autenticación que se desean definir.
- Si se implementará un entorno de alta disponibilidad.

Diseño de la solución

En este apartado de describe el diseño propuesto para la implantación de la solución elegida de SSO. Para ello se ha optado por la implantación de OpenAM como solución de Single Sign-On para la protección de los recursos web y aplicativos de la organización. Se ha diseñado el despliegue de una infraestructura virtual con todos los componentes necesarios para el correcto funcionamiento de la solución propuesta. Al ser un despliegue virtual será más sencillo poder dimensionar la solución en caso de requerir un aumento de recursos o la implantación de nuevos servidores de aplicación o de otra índole.

Se describirán los componentes físicos y lógicos que formarán parte del proceso de protección de los recursos y aplicaciones corporativas, diferenciando entre métodos de autenticación de usuario y sensibilidad de los recursos a proteger.

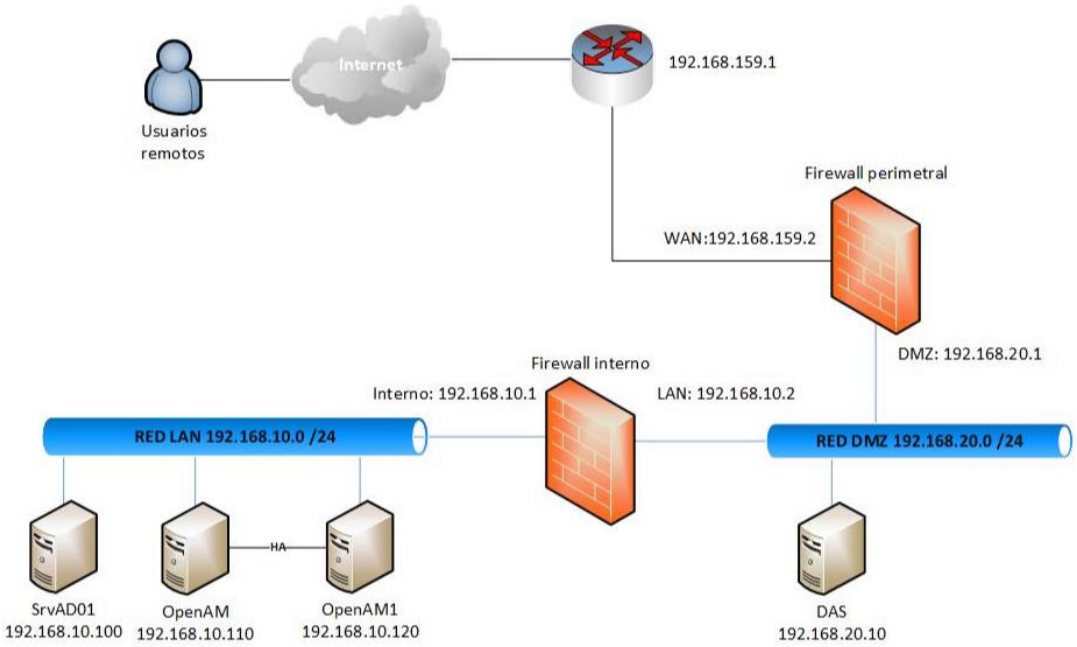
Aunque el alcance inicial del proyecto no valoraba medidas de seguridad perimetral más allá de la separación de las redes y el uso de un proxy o autenticación mediante LDAP, se decide implantarlas como valor añadido al proyecto. Igualmente la solución elegida permite la implantación de medidas de múltiple factor de autenticación (MFA) como protección adicional para evitar que, si se vulnera la contraseña del usuario el atacante consiga acceso a las aplicaciones del usuario, mitigando así los riesgos asociados a este tipo de soluciones.

Infraestructura

En primer lugar, nos centraremos en el despliegue de una infraestructura de red que nos dé el soporte necesario para posteriormente realizar la puesta en marcha del aplicativo de SSO.

Aunque no se ha definido como requisito, debemos tener presente en todo momento establecer unas medidas mínimas de seguridad perimetral y de la propia red. Esto debería ser requisito inherente a cualquier diseño que se realice.

Para empezar se plantea un esquema de la red que se va a implantar para este proyecto:



Esquema 1. Esquema de red

Como se puede apreciar en el Esquema 1, se ha definido una red LAN donde estarán ubicados los servidores que no deberían ser accesibles directamente desde internet, como son los servidores de directorio activo, aplicaciones y SSO y el resto de los ordenadores corporativos.

Por otro lado, se ha definido una DMZ con los servicios que deben ser accesibles desde internet. Además, se define un firewall perimetral que gestionará las reglas de acceso de red entre la LAN, DMZ e Internet.

Todos los elementos definidos en este esquema podrían protegerse mediante soluciones que garanticen alta disponibilidad. Por ejemplo, los servidores podrían estar virtualizados en un cluster de servidores físicos garantizando así que, si hay un fallo crítico en uno de ellos, no se produzca una caída del servicio. También se pueden generar clúster en los router o incluso en los cortafuegos dotándolos de tolerancia a fallos y permitiendo configurar balanceo de cargas.

Para nuestro caso concreto, se debe proteger la solución de SSO mediante la creación de un clúster de servidores de OpenAM, impidiendo de esta manera que si se produce la caída de un servidor de autenticación, la solución deje de dar servicio a los usuarios, ocasionando que no

puedan acceder a las distintas aplicaciones corporativas y recursos de la organización. Además este clúster permitirá el balanceo de cargas entre ambos nodos de OpenAM.

Ahora se van a describir los distintos elementos que se plantean en el esquema:

- **Usuarios remotos:**
  Todos aquellos usuarios que acceden a los aplicativos de forma remota desde internet.

- **Router:**
  Se encarga del enrutado desde y hacia internet, gestiona la IP pública pero se configura un DMZ host hacia el firewall para poder gestionar el tráfico. En ciertas circunstancias se podría obviar este dispositivo y enrutar directamente desde el firewall quitando así un punto de fallo.

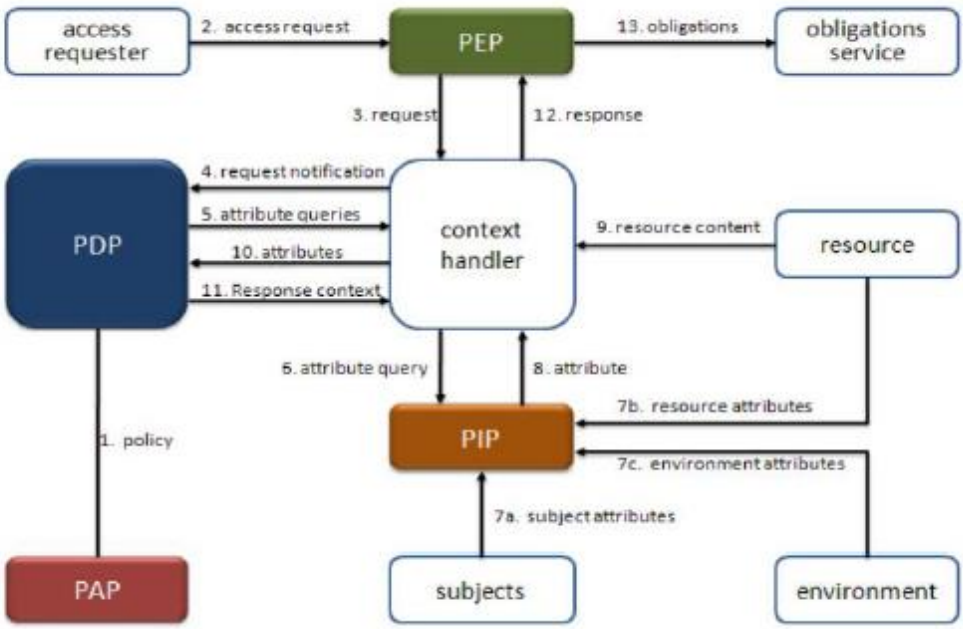
- **Firewall:**
  Desde este dispositivo se gestionan todos los accesos de red entre las distintas redes de la organización. Para este caso concreto y por medidas de seguridad, se ha optado por una implantación de dos firewalls:
  - Firewall perimetral: Controla los accesos entre internet y la DMZ
  - Firewall interno: Controla los accesos entre DMZ y la red interna.

