Guía de Seguridad de las TIC
CCN-STIC 1111

Procedimiento de Empleo Seguro de SailPoint – IdentityIQ



Noviembre de 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 5
1.1 IDENTITYIQ LIFECYCLE MANAGER 5
1.2 IDENTITYIQ COMPLIANCE MANAGER 6
1.3 CONECTORES E INTEGRACIONES AVANZADAS 6
2 OBJETO Y ALCANCE 7
3 ORGANIZACIÓN DEL DOCUMENTO 8
4 FASE PREVIA A LA INSTALACIÓN 9
4.1 ENTREGA SEGURA DEL PRODUCTO 9
4.2 ENTORNO DE INSTALACIÓN SEGURO 9
4.3 REGISTRO Y LICENCIAS 9
4.4 CONSIDERACIONES PREVIAS 9
4.4.1 PLATAFORMAS SOPORTADAS 10
4.4.2 ARQUITECTURA DE DESPLIEGUE 10
5 FASE DE INSTALACIÓN 15
5.1 INSTALACIÓN SEGURA 15
5.1.1 INTEGRACIÓN CON DIRECTORIO ACTIVO 15
5.1.2 APLICACIONES REMOTAS 16
5.1.3 ARQUITECTURA Y REQUISITOS 16
6 FASE DE CONFIGURACIÓN 17
6.1 MODO DE OPERACIÓN SEGURO 17
6.1.1 HTTPS EN SERVICIOS WEB 17
6.1.2 CONFIGURAR ALMACÉN DE CLAVES 17
6.2 AUTENTICACIÓN 20
6.2.1 DATOS EN TRANSITO 20
6.3 ADMINISTRACIÓN DEL PRODUCTO 24
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 24
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 24
6.3.3 POLÍTICA DE CONTRASEÑAS 26
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 28
6.5 GESTIÓN DE CERTIFICADOS 29
6.6 SERVIDORES DE AUTENTICACIÓN 29
6.6.1 AUTENTICACIÓN MEDIANTE MÉTODO DE *PASS-THROUGH* (PTA) 29
6.6.2 AUTENTICACIÓN MEDIANTE INICIO ÚNICO (SSO) 30
6.6.3 AUTENTICACIÓN MEDIANTE CUENTA LOCAL 31
6.6.4 ORDEN DE PROCESAMIENTO DEL MÉTODO DE AUTENTICACIÓN 31
6.7 ACTUALIZACIONES 32
6.8 ALTA DISPONIBILIDAD 33
6.9 AUDITORÍA 33
6.9.1 REGISTRO DE EVENTOS 33
6.9.2 ALMACENAMIENTO LOCAL 35
6.9.3 ALMACENAMIENTO REMOTO 35
6.10 BACKUP 36

7 FASE DE OPERACIÓN 37
8 CHECKLIST 39
9 REFERENCIAS 40
10 ABREVIATURAS 43

ÍNDICE DE TABLAS

Tabla 1: Plataformas soportadas 10
Tabla 2: Aprovisionamiento 11
Tabla 3: Consideraciones adicionales 14
Tabla 4: Almacenamiento remoto 36
Tabla 5: Checklist 39

ÍNDICE DE FIGURAS

Figura 1: Componentes funcionales de IdentityIQ 5
Figura 2: Descarga de Software 9
Figura 3: Arquitectura para Categoría de instalación Micro 12
Figura 4: Arquitectura para Categoría de instalación Pequeña. 12
Figura 5: Arquitectura para Categoría de instalación Mediana 13
Figura 6: Arquitectura para Categoría de instalación Grande 14
Figura 7: Diagrama de comunicación de IQService 15
Figura 8: Diagrama de arquitectura 16
Figura 9: Ejemplo de fichero iiq.properties 19
Figura 10: Rutas de tránsito de datos que pueden cifrarse en SailPoint IdentityIQ, conector Gateway e IQServices 21
Figura 11: Despliegue de 3 agentes desplegados en 3 controladores de dominio. 22
Figura 12: Listado de capacidades 25
Figura 13: Detalle de la herencia de capacidades 25
Figura 14: Pantalla de definición de caracteres permitidos en la contraseña 26
Figura 15: Pantalla de definición de política de contraseña 27
Figura 16: Parámetro de configuración de inicio de sesión 28
Figura 17: Pantalla de configuración de Inicio de sesión. 30
Figura 18: Pantalla de configuración de SSO basado en regla 30
Figura 19: Pantalla de configuración de SSO basado en SAML 31
Figura 20: Diagrama de inicio de sesión único (SSO) 31
Figura 21: Diagrama de Autenticación pass-through 32
Figura 22: Arquitectura para instalaciones en Alta disponibilidad 33
Figura 23: Interfaz de configuración de Auditoria 34
Figura 24: Interfaz de configuración de Analítica avanzada. 34
Figura 25: ejemplo de fichero logs de SailPoint IdentityIQ aplicando el patrón descrito con anterioridad. 35
Figura 26: Contenido de la tabla spt_audit_event 35

Figura 27: Interfaz de configuración de Analítica avanzada, con tipo de búsqueda Syslog. 36
Figura 28: Pantalla para la configuración de la monitorización de aplicaciones. 37
Figura 29: Estado del servidor de SailPoint IdentityIQ 38
Figura 30: Listado de todas las tareas de aprovisionamiento 38

1 INTRODUCCIÓN

SailPoint IdentityIQ es una plataforma de **Gestión de Identidades y Gobierno de los Accesos (IGA)** que ofrece una amplia gama de funcionalidades:

- Aprovisionamiento: onboarding de nuevos usuarios, cambios y desa-provisionamiento, automatización en los procesos; para usuarios internos, colaboradores y/o proveedores.
- Gobierno de acceso: visibilidad completa de los accesos de la organización, on-premise y/o en nube. Revisión de accesos, cumplimiento de acceso según políticas de usuarios a aplicaciones y datos
- Gestión de contraseñas.
- Segregación de funciones.