- **LAN:**
  - Servidor de Directorio activo: Este servidor dará servicio de directorio en la red, será donde se verifiquen las credenciales de los usuarios. Además de gestionar los ordenadores del dominio, políticas de GPO de la organización y dará servicio de DNS en la red interna.
  - Servidor de aplicaciones: Almacenará una o varias aplicaciones que serán algunos de los recursos protegidos por la solución de SSO.
  - Servidor de SSO: Servidor encargado del proceso de validación del usuario a los recursos.

- **DMZ:**
  - Servidor proxy: Servidor a través del cual se realizarán las solicitudes de acceso a los distintos recursos.
  - Servidor DNS: Realizará las resoluciones de nombres de la DMZ.
  - Servidor web: Servidor que gestiona recursos web. Estas webs será recursos protegidos por la solución de SSO.

Sistema de Single Sign-On

Para comprender el funcionamiento que ha de tener la solución planteada y tener una visión global del proceso de validación de accesos a los recursos protegidos, se van a definir los distintos componentes que intervienen en este proceso:



Esquema 2. Proceso de validación

- **Policy Enforcement Point (PEP):** Recibe el request de acceso de un usuario a un recurso, el PEP realiza una solicitud de autorización al PDP e informa nuevamente al usuario de la respuesta. Por tanto, PEP hace de "portal" al usuario, en este caso el servidor Proxy situado en la DMZ asume esta función mediante los agentes de Java y AM web.

- **Policy Decision Point (PDP)**: Evalúa las solicitudes de acceso a recursos recibidas desde PEP e interroga al PAP para evaluarlas y autorizar o deniega la solicitud. Es decir, que el servidor de SSO situado en la red interna será el responsable de evaluar las solicitudes, recopilando la información necesaria para permitir o denegar el acceso al recurso.

- **Policy Administration Point (PAP):** Gestiona todas las políticas de acceso. Evidentemente esta función también es asumida por el servidor de SSO ya que las políticas de acceso a recursos protegidos por la solución son almacenadas ahí.

- **Policy Information Point (PIP)**: Fuente de atributos. PIP consulta los atributos solicitados por el PDP para que pueda evaluar la solicitud de acceso, estos atributos pueden ser consultados a diversas fuentes dentro de la red interna o DMZ.

Recursos protegidos

En este proyecto se abarca la protección de un conjunto de aplicaciones corporativas que se encuentran en el servidor de aplicaciones situado en la red de confianza de la organización. El objetivo principal del proyecto es la creación de las políticas de seguridad necesarias para garantizar una protección efectiva de los aplicativos frente a acciones no autorizadas y disponer de un proceso de auditoría de accesos. Se valorará también realizar la protección de recursos webs ubicados en la DMZ, además de los aplicativos.

Para el acceso a estos recursos se va a realizar validación de usuarios mediante autenticación contra directorio activo y mediante certificado digital en función de la sensibilidad de la acción a realizar y el recurso sobre que se desea realizar.

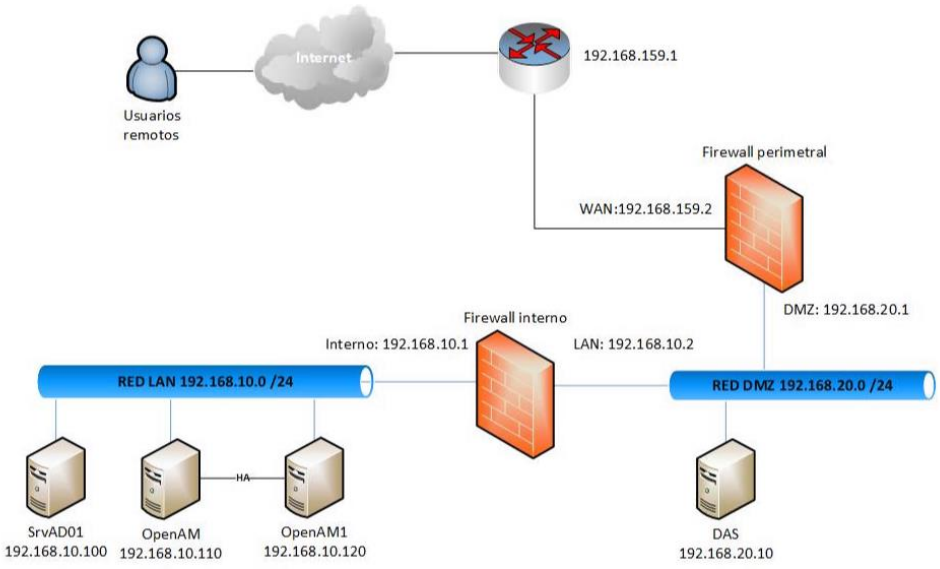
Implantación de la solución

En este apartado nos centraremos en el despliegue y configuración de la infraestructura necesaria para poner en producción la implantación de OpenAM como solución de SSO. Se verifica que la versión Open Source (community edition) está actualmente en su versión 11.0.3. Por tanto será dicha versión la que se despliegue en esta fase.

Toda la infraestructura descrita en esta fase está desplegada de manera virtual mediante una solución del fabricante VMware. Como se comentó en el diseño de la solución, esto nos permitirá tener recuperaciones mucho más rápidas ante un fallo en una máquina virtual y nos dará redundancia ante posibles fallos físicos de las máquinas que la soportan.

Despliegue de infraestructura

Se procede con la descripción del esquema indicando durante el diseño de la solución "Esquema 1", el cual se expone nuevamente para una mayor claridad:



Esquema 1. Esquema de red

Como se puede apreciar se ha optado por un despliegue de red mantenimiento unas medidas de seguridad que se consideran indispensables. Entre estas medidas están:

- Segmentación de red, definiendo una red LAN o una DMZ. Protegiendo los recursos más importantes en la LAN y permitiendo el acceso desde internet a los servidores de la DMZ.
- Clusterización de los servidores de OpenAM ya que es un servicio crítico. Este servicio debe estar siempre disponibles debido a que un fallo en el servicio impedirá que lo usuarios pueden autenticarse en las aplicaciones y demás recursos protegidos en la organización. Se implanta un balanceador de carga en la DMZ para no saturar los servidores openam impidiendo que queden inaccesible la solución de SSO por saturación de un host.

- Implantación de un firewall perimetral y otro interno: Se ha optado por la seguridad en dos capas, diferenciando entre la seguridad de la zona desmilitarizada de accesos desde internet y los accesos entre DMZ-LAN. Cabe destacar que el firewall perimetral debería contener servicios de seguridad perimetral como antivirus, IPS, sandbox protegiendo los servidores que son accesibles desde internet, y que por tanto, corren un mayor riesgo de infección o vulneración. Existen muchos fabricantes que implementan estos servicios de seguridad pero en este caso concreto solo se ha implementado un control de paquetes, inspeccionando las cabeceras para determinar origen, destino, protocolo etc. Por último, destacar la importancia de que en un entorno corporativo es muy recomendable (en algunos casos obligatorio) que ambos firewalls sean de distintos fabricantes, impidiendo así que una vulnerabilidad en uno de ellos permita el acceso a la zona más segura de la red (LAN).

- Se implementa un DAS en la zona desmilitarizada como medida de seguridad impidiendo un acceso directo a los servidores CORE de OpenAM situados en la LAN. Esta implantación es parte de un despliegue seguro, proporcionando una interfaz de login al usuario en la DMZ y gestionando desde este servidor las peticiones a la LAN.

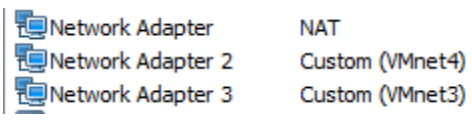
- Se implanta un servidor de Directorio Activo donde se gestionarán las credenciales de los usuarios en la organización y donde se puede gestionar el almacén de certificados para accesos que requieren un mayor nivel de seguridad.

Configuración de Firewalls

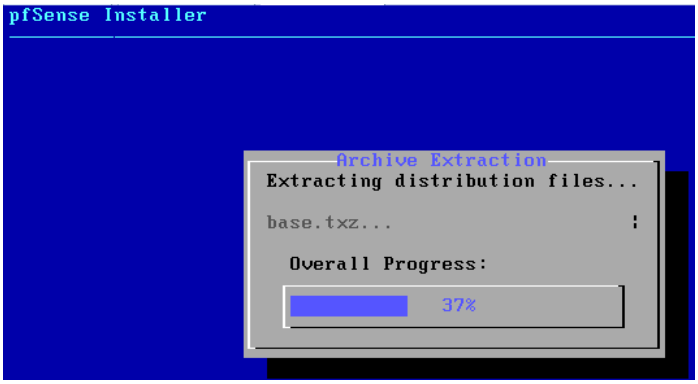
Se opta por el despliegue de dos firewall PfSense, uno perimetral y otro interno como se ha definido con anterioridad.