La plataforma de SailPoint, dispone de un amplio catálogo de conectores que ofrecen una integración inteligente con las aplicaciones y servicios.

Los componentes funcionales principales de SailPoint IdentityIQ son:

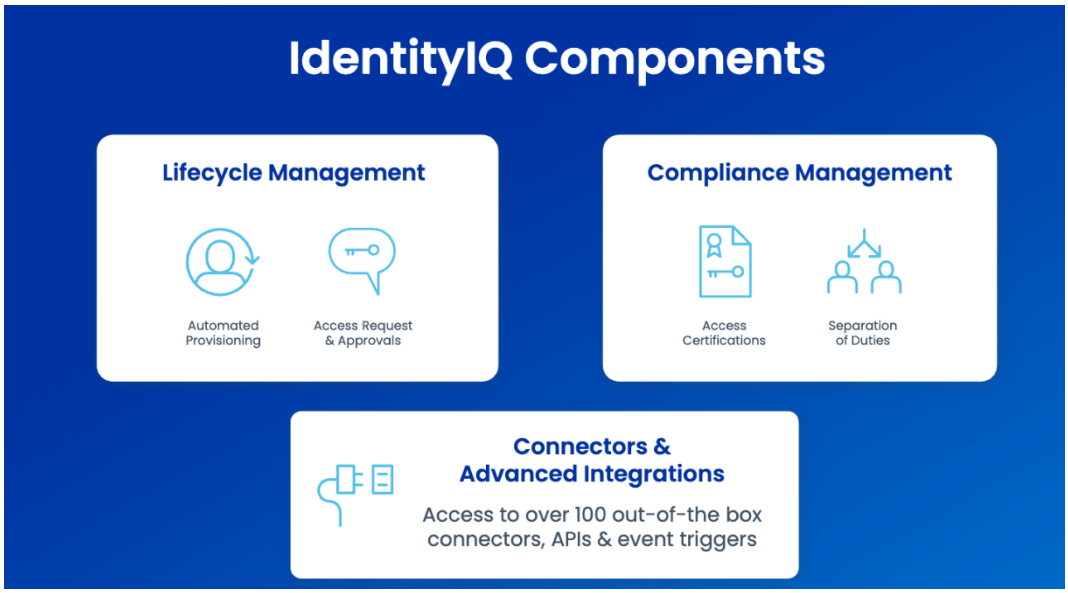


Figura 1: Componentes funcionales de IdentityIQ

A continuación, se identifican las principales funcionalidades de los distintos componentes.

1.1 IDENTITYIQ LIFECYCLE MANAGER

Solicitudes y aprobaciones de acceso: Portal de autoservicio que permite a los usuarios solicitar acceso a aplicaciones y servicios.

- Centralización la solicitud de accesos a través de una interfaz única para solicitar y aprobar accesos.
- Gestión de políticas automática: aplicación de políticas corporativas durante el proceso de solicitud de accesos.

- Integración con herramientas de ticketing, para poder trazar end-to-end la gestión de cambios.

Aprovisionamiento automatizado: Proporciona acceso unificado y automático a las aplicaciones y servicios, basado en funciones.

- Automatiza la creación de cuentas y el acceso a aplicaciones y servicios.
- Activa automáticamente cambios en los accesos del usuario si ha habido cambio de rol del empleado.
- Elimina cuentas si el usuario abandona la organización

1.2 IDENTITYIQ COMPLIANCE MANAGER

Certificaciones de acceso: Permite revisar y ejecutar rápidamente revisiones de acceso en todas sus aplicaciones y recursos.

Separación de funciones: Detecta y evita conflictos de intereses y posibles fraudes en todas las aplicaciones con la separación de funciones basada en políticas.

1.3 CONECTORES E INTEGRACIONES AVANZADAS

La lista de conectores disponibles bajo la plataforma se encuentra documentada en el web de SailPoint [REF1].

2 OBJETO Y ALCANCE

El objeto del presente documento es servir como guía de buenas prácticas de seguridad durante la configuración del producto IdentityIQ v8.3p5 así como describir las configuraciones de seguridad recomendadas.

IdentityIQ se puede desplegar tanto en entornos on-premise como en entornos de nube públicas o privadas, además de soportar entornos virtualizados.

El repositorio, basado en una base de datos relacional, contiene todos los datos (identidades, estructuras, permisos, recursos, roles…etc) y configuraciones del sistema (flujos de trabajo, asignaciones, delegaciones, ámbitos, formularios…etc)

El acceso a la herramienta, y su configuración, se realiza mediante acceso al portal web de la herramienta.

El producto SailPoint IdentityIQ v8.3p5 ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF25].

3 ORGANIZACIÓN DEL DOCUMENTO

La estructura del presente Procedimiento de Empleo Seguro se divide en los siguientes apartados:

a) Apartado 4. **Fase Previa a la instalación**: En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. **Fase de instalación:** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. **Fase de configuración:** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado 7. **Fase de operación**: En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Para instalación SailPoint IdentityIQ es necesario descargar la versión deseada, en este caso 8.3p5, que se encuentra disponible en la web de soporte de SailPoint (*Compass Community*) con el nombre *identityiq-8.3p5.jar*. El acceso a dicha web se hace mediante usuario y contraseña después de realizar el autorregistro.

Además, en la web de descarga [REF26] de SailPoint IdentityIQ se puede encontrar el valor del hash, en la sección *Downloads*, el cual se puede usar para verificar la integridad del fichero descargado mediante el comando Get-FileHash en la consola de Powershell:

```
$Get-FileHash identityiq-8.3p5.jar | Format-List
```

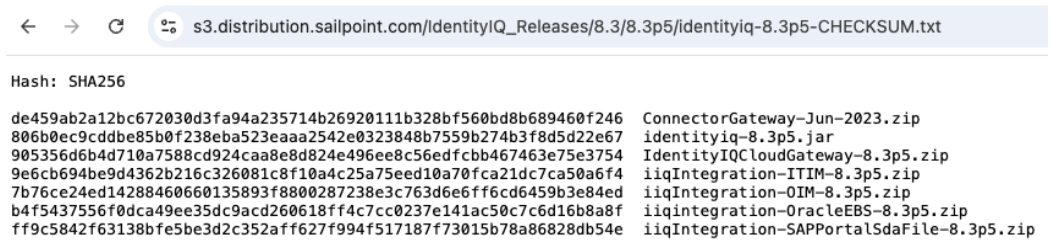


Figura 2: Descarga de Software

Comprobar que la web es la correcta y la validez del certificado de la web antes de iniciar la descarga o comprobar el hash. En caso de duda póngase en contacto con el proveedor.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Los componentes del producto deben instalarse en un entorno en el que el personal técnico encargado disponga de autorización para la configuración, despliegue y mantenimiento del producto. Además, se requiere de un control de acceso físico para limitar el personal con acceso físico al producto.

4.3 REGISTRO Y LICENCIAS

SailPoint IdentityIQ no requiere la activación de licencias para su instalación o uso.

4.4 CONSIDERACIONES PREVIAS

Previo proceso de instalación será necesario:

a) Revisar las plataformas soportadas (hardware y software) por SailPoint IdentityIQ.

b) Identificar el número de servidores y sus características hardware para soporta la organización.

4.4.1 PLATAFORMAS SOPORTADAS

Sistemas Operativos	• Windows Server 2022 y 2019 • Solaris 11 y 10 • IBM AIX 7.3 y 7.2 • Red Hat Linux 8.5 • SuSe Linus 15
Servidores de aplicación	• Apache Tomcat 9.0 • Oracle WebLogic 14c y 12cR2 • IBM WebSphere 9.0 • JBoss Enterprise 7.4 y 7.3 • IBM WebSphere Liberty 21.0 y 20.0
Base de datos	• IBM DB2 11.5 • MySQL 5.7 y 8.0 • MS SQL Server 2019 y 2017 • Oracle 19c
Plataformas nube	• AWS EC2 • AWS Aurora • AWS RDS (MySQL, MS SQL, Oracle) • Azure (VM, Azure SQL) • Google Cloud Platform - Google Compute Engine
Plataforma Java	• Sun, Oracle o IBM JDK 1.8 (8), JDK 11 y JDK 17. • OpenJDK11 y Adopt OpenJDK 11 • Hat OpenJDK 11 y 17 para Linux.

Tabla 1: Plataformas soportadas

Para más información, revisar la documentación detallada referente a la instalación en el portal de documentación de SailPoint en [REF2], en el apartado prerrequisitos de instalación.

4.4.2 ARQUITECTURA DE DESPLIEGUE

SailPoint IdentityIQ ofrece una arquitectura compuesta por tres (3) capas:

a) Repositorio Central (capa de datos)

b) Interfaz de usuario (capa de presentación)

c) Aprovisionamiento (capa de aplicación)

Estas tres capas pueden distribuirse entre un único servidor o multitud de servidores para ofrecer alta disponibilidad y tolerancia a fallos.

Para definir la estrategia de despliegue de SailPoint IdentityIQ, basado en las 3 capas mencionadas con anterioridad, se tendrá en cuenta el número de identidades que la organización vaya a manejar según los datos de la siguiente tabla:

Categoría	Descripción
Micro	Instalación en un entorno no-productivo por debajo de las 5.000 identidades. Todos los componentes se desplegarán sobre un mismo servidor incluido la base de datos.
Pequeña	Instalación para un entorno hasta 10.000 identidades.
Mediana	Instalación para un entorno entre 10.001 y 50.000 identidades.
Grande	Instalación para un entorno entre 50.001 y 500.000 identidades.
Personalizada	Instalaciones que tendrán que ser validadas por servicios profesionales de SailPoint.

Tabla 2: Aprovisionamiento

Las diferentes categorías de despliegue aquí descritas están soportadas bajo entorno virtualizados y entornos físicos.

4.4.2.1 MICRO

Entorno utilizado para sandbox o desarrollo. Todos los componentes, serán alojados sobre el mismo servidor, incluido la base de datos.

Requisitos mínimos:

- 1 servidor con IdentityIQ (con todos sus componentes) y motor de base de datos
- CPU: 1-2
- Memoria: 2GB, 4GB o más es recomendado.
- Espacio en disco: 40GB para los binaries de IdentityIQ, logs y datos de la base de datos

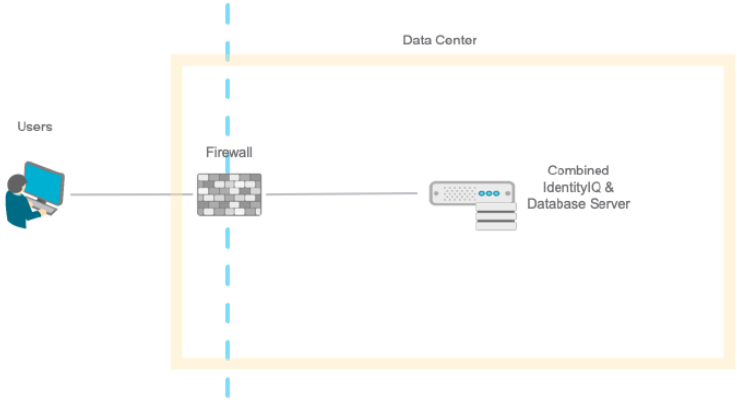


Figura 3: Arquitectura para Categoría de instalación Micro

4.4.2.2 PEQUEÑA

Entorno utilizado para organizaciones con un volumen de identidades inferior a 10.000. Los componentes se separan en dos servidores (interface de usuario y aprovisionamiento) y la base de datos está alojada bajo uno de ellos.