Perimetral

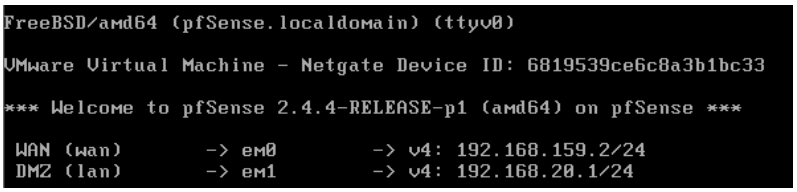
Se empieza con el despliegue de la máquina virtual con unas modificaciones en las interfaces asociadas a la máquina, definiendo 3 interfaces que darán conexión a las distintas redes:



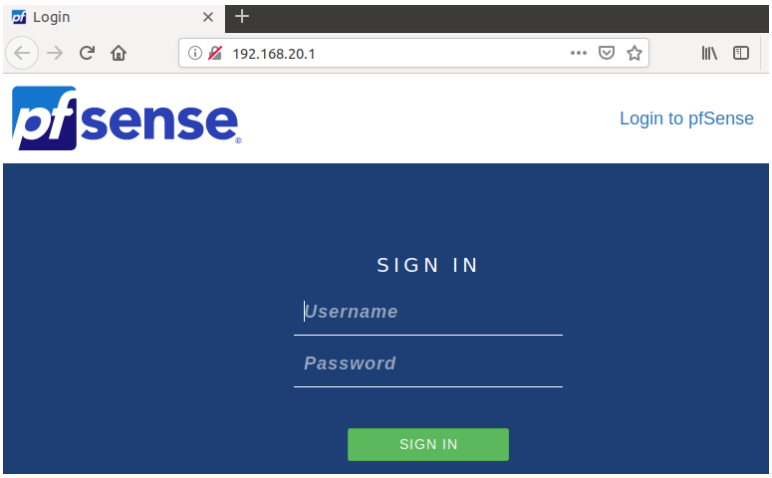
Una vez tenemos definidos los componentes físicos del dispositivo, se procede con el despliegue del firewall:



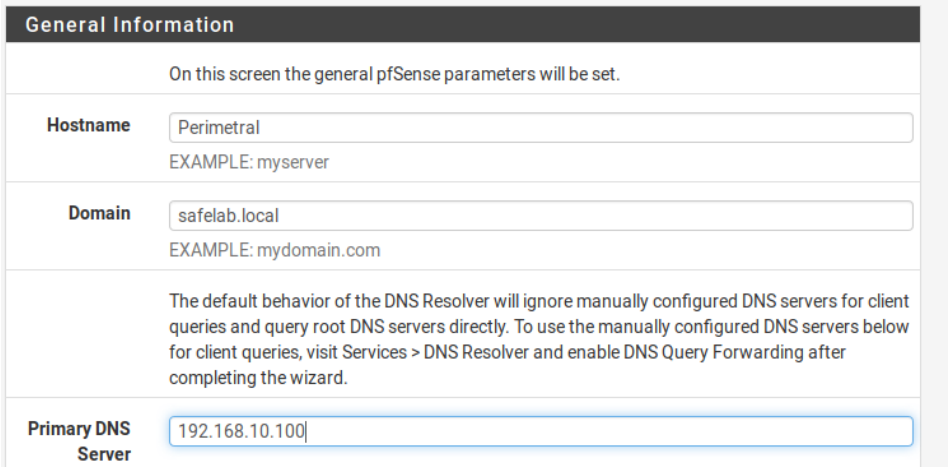
Se introduce una primera configuración básica para poder acceder a la interfaz web del firewall. Se define una red interna y otra DMZ:



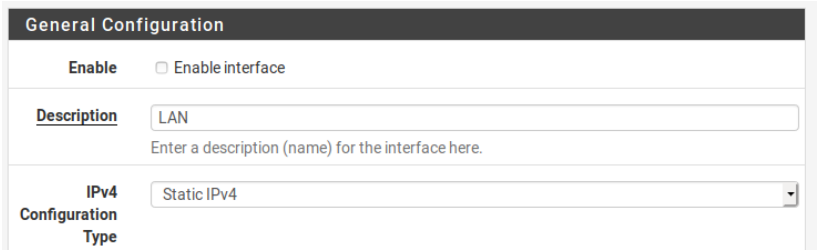
Se accede al portal web visible desde la DMZ para introducir la configuración más avanzada:



Se introduce información general sobre el firewall:

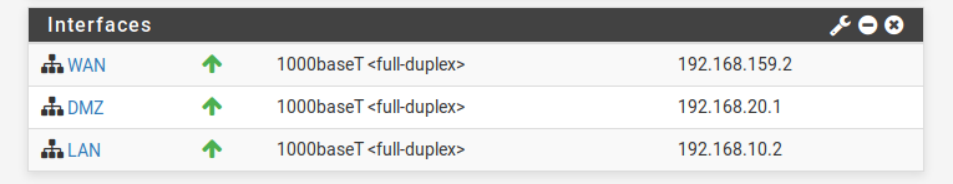


Se configura la interfaz que conectará con el firewall interno que desplegaremos a continuación:



Se asigna la configuración de red de la nueva interfaz:

Finalmente las interfaces quedan definidas de la siguiente manera:



Ahora se va a describir las reglas más destacables en lo referente a las comunicaciones de OpenAM:

WAN:

	✔	0 /0 B	IPv4 TCP	*	80 (HTTP)	192.168.20.10	8888	*	none	NAT NAT DAS

En este caso, se realiza un nateo de solicitudes desde el puerto 80 al servidor DAS situado en la DMZ por un puerto específico 8888.

DMZ:

	✔	0 /0 B	IPv4 TCP	192.168.20.10	*	WAN net	80 (HTTP)	*	none	
	✔	0 /0 B	IPv4 TCP	192.168.20.10	*	192.168.10.110	8080	*	none	OpenAM
	✔	0 /0 B	IPv4 TCP	192.168.20.10	*	192.168.10.120	8080	*	none	OpenAM1
	✔	0 /0 B	IPv4 TCP/UDP	192.168.20.10	*	192.168.10.100	53 (DNS)	*	none	DNS

En la DMZ se realizan conexiones desde el servidor DAS al servidor DNS en la LAN, además de las comunicaciones entre DAS y los servidores de OpenAM en la LAN y comunicaciones salientes con destino WAN.

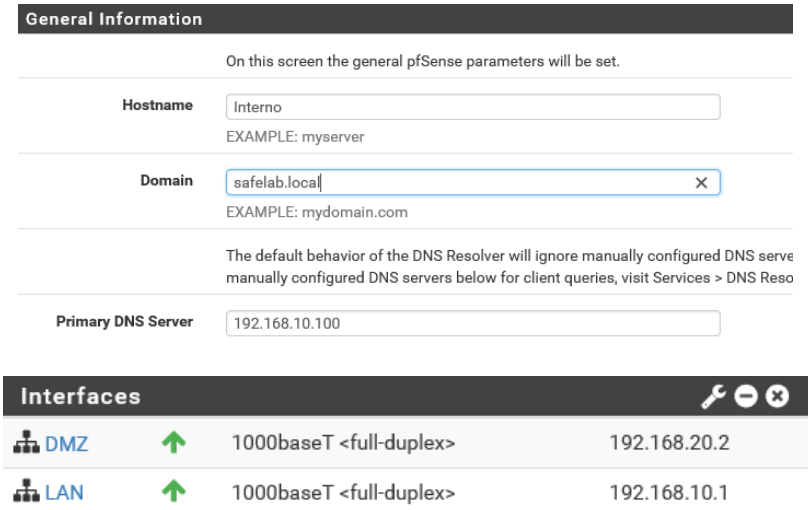
LAN:

✔	0 /0 B	IPv4 TCP	LAN net	*	192.168.20.10	8080	*	none	LB
✔	0 /0 B	IPv4 TCP	LAN net	*	192.168.20.10	8888	*	none	DAS
✔	0 /0 B	IPv4 TCP	192.168.10.100	*	DMZ net	53 (DNS)	*	none	DNS

Respecto a las comunicaciones de la red interna con la DMZ, se permiten el tráfico con el servidor de balance de cargas, DAS y resoluciones DNS.

Interno

Ahora procedemos con el despliegue del firewall interno:



Se muestran las reglas más relevantes que podemos encontrar en este firewall en lo referente con las comunicaciones necesarias para OpenAM.