Requisitos mínimos:

- 2 servidores con IdentityIQ, uno de ellos con el motor de base de datos
- CPU: 4
- Memoria: 8GB
- Espacio: 50GB para los binaries de IdentityIQ y logs y datos de la base de datos
- Espacio base de datos: 250GB protegidos en RAID.

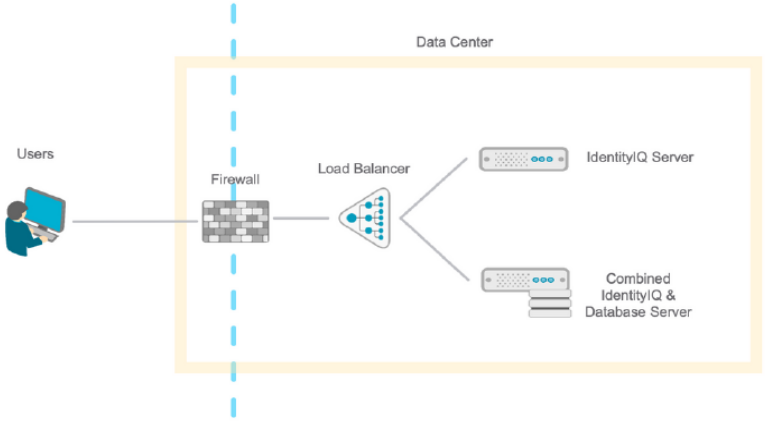


Figura 4: Arquitectura para Categoría de instalación Pequeña.

4.4.2.3 MEDIANA

Entorno utilizado para organizaciones con un volumen de identidades entre 10.001 y 50.000 identidades. Todos los componentes, interfaz de usuario, base de datos y aprovisionamiento (procesamiento por lotes) son separados para ofrecer alta disponibilidad y tolerancia a fallos en toda la arquitectura. Además, se recomienda que

el despliegue de balanceo de carga a nivel de interfaz de usuario por el volumen de carga.

Requisitos mínimos:

- 2 servidores con IdentityIQ de aprovisionamiento (procesamiento por lotes)
  - CPU: 4
  - Memoria: 8GB
  - Espacio: 50Gb, binarios y logs
- 2 servidores con IdentityIQ de interfaz de usuario
  - CPU: 4
  - Memoria: 8GB
  - Espacio: 50Gb, binarios y logs
- 1 servidor dedicado de base de datos
  - CPU: 8
  - Memoria: 64GB
  - Espacio: 500Gb para la base de datos y protegido RAID

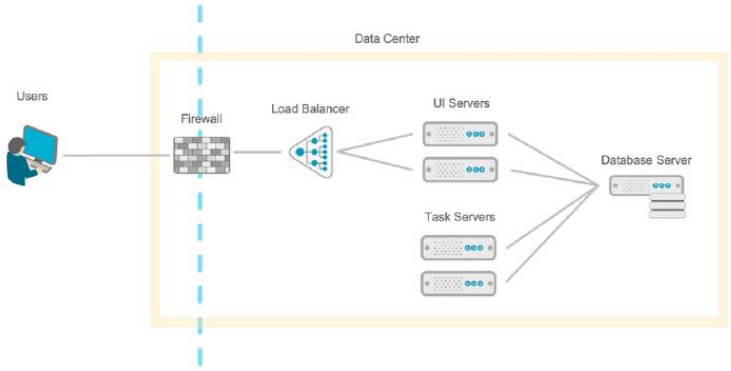


Figura 5: Arquitectura para Categoría de instalación Mediana

4.4.2.4 GRANDE

Entorno utilizado para organizaciones con un volumen de identidades entre 50.001 y 500.000 identidades. Todos los componentes, interfaz de usuario, base de datos y aprovisionamiento (procesamiento por lotes) son separados para ofrecer alta disponibilidad, tolerancia a fallos y rendimiento óptimo en toda la arquitectura. Además, se considera como requisito indispensable, el despliegue de balanceadores de carga y clusterización de base de datos.

Requisitos mínimos:

- 2 servidores con IdentityIQ de aprovisionamiento (procesamiento por lotes)
  - CPU: 4
  - Memoria: 16GB
  - Espacio: 50Gb, binarios y logs

- 2 servidores con IdentityIQ de interfaz de usuario
  - CPU: 4
  - Memoria: 8GB
  - Espacio: 50Gb, binarios y logs
- 1 servidor dedicado de base de datos
  - CPU: 16
  - Memoria: 128GB
  - Espacio: 1TB para la base de datos y protegido RAID

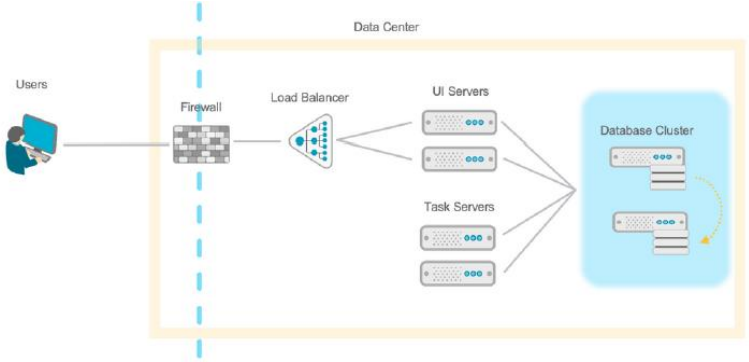


Figura 6: Arquitectura para Categoría de instalación Grande

Consideraciones de componentes adicionales a la arquitectura propuesta.