DMZ:

✔	0 /0 B	IPv4 TCP	192.168.20.10	*	192.168.10.120	8080	*	none	LB
✔	0 /0 B	IPv4 TCP	192.168.20.10	*	192.168.10.110	8080	*	none	LB
✔	0 /0 B	IPv4 TCP	DMZ net	*	192.168.10.100	53 (DNS)	*	none	DNS

Comunicaciones desde la DMZ para servicio de DNS y accesos a los Core de OpenAM.

LAN:

✔	0 /0 B	IPv4 TCP	LAN net	*	192.168.20.10	8888	*	none	DAS
✔	0 /0 B	IPv4 TCP	192.168.10.120	*	192.168.20.10	8080	*	none	LB
✔	0 /0 B	IPv4 TCP	*	*	192.168.10.110	8080	*	none	LB
✔	0 /0 B	IPv4 TCP	192.168.10.100	*	192.168.20.10	53 (DNS)	*	none	DNS

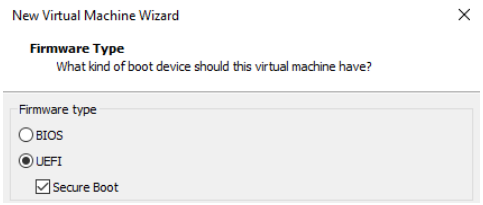
Comunicaciones para acceso a DAS y comunicaciones de los core con el balanceador de cargas.

Configuración de segmento LAN

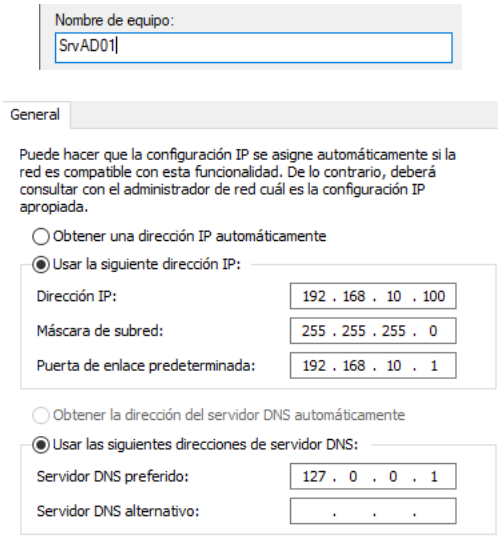
Instalación y configuración DA y DNS

Se opta por instalar Windows Server 2019 obviando un poco los pasos más banales de la instalación y haciendo énfasis en los aspectos más importantes.

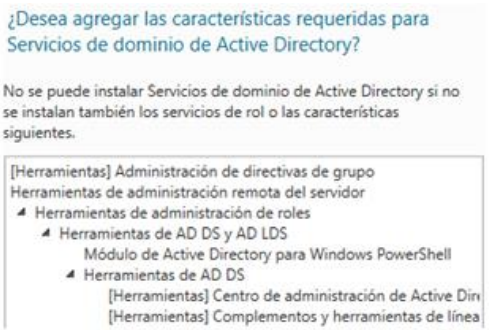
En primer lugar se despliega la máquina con Secure Boot para impedir la ejecución de software que no esté certificado por el fabricante evitando que una amenaza se pueda ejecutar durante el arranque del sistema:

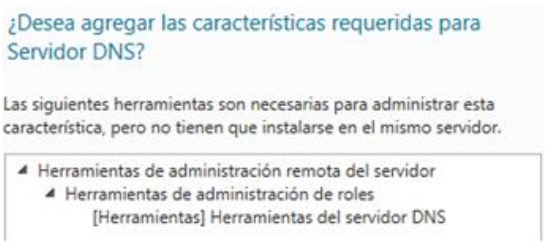


Una vez terminado el proceso de instalación se establece una contraseña al sistema para protegerlo de acceso no autorizados, se establece el nombre de servidor y se establece la configuración de red asociada a la LAN:

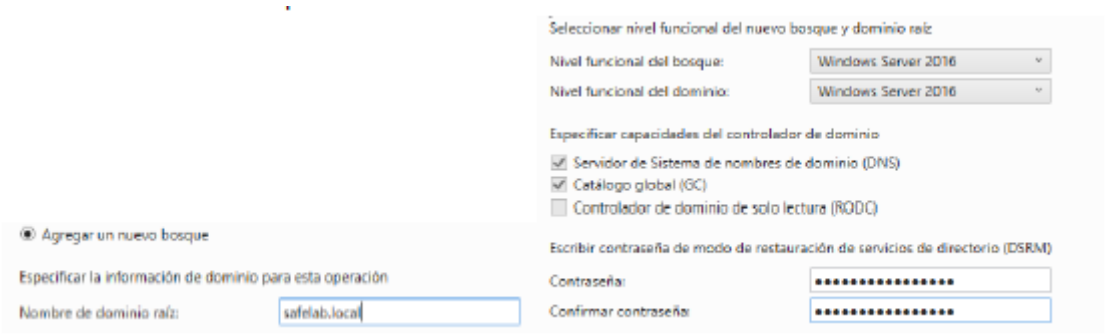


Una vez realizada la configuración más básica, se procede con la instalación del directorio activo y DNS:

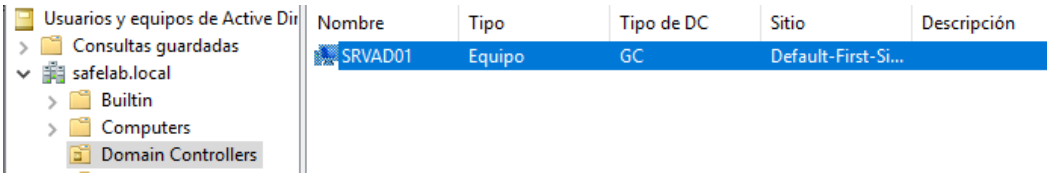




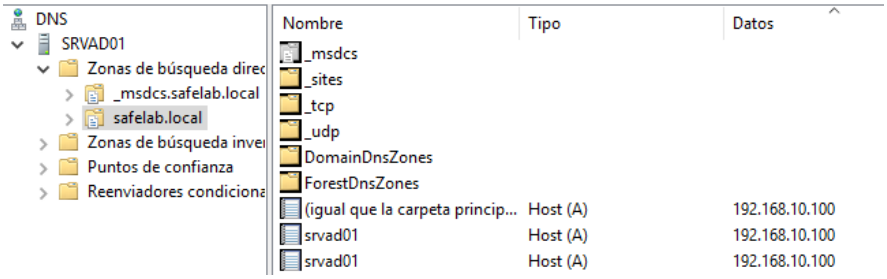
Se establece nuevo bosque “Safelab.local”, definiendo también su nivel funcional:



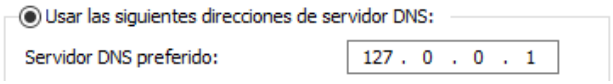
Tras el despliegue del servidor se puede observar el controlador de dominio creado:



Se comprueba la correcta instalación de servidor de DNS, la creación de la zona, la asignación de nombre al servidor instalado, la correcta configuración de los reenviadores DNS:

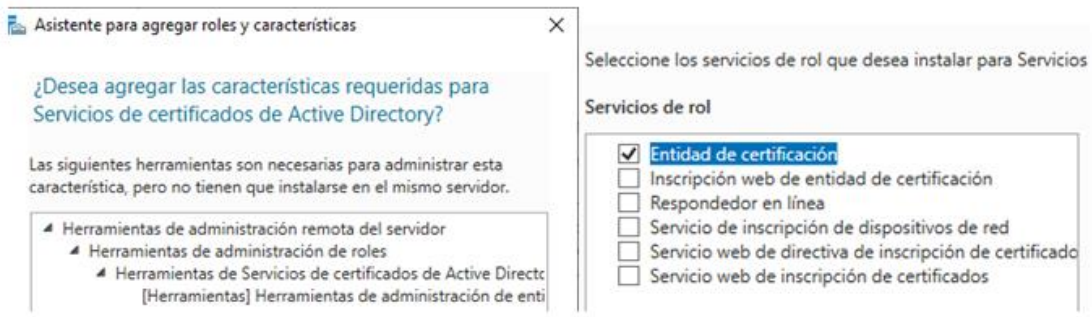


Por último se comprueba cómo se ha realizado el cambio de la configuración DNS del adaptador de red de la propia máquina, indicando que las resoluciones se harán localmente:



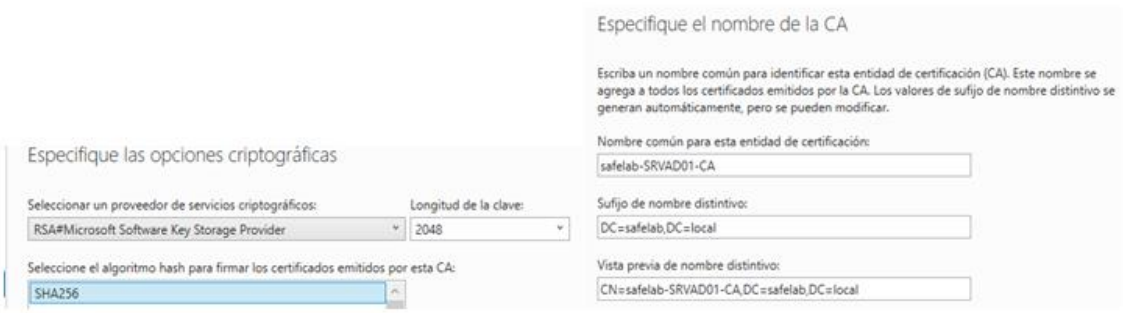
Instalación de Entidad de Certificación

Una vez instalado y configurado el directorio activo se procede con la instalación del rol de entidad de certificación que nos permitirá realizar conexiones seguras y gestión centralizada de certificados:



Tras la instalación del nuevo rol se procede con su configuración especificando que se va a desplegar un CA empresarial:

Se especifica el cifrado que va a utilizar, en este caso SHA256 y los datos referentes a la CA:

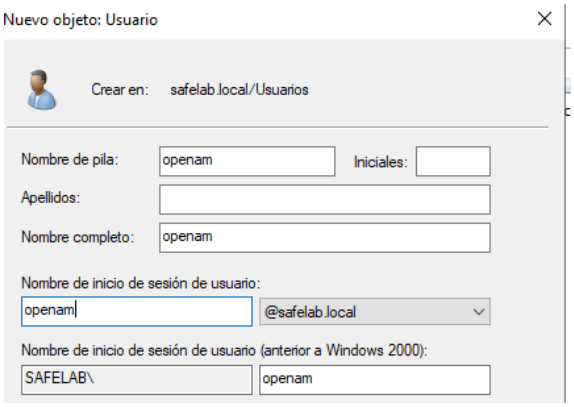


Una vez configurado se exporta la CA pública del dominio para ser importada en los servidores de OpenAM una vez desplegados:

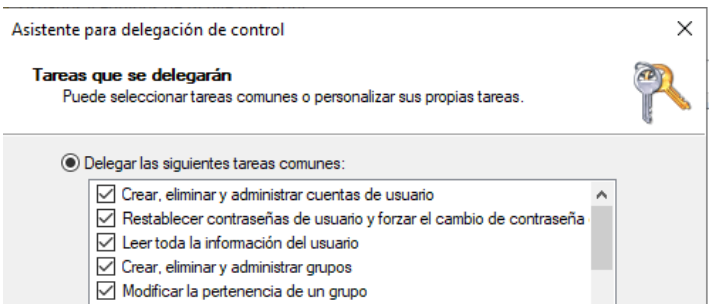
```
C:\Users\Administrador>certutil -ca.cert -f ca.cer
Certificado de CA[0]: 3 -- válida, válido
Certificado de CA[0]:
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgIQGp9GMnkCAaJIhH9xIImW3TANBgkqhkiG9w0BAQsFADBN
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdzYWZlbGFi
MRswGQYDVQQDExJzYWZlbGFiLVNSVkFEMDEtQ0EwHhcNMTkwNDI3MTYxODExWhcN
MjQwNDI3MTYyODEwWjBNMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJ
k/IsZAEZFgdzYWZlbGFiMRswGQYDVQQDExJzYWZlbGFiLVNSVkFEMDEtQ0EwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDiWIs9YbW+ppQG+cbyaQImo2Ay
mApVUah0MbsI78JHMz2TH6yIEhwTnI4I3DGBwu2hlcKDhzKt2EKNf9WW75fs8eCw
HXM1PFRo29keYdVsMUG5x7K9GYuOPPXz0dT0eJFbx4m0kdJmDMzi2Z2BaIhTyzu4
TPZ2cF0ceubPxsRCZh76SRuz7n+0/xS+OxkYVAOYXiyOA5Rv1inClESZBWprs5oJ
GWjwcPw4Nd4l+8kJdAMMb3aruICIGnv0yp4I0iFBt0kI9w9JWO7nw2JhlDuB0a6T
64VjjdaNsU2zwOQYRQsmO1zE62+PL1H9DI/lhqhEYPjU/9UK+bqRuHmItVzxAgMB
AAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ8
QXx0sNvz1J8n/sLzDdGO9gm2yTAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B
AQsFAAOCAQEAlQri7RcewFhQLKqGOTQqGMw1uj1JtpzSTQ/JyTH1XAhklRyXHmAT
ZL6suGWcJTNNosyfDxWATDYfszmUTjDtBnA3wSgvfK4byN+1pinrHm2SXFw4gyQb
vnc1vZEqcYGVVZ3mN6ElpqfroTNjVqTw11H9jKy5U3qBDDm5vfPzkrCViNAmKaOw
Jv1D2qL2Qz8uXVvIsC1s8HDwPTaMUo0gmPSZeyVg7Nx1gkMPnu9Ni9uRPhXjVdIk
NezRwDFnWYjzvHRsr70gsQdSWDeA0PkQPaYSIqPUwoiVR31XnPvV7AjnZ1AAku04
Q/Y4uGsQszNlo2K8M+nyK8Sv6efJ4r9+Bw==
-----END CERTIFICATE-----

CertUtil: -ca.cert comando completado correctamente.
```

Configuración de usuarios

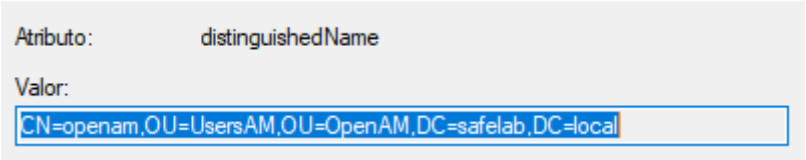
Tras esta instalación se genera una unidad organizativa (OU) específica para la gestión de OpenAM y se genera un nuevo usuario de gestión del servicio:



Es necesaria la asignación de ciertos permisos para la realización de tareas relacionadas con la gestión de usuarios requerida por el servicio. Para ello se procede una delegación del control:



Por último, se recupera el distinguishedName que será utilizado durante el despliegue de OpenAM.



Ya hemos desplegado lo necesario para realizar la gestión de usuarios y certificados, además de todas las tareas organizativas y de control que termite un directorio activo pero en las que no vamos a entrar en este desarrollo.

Despliegue del Core de OpenAM

Ahora se procede con la instalación de las máquinas que serán miembro del cluster de OpenAM. Se opta por desplegar Ubuntu 18.04 con una configuración básica de desplieuge, asique nos centraremos en la instalación de los servicios asociados para no alagar en exceso este documento. Estas máquinas también son desplegadas en el segmento LAN, ya que conforman en Core de OpenAM y gestionan información privilegiada.