Descripción	Componente	Características
Plataforma para aprovisionar (alta, baja y modificación): • Directorio activo • SharePoint • Lotus Notes • AzureAD • Exchange	IQService	Ver documento de instalación de IQServices [REF3]
Permite a IdentityIQ conectarse de forma segura y administrar de forma remota aplicaciones ubicadas en zonas diferentes a las de IdentityIQ no puede acceder directamente.	Cloud Gateway	Ver documento de instalación de Cloud Gateway. [REF4]
Mainframe: • RACF • ACF2 • Top Secret	Connector Gateway	Ver documento de instalación de Connector Gateway [REF5]

Tabla 3: Consideraciones adicionales

SailPoint IdentityIQ requiere para su instalación y operación, la configuración de cuentas y permisos de usuarios, tanto en los sistemas donde se vayan a desplegar como en los sistemas finales a gestionar.

Estos requisitos se encuentran definidos en la guía de instalación de [REF2], en el apartado prerrequisitos de instalación.

La instalación del motor de base de datos y el servidor de aplicación **queda fuera del ámbito de este documento**.

5 FASE DE INSTALACIÓN

5.1 INSTALACIÓN SEGURA

El proceso de instalación de SailPoint IdentityIQ, consiste en:

a) Despliegue de la aplicación (fichero *war*) sobre el servidor de aplicaciones

b) Ejecución de la creación de las bases de datos (*identityiq* e *identityiqplugin*)

Documento de referencia [REF2].

5.1.1 INTEGRACIÓN CON DIRECTORIO ACTIVO

Si la organización dispone, como parte de su proceso de aprovisionamiento, un directorio activo, será necesario añadir la instalación del componente: *IQService*.

5.1.1.1 ARQUITECTURA Y REQUISITOS

La arquitectura para realizar la integración con directorio es la siguiente:

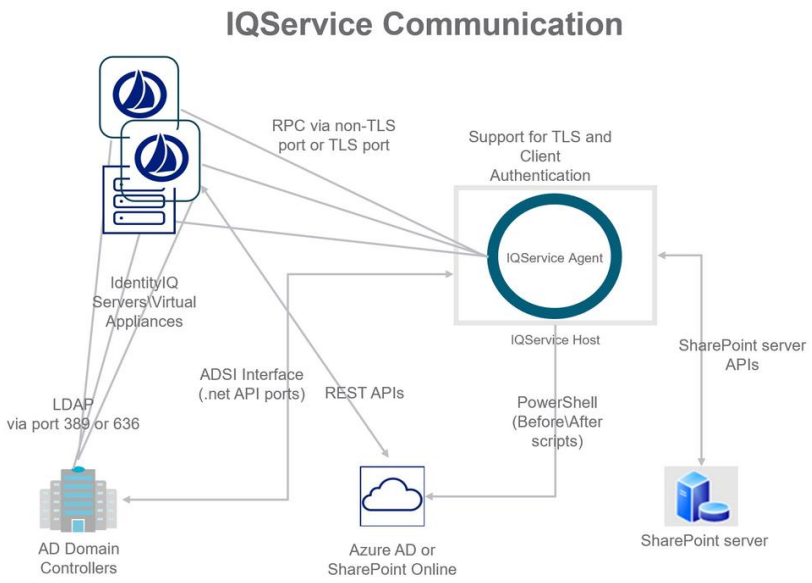


Figura 7: Diagrama de comunicación de IQService

Los requisitos para realizar esta integración será contar con un Servidor virtual o físico con las siguientes características:

- Sistema Operativo: Microsoft Windows 2019, 2016, 2012 R2 o 2012.
- Framework .NET 4.5.2
- CPU: 1, 2 recomendado
- Memoria: 500MB
- Espacio: 250MB

5.1.1.2 PROCESO DE INSTALACIÓN

Requisitos y el proceso de instalación del componente se encuentra referenciado en [REF3].

Despliegue del componente de IQService en alta disponibilidad, se encuentra referenciado en [REF6]

5.1.2 APLICACIONES REMOTAS

Si la organización dispone, de aplicaciones ubicadas en zonas diferentes a las de IdentityIQ no puede acceder directamente, será necesario añadir la instalación el componente: *Cloud Gateway*

5.1.3 ARQUITECTURA Y REQUISITOS

La arquitectura para realizar la integración con aplicaciones ubicadas en zonas diferentes es la siguiente:

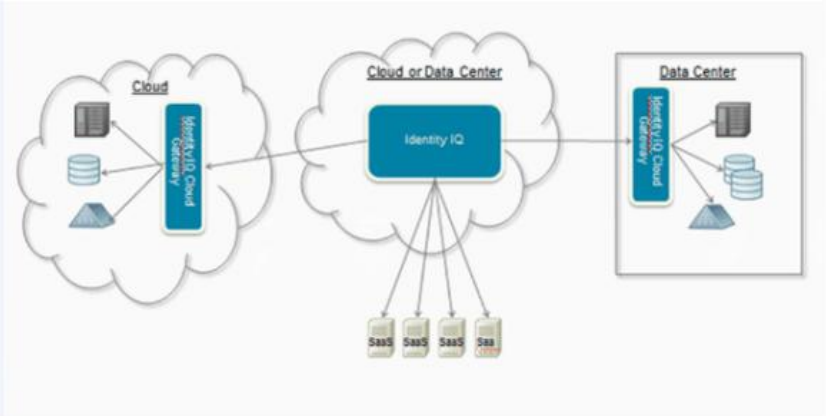


Figura 8: Diagrama de arquitectura

Los requisitos para realizar esta integración será contar con un Servidor virtual o físico con las siguientes características:

- Sistemas Operativos:
  - Microsoft Windows 2019, 2016, 2012 R2, 2012
  - Red Hat Enterprise Linux 8.0, 7.6, 7.4, 7.2 and 7.1
- Servidor de aplicaciones:

- Apache Tomcat versión 7.0 (prepaquetizad0 con IdentityIQ) 8.0. 9.0 y superiores
- Plataforma Java:
  - Sun, Oracle JRE para las versiones de Java 7 u 8
  - OpenJDK 8 y 11
- CPU: 4 núcleos
- Memoria: 8GB
- Espacio: 50GB

5.1.3.1 PROCESO DE INSTALACIÓN

Requisitos y el proceso de instalación del componente se encuentra referenciado en [REF4]

Si la organización dispone, como parte de su proceso de aprovisionamiento, mainframe, será necesario añadir la instalación el componente: *Connector Gateway*.

Los Requisitos y el proceso de instalación del componente se encuentra referenciado en [REF5]

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Es importante notar que el producto hace uso de las librerías criptográficas, junto con la implementación de TLS, del sistema operativo, para el uso seguro de los protocolos y de las funcionalidades criptográficas necesarias.

Los cambios a realizar para el correcto uso de los protocolos y algoritmos criptográficos se han de hacer sobre el sistema operativo, ya que, como se ha mencionado anteriormente, el producto hace uso de las librerías del sistema operativo

6.1.1 HTTPS EN SERVICIOS WEB

Dada la variedad de servidor de aplicaciones soportados por SailPoint IdentityIQ, se adjunta una guía por cada uno de los servidores soportados. Se recomienda configurar TLS 1.2 o superior para proteger adecuadamente la comunicación.

a) Apache Tomcat [REF7]

b) Oracle WebLogic [REF8]

c) JBoss [REF9]

d) IBM WebSphere [REF10]

6.1.2 CONFIGURAR ALMACÉN DE CLAVES

En una instalación estándar de SailPoint IdentityIQ, todas las contraseñas se cifran utilizando el mismo secreto de cifrado.

Para la creación y gestión del almacén de claves (*keystore*), iniciar sesión administrativa por la línea de comando desde la carpeta WEB-INF/bin en SailPoint IdentityIQ:

a) Sistemas Unix

```
$ ./iiq keystore
```

b) Sistemas Windows

```
C:> iiq.bat keystore
```

Una vez aparece el prompt, escribir **addKey,** y pusar **y**

```
> addKey
Generate a new encryption key (y/n)?
y
Generating a new encryption key for keystore [/var/tomcat/webapps/identity
New encrpytion key successfully saved to keystore.
All application servers must be restarted for changes to take effect.
>
```

Listar la nueva key generada mediante el comando **list**

```
> list
Listing contents for keystore [/var/tomcat/webapps/identityiq/WEB-INF/clas
KeyAlias   Algorithm Format       Object

2          AES    RAW          javax.crypto.spec.SecretKeySpec@fffe81cd
>
```

Escribir **exit**, para salir de la consola

```
> exit
```

c) Copiar los ficheros generados iiq.dat e iiq.cfg en todos los servidores que componen la arquitectura de SailPoint IdentityIQ en la carpeta WEB-INF/classess (por defecto) o en la carpeta donde esté ubicado el fichero iiq.properties (si se ha cambiado previamente).

d) Reiniciar los servidores de aplicaciones.

e) Para más información consultar el Documento de uso KeyStore de IdentityIQ [REF11].

6.1.2.1 CLOUD GATEWAY

Si la arquitectura incluye el despliegue del componente Cloud Gateway, los archivos del almacén de claves deben estar presentes en el servidor que ejecuta el servicio Cloud Gateway.

Es necesario modificar el archivo iiq.properties para que apunte a la ubicación de los ficheros como se muestra en la imagen.

```
##### iiq.properties #####
#
# (c) Copyright 2008 SailPoint Technologies, Inc., All Rights Reserved.
#
# This file contains configuration settings for the Cloud Identity Bridge.
# For your unique environment, you will need to adjust the properties belo
#



#
# CIB Keystore and Master Password properties
#

# file location of the CIB keystore
# (override of the default $SPHOME/WEB-INF/classes/iiq.dat )
#
#keyStore.file=/example/path/filename
keyStore.file  = /var/lib/CloudGateway/iiq.dat

# encrypted master password
#
#keyStore.password=1:p+qvPBo4==
keyStore.passwordFile = /var/lib/CloudGateway/iiq.cfg

#
# CIB credentials and Master Password properties
#
cib.username=cibadmin
cib.password=1:p+qvPBo4Rig8PYlNWbr3Zg==
```

Figura 9: Ejemplo de fichero iiq.properties

6.2 AUTENTICACIÓN

El acceso del usuario a SailPoint IdentityIQ se controla mediante un proceso de en el que las credenciales de inicio de sesión se validan con una fuente de autenticación. El administrador del sistema puede configurar la aplicación web IdentityIQ para que la autenticación se realice de una de estas tres formas:

a) Autenticación interna de IdentityIQ

b) Configuración de autenticación *pass-through* (PTA)

c) SSO basado en SAML

De forma predeterminada, SailPoint IdentityIQ autentica los usuarios con autenticación interna. Sin embargo, la autenticación *pass-through* y SSO se puede habilitar y configurar a través del interfaz gráfico de IdentityIQ. De hecho, SailPoint IdentityIQ permite utilizar mecanismos de autenticación al mismo tiempo.

Para más información consultar el documento Pass-Through Authentication Overview [REF12] y al documento IdentityIQ SAML support guide

6.2.1 DATOS EN TRANSITO

La comunicación entre todos los componentes de la arquitectura de IdentityIQ puede y debe cifrarse cuando circule por redes externas a la organización.

Esto incluye los datos enviados desde el servidor de aplicaciones de IdentityIQ a la base de datos y los datos intercambiados hacia y desde los sistemas destino (directamente o a través de agentes/servicios). El siguiente diagrama muestra las diferentes rutas de tránsito de datos que pueden cifrarse en SailPoint IdentityIQ, conector Gateway e IQService.