Instalación de Apache y Tomcat

En primer lugar se prepara el sistema para poder implantar posteriormente los servicios de apache y tomcat:

```
root@ubuntu18:/etc# apt-get install build-essential checkinstall_
```

Se realiza instalación de Apache 2.4:

```
root@ubuntu18:/etc# apt install apache2_
```

```
root@ubuntu18:/etc# apache2 -v
Server version: Apache/2.4.29 (Ubuntu)
Server built:   2019-04-03T13:22:37
```

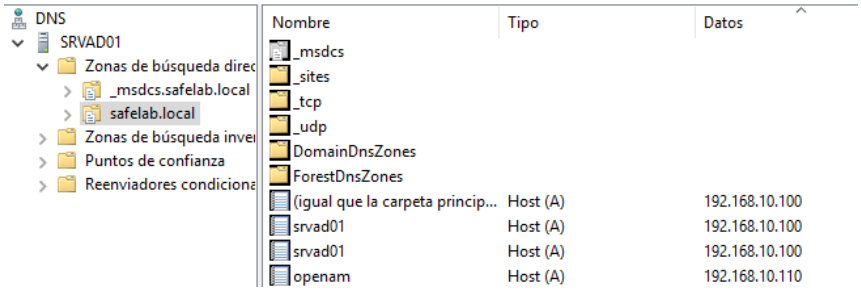
Se establece que el puerto de escucha de apache sea el 8000:

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 8000
```

Se establece la configuración de red del servidor mediante netplan:

```
network:
    ethernets:
        ens33:
            addresses: [192.168.10.110/24]
            gateway4: 192.168.10.1
            nameservers:
                addresses: [192.168.10.100]
            dhcp4: no
    version: 2
```

Se establece la configuración necesaria en el DNS de dominio:



Instalación de JDK y OpenDJ

Se realiza la instalación del JDK 7, ya que según la documentación de OpenAM Community Edition 11.0.3 se debe desplegar JDK 6 o 7. Para ello se descarga desde la página de Oracle y se procede con la configuración necesaria en el sistema para su correcto funcionamiento:

```
root@ubuntu18:/opt# update-alternatives --install /usr/bin/java java /opt/jdk7/bin/java 100
update-alternatives: using /opt/jdk7/bin/java to provide /usr/bin/java (java) in auto mode
root@ubuntu18:/opt# update-alternatives --install /usr/bin/javac javac /opt/jdk7/bin/javac 100
update-alternatives: using /opt/jdk7/bin/javac to provide /usr/bin/javac (javac) in auto mode
```

Se verifica que se instaló de manera correcta en el sistema:

```
root@ubuntu18:/opt# java -version
java version "1.7.0_80"
Java(TM) SE Runtime Environment (build 1.7.0_80-b15)
Java HotSpot(TM) 64-Bit Server VM (build 24.80-b11, mixed mode)
```

Ahora se procede con la instalación de Tomcat 7 en el sistema donde se desplegará la aplicación de OpenAM, de igual manera se descarga el software necesario de la página del fabricante y se despliega y configura el servicio asociado para que establezca configuraciones necesarias para el correcto funcionamiento de OpenAM:

```
CATALINA_HOME="/opt/tomcat7"
export CATALINA_HOME
JAVA_HOME=/opt/jdk7
JRE_HOME=/opt/jdk7/jre
export JAVA_HOME
export JRE_HOME
CATALINA_OPTS="-server -Xmx2048m -XX:MaxPermSize=256m"
export CATALINA_OPTS

case "${1}" in
start)
  /bin/su root -c "${CATALINA_HOME}/bin/startup.sh"
  exit ${?}
  ;;
stop)
  /bin/su root -c "${CATALINA_HOME}/bin/shutdown.sh"
  exit ${?}
  ;;
*)
  echo "Usage:  $0 { start | stop }"
  exit 1
  ;;
esac
```

Se despliega la aplicación de OpenAM Community en la carpeta de webapps y se levanta el servicio:

```
root@ubuntu18:/etc/init.d# ./tomcat start
Using CATALINA_BASE:   /opt/tomcat7
Using CATALINA_HOME:   /opt/tomcat7
Using CATALINA_TMPDIR: /opt/tomcat7/temp
Using JRE_HOME:        /opt/jdk7/jre
Using CLASSPATH:       /opt/tomcat7/bin/bootstrap.jar:/opt/tomcat7/bin/tomcat-juli.jar
Tomcat started.
```

Se despliega OpenDJ para ser usado como almacén de datos en el propio servidor:

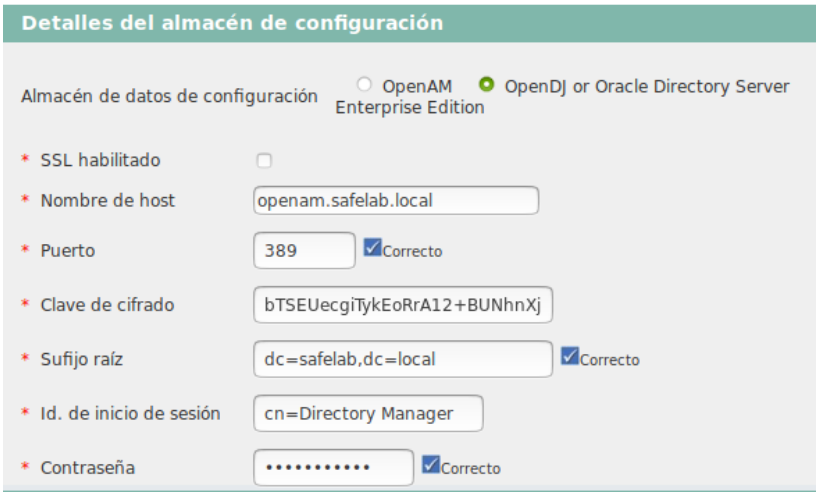
```
Resumen de configuración
=============
Puerto de escucha de LDAP:            389
Puerto del conector de administración: 4444
Acceso seguro de LDAP:                deshabilitado
ND del usuario root:                  cn=Directory Manager
Datos del directorio:                 Crear nuevo ND de base
dc=safelab,dc=local.
Datos de ND de base: Crear sólo entrada de base (dc=safelab,dc=local)
```

Se procede con una instalación personalizada del aplicativo:

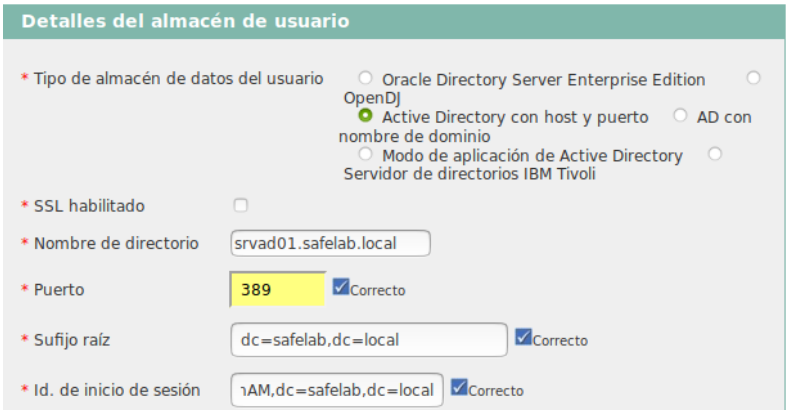
Instalación de OpenAM

Se establecen los datos referentes al servidor como primera instancia de la solución ya que no se va a agregar a una solución existente:

Se define que el almacén los datos y configuraciones van a estar embebidos en el propio servidor mediante el OpenDJ que se ha desplegado con anterioridad:

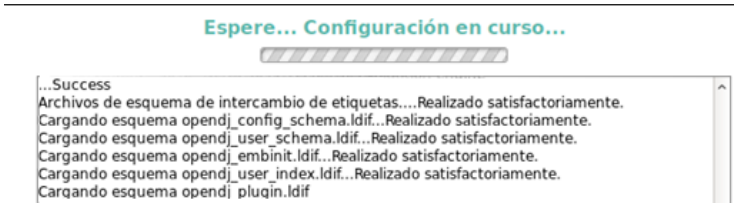


En el caso de la gestión de credenciales de usuario, a diferencia del almacén de configuraciones, se opta por consultar el directorio activo que hemos definido con anterioridad, en este caso se despliega mediante una configuraciones sin SSL aunque más adelantes la añadiremos para casos más concretos.

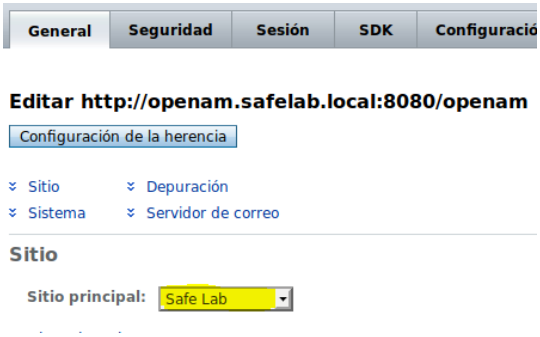


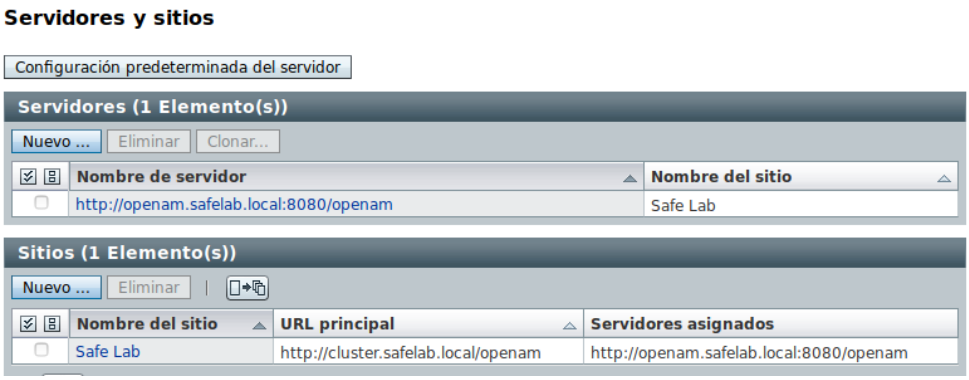
No se genera un nuevo sitio aún pero se generará de forma manual posteriormente.

Se procede con la instalación del aplicativo:



Se accede al portal del aplicativo mediante el usuario de administración amAdmin y se procede con la generación de un nuevo sitio llamado SafeLab y la asignación del servidor que se acaba de crear. La dirección del clúster de OpenAM estará situado en un servidor en la DMZ que tendrá las funciones de balanceador de cargas y DAS, aunque en esto entraremos más en detalle próximamente:

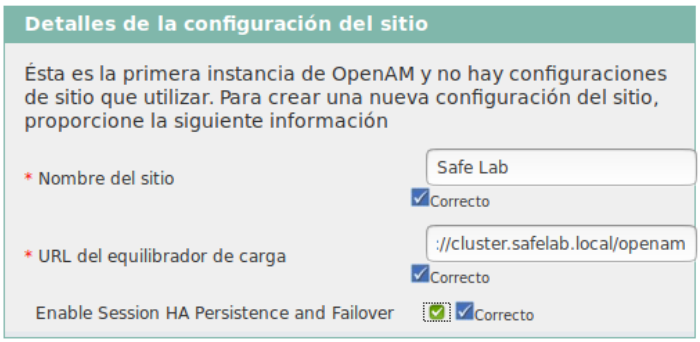




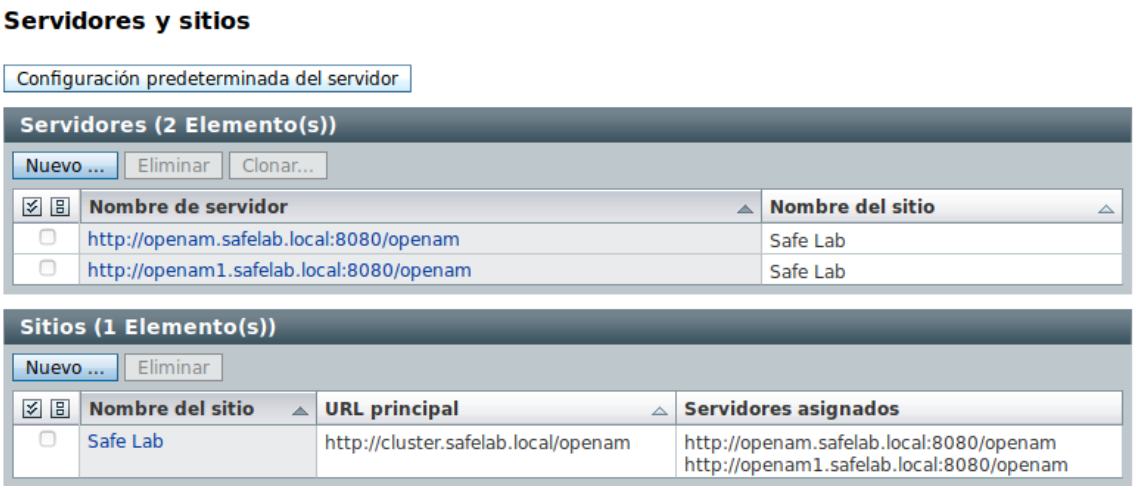
Ahora se procede con idénticos pasos para el despliegue del otro servidor del clúster variando simplemente los datos referentes al servidor:

En este caso se agrega a una implantación existente y no como primera instancia:

Además se añade al sitio que se ha creado con anterioridad, permitiendo así la clusterización de la solución mediante un portal centralizado de SSO que balanceará las cargas entre ambos servidores del clúster, permitiendo la persistencia de sesiones de usuario y dotando de tolerancia a fallos y sobrecargas de una de las máquinas virtuales.



Tras el despliegue inicial de la segunda máquina virtual, accedemos y comprobar la correcta configuración del clúster:



En este punto ya hemos desplegado la parte correspondiente a la LAN, aunque en este segmento de red podrán existir servidores de aplicaciones, intranets y recursos compartidos t otros recursos internos que puedan securizarse mediante esta solución.

Configuración del segmento DMZ

A partir de este punto nos centraremos en el despliegue de los sistemas que estará contenidos dentro de la DMZ y que por tanto van a ser accesibles desde internet y harán de portal único a los usuarios.

Despliegue de balanceador de cargas

Se opta por la implantación de HAproxy como servicio de balanceador de cargas, aunque también se podría haber usado el propio Apache. Este servidor monta una configuración básica con (Apache) y será el encargado de realizar equilibrio de cargas de peticiones a los servidores Core de OpenAM. Lo mencionamos anteriormente durante la creación del Site con la dirección de clúster "cluster.safelab.local:8080/openam"

Se realiza la instalación y se realiza configuración para que este servidor actúe como Frontend y realice un reparto de cargas entre los core de OpenAM (Backends):