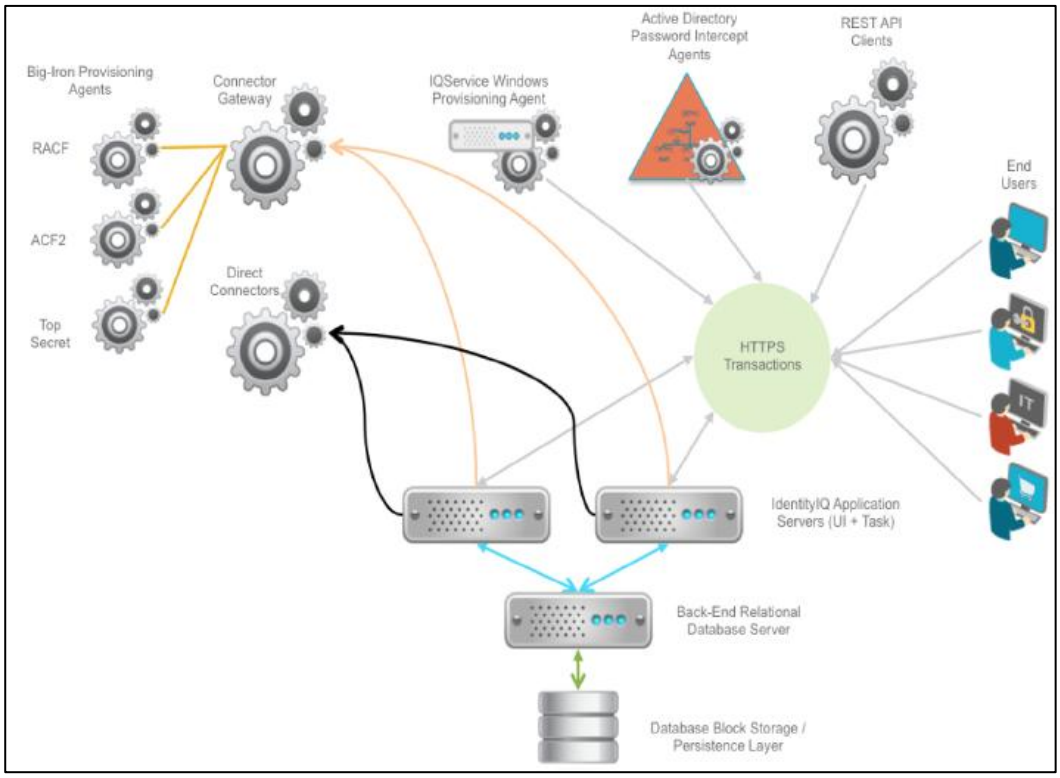


Figura 10: Rutas de tránsito de datos que pueden cifrarse en SailPoint IdentityIQ, conector Gateway e IQServices

Nota sobre cifrado: Los protocolos de comunicación son gestionados por el servidor de aplicaciones, no por IIQ, por lo que se pueden utilizar protocolos con cifrado de 3072 (mínimo) o 4096 (recomendado) bits, según lo requerido por CCN. Sin embargo, es importante aclarar que aunque IIQ lo soporta, la configuración debe realizarse en el servidor de aplicaciones (proporcionado por el cliente) y en los sistemas destino a los que se conecta IIQ.

IdentityIQ soporta los protocolos de cifrado SSL 3.0 y TLS 1.3 con certificados de 4096 bit.

Los datos sensibles (típicamente credenciales de autenticación) que se almacenan en IdentityIQ se cifran antes de guardarse en la base de datos, utilizando servicios proporcionados por Java en el paquete java.crypto. IdentityIQ utiliza un algoritmo de clave AES y un algoritmo de cifrado AES, y codifica los datos cifrados mediante codificación Base 64. IdentityIQ se entrega con una clave de cifrado predeterminada y se puede configurar para usar una clave almacenada en un almacén de claves en el sistema de archivos. IdentityIQ soporta el cifrado en tránsito al leer y escribir datos desde/hacia sistemas gestionados. Utilizamos tecnologías de cifrado disponibles como SSL y SSH al conectarnos a directorios, sistemas y bases de datos. IdentityIQ proporciona cifrado a través de SSL para muchos otros sistemas mientras los datos están en tránsito.

IdentityIQ funciona sobre redes TCP/IP y utiliza protocolos estándar (HTTP, HTTPS, FTP, XML/SOAP, SNTP, SNMP). IdentityIQ puede desplegarse para usar solo conexiones HTTPS, lo cual es fuertemente recomendado para entornos de producción. Los métodos

y versiones de cifrado específicos (SSL, TLS) soportados dependen de su servidor de aplicaciones.

6.2.1.1 SERVIDOR IDENTITYIQ E IQSERVICES

El Servidor de IdentityIQ y el servicio IQService vienen instalados con claves públicas y privadas predeterminadas. Una nueva clave de sesión se genera por solicitud y utilizada para cifrar el *payload*. La clave de sesión está cifrada con la clave pública de IQService.

Para cambiar los certificados utilizados de cifrado, consultar el documento Arquitectura IQService: puertos de comunicación. [REF3].

6.2.1.2 SERVIDOR IDENTITYIQ Y AGENTE INTERCEPTOR DE CONTRASEÑAS

El agente de intercepción de contraseña del directorio activo comunica los eventos de cambio de contraseña a IdentityIQ mediante una llamada a la API REST. Estas llamadas se realizan a los mismos hosts a los que se conectan los usuarios finales mediante el navegador.