```
frontend http-in
        bind *:8080
        default_backend open

backend open
        cookie SERVERID insert nocache
        balance roundrobin
        server open1 192.168.10.110:8080 cookie 01 id 1001 check inter 200 rise 2 fall 5
        server open2 192.168.10.120:8080 cookie 03 id 1003 check inter 200 rise 2 fall 5
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http
```

Como se puede apreciar en la configuración se realiza una captura del tráfico obtenido en el servidor en el puerto 8080 que es el que se ha establecido en el clúster y se realiza un balanceo de cargas mediante Round Robin entre los servidores de OpenAM. En este punto es importante destacar algunas opciones como:

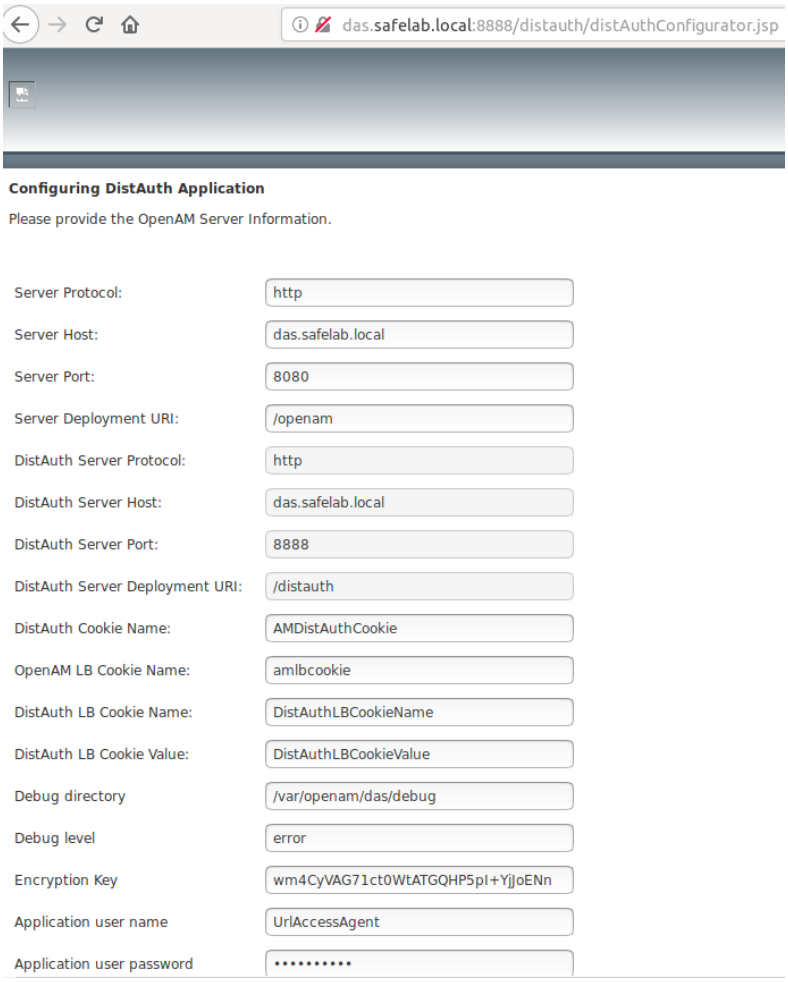
- Cookie insert nocahe: Para permitir la persistencia de sesiones entre los servidores insertándola en el paquete y evitando a que la cookie quede cacheada.
- Balance Round Robin: Indica que el equilibrio de carga se realiza mediante Round Robin.
- Server: Indica cada servidor que se va a definir dentro del balance de cargas, indicando el FQDN del servidor y los datos relativos a cookies que serán insertados en los paquetes.
- Por último, se definen las pantallas de error que se mostrarán antes cada código de error devuelto.

Una vez desplegado y configurado, se inicia el servicio y los accesos mediante la URL http://das.safelab.local:8080 balancearán entre ambos cores de OpenAM.

Despliegue de DAS

Como se comentó al inicio del apartado de implantación de la solución, se decide implantar un DAS como portal del Login para los usuarios y dotará de una mayor seguridad a la infraestructura de manera complementaria a los firewalls.

En este caso, el servidor de DAS se va a desplegar en el mismo servidor que se desplegó en balanceo de carga, ya que están íntimamente relacionados y no se cree necesario la implantación de esta aplicación en un sistemas aislado. Para su despliegue se descarga la aplicación y se despliega en el Tomcat implantado en el servidor:

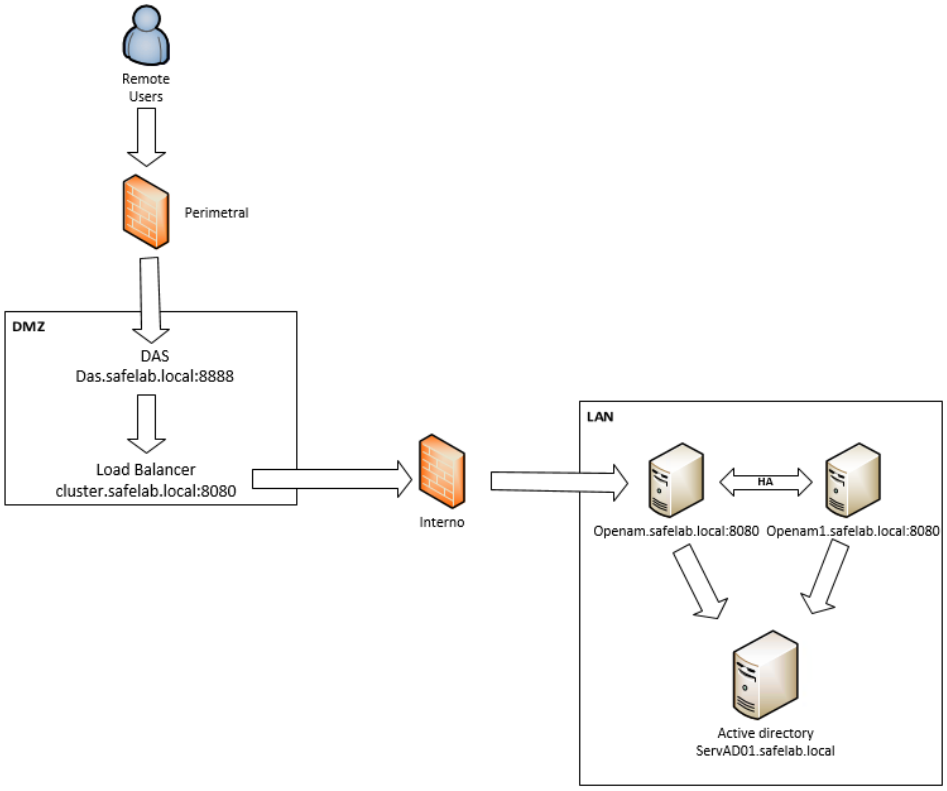


DistAuth application is successfully configured.
AMDistAuthConfig.properties created at /root/FAMDistAuth/_opt_tomcat7_webapps_distauth_AMDistAuthConfig.properties

En este caso, podemos observar que básicamente se especifica la dirección del portal del clúster de OpenAM y el portal donde se va a implantar la esta aplicación, además de los datos relativos a cookies y el usuario utilizado para recuperar las configuraciones en los servidores de OpenAM.

Portal del DAS: http://das.safelab.local:8080/DistAuth/UI/Login

Para hacernos una idea global del flujo de datos ante una petición de usuario sería el siguiente:



Esquema 3. Flujo de usuario

En conclusión, los usuarios que accedan mediante el portal DAS serán redireccionados en el mismo servidor al servicio de balanceo de cargas que balanceará mediante un Round Robin a los servidores core situados en el segmento de red más protegido, donde se realizarán las consultas de autenticación y autorización de usuarios.

Ésta es una de las soluciones que se pueden implantar como medida de seguridad pero existen otros muchos tipos de implantaciones para este acometido, como pueden ser proxys inversos o soluciones más profesionales como Web Application Firewalls (WAF) que dará un mayor nivel de seguridad y permitirá proteger todos los aplicativos y recursos de la DMZ ante posibles ataques más sofisticados.

Autenticación de usuarios

Durante el despliegue se ha configurado una autenticación de usuarios mediante una conexión LDAP con el directorio activo, pero hemos configurado un acceso seguro mediante el despliegue de una entidad de certificación que nos permitirá conexiones SSL sobre el puerto 636 en el directorio activo, esto nos permitirá autenticación LDAPS y autenticaciones más seguras mediante comprobación con un certificado digital.

Al realizar la configuración LDAP durante el despliegue se ha establecido como método de autenticación por defecto pero se puede establecer un nuevo dominio donde podemos establecer un método de autenticación más estricto para datos de una mayor sensibilidad. Por ello vamos a crear un nuevo dominio y establecer a ese dominio una autenticación cifrada.

Por tanto, comenzamos creando un nuevo dominio para asignarle una autenticación de mayor seguridad para el acceso a recursos más protegidos:

En este caso, se securiza el acceso a un nuevo alias definido para este dominio nominas.safelab.local. Asociamos una autenticación SSL específica para este nuevo dominio:

Active Directory

Atributos de dominio

Servidor principal de Active Directory

Valores actuales srvad01.safelab.local:636 — Eliminar

Nuevo valor — Agregar

DN para iniciar búsqueda de usuario

Valores actuales dc=safelab,dc=local — Eliminar

Nuevo valor — Agregar

Formato: nombre_servidor|DN_búsqueda
Cuando escriba varias entradas, cada una de ellas deberá tener el nombre del servidor local como prefijo.

Enlazar ND de usuario: cn=openam,ou=UsersAM,ou=OpenAM,dc=safelab,dc=local

The DN of an admin user used by the module to authentication to the LDAP server

Enlazar contraseña de usuario: ••••••••••

The password of the administration account.

Enlazar contraseña de usuario (confirmar): ••••••••••

Ámbito de búsqueda:
- OBJETO
- (•) SUBÁRBOL
- UNNIVEL

The level in the Directory Server that will be searched for a matching user profile.

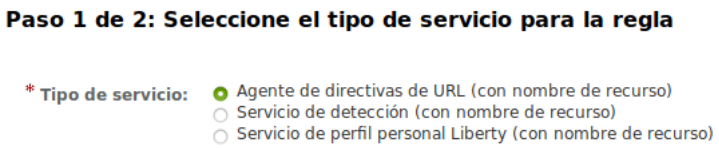
Acceso SSL al servidor de Active Directory: [x] Habillitado

Ensures the SSL/TLS will be used to establish connections to the LDAP server.

Devolver DN de usuario a DataStore: [x] Habillitado

Controls whether the DN or the username is returned as the authentication principal.

Y nos aseguramos de habilitar la opción de Acceso SSL al AD. A continuación indicamos el recurso web del aplicativo de nóminas que deseamos securizar:



Y se debe desplegar el agente en el recurso web que vamos a securizar mediante OpenAM. Al igual que usamos este tipo de autenticación tenemos a nuestra disposición un largo número de procesos de autenticación que, como hemos visto, podemos definir para cada recurso a proteger en función de la sensibilidad de los datos que allí se manejen, desde una autenticación básica con usuario y contraseña a una cadena de procesos de autenticación:

En esta fase se ha realizado el despliegue y configuración de la infraestructura y servicios asociados a la solución de SSO que se ha propuesto para este proyecto. Se han indicado muchas posibles mejoras que se pueden implantar para aumentar la seguridad de la solución como la implantación de servicios de seguridad perimetral, establecer diferentes fabricantes de firewalls, implantación de un WAF, redundancia del directorio activo mediante la implantación de un segundo controlador de dominio, etc.