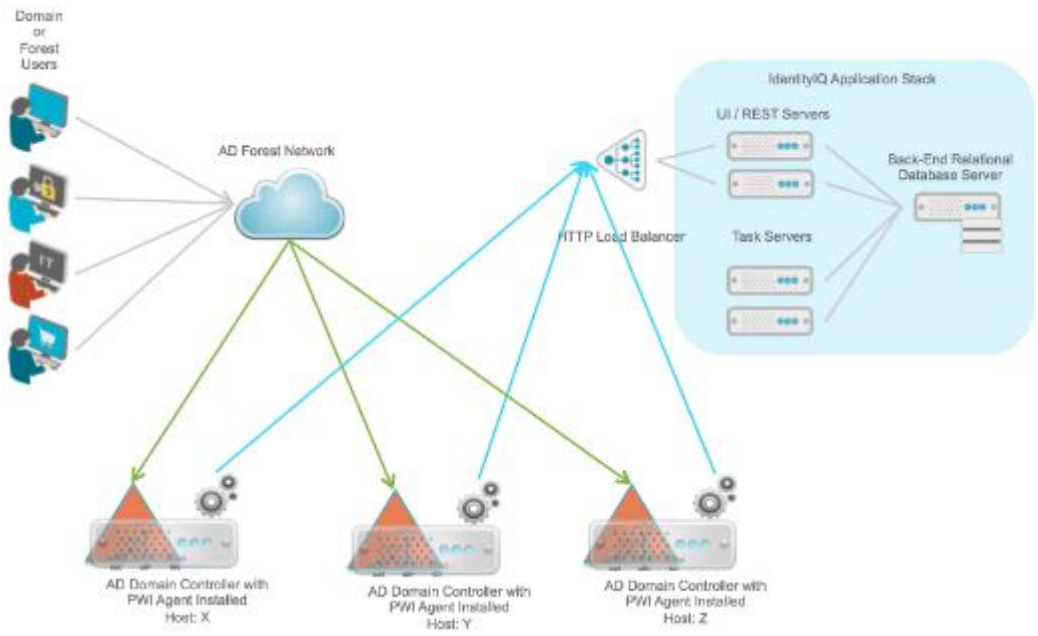


Figura 11: Despliegue de 3 agentes desplegados en 3 controladores de dominio.

El agente interceptor de contraseñas debe estar instalado en cada uno de los controladores de dominio gestionados por SailPoint IdentityIQ.

Para que el agente use encriptación FIPS, la instalación del agente se deberá realizar con el parámetro **useSiteSpecificEncryptionKey**.

La comunicación entre el servidor de IdentityIQ y el agente es encriptada utilizando TLS 1.2.

Para más información sobre configuración FIPS, y como deshabilitar Algoritmo FIPs consultar el siguiente enlace http://support.microsoft.com/kb/811833

6.2.1.3 SERVIDOR IDENTITYIQ Y USUARIOS

Los usuarios finales se conectan a los servidores web de IdentityIQ mediante un protocolo protegido por HTTPS. El mismo certificado SSL y mecanismo de cifrado se utiliza para proteger el tráfico entre los usuarios finales, los clientes REST y el Agente de intercepción de contraseñas de directorio activo e IdentityIQ.

6.2.1.4 SERVIDOR IDENTITYIQ Y BASE DE DATOS

IdentityIQ se conecta con bases de datos a través de controladores JDBC; sin embargo, estos no forman parte de los binarios del producto. Dependiendo del motor de base de datos utilizado, se deberá descargar los controladores necesarios. Revisar la Guía de instalación [REF2] .

La seguridad del transporte se puede configurar para proteger las comunicaciones entre los controladores JDBC y la base de datos. Los parámetros de configuración serán:

Cifrar la conexión entre los clientes y el servidor de la base de datos.

Autenticar el nivel de cliente de la red: el servidor de la base de datos solo acepta conexiones de clientes que tengan un certificado firmado por una autoridad confiable. Cualquier intento de conexión desde un nivel de cliente, una aplicación o instancia de IdentityIQ en la que la base de datos no confíe, fallará.

Autenticar el nivel de la base de datos: el controlador JDBC se puede configurar para validar el certificado de la base de datos. Si no ha sido firmado por una autoridad confiable, la conexión fallará. Desde el punto de vista de IdentityIQ, tiene pruebas de que se puede confiar en la base de datos.

Consulte la versión específica de su base de datos y controlador JDBC en los siguientes enlaces:

- Oracle https://www.oracle.com/technetwork/topics/wp-oracle-jdbc-thin-ssl-130128.pdf
- Microsoft SQL Server : https://docs.microsoft.com/en-us/sql/connect/jdbc/using-ssl-encryption?view=sql-server-2017
- IBM DB2: https://www.ibm.com/developerworks/data/library/techarticle/dm-1306securesocketlayers/
- MySQL : https://dev.mysql.com/doc/refman/5.7/en/encrypted-connections.html https://dev.mysql.com/doc/connector-j/5.1/en/connector-j-reference-using-ssl.html

El certificado y las claves que se utilizan aquí, son específicos para proteger este canal y no se pueden utilizar en ninguna otra parte del producto.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

SailPoint IdentityIQ provee dos modos de administración

a) **Línea de comando**: se podrá acceder de forma local o remota mediante la ejecución del comando iiq console desde la ruta /WEB-INF/bin. Podrán realizarse tareas administrativas como la ejecución de Workflows, exportación e importación de objetos, aprobar o rechazar un tarea (*workitem*), ejecutar un consulta sobre los objetos de la base de datos…etc. Para más información, consulte la Guía de uso de la consola para IIQ v8.3 [REF14] y [REF15]

b) **Interfaz web usuario**: permite establecer la configuración de todos los elementos que componen SailPoint IdentityIQ de forma gráfica y a través de interfaz web https://<nombre del host>:<puerto>/[directorio de la aplicación]

c) **Página de depuración**: ofrece capacidades avanzadas de edición de objetos para los administradores del sistema IdentityIQ, así como un lugar para encontrar información detallada de la instalación de SailPoint IdentityIQ. En las páginas de depuración, puede ver y editar todos los objetos, y objetos de configuración, en formato XML. El acceso es accesible vía portal web https://<nombre del host>:<puerto>/[directorio de la aplicación]/debug. Para más información, consúltela documentación alrededor del Debug pages. [REF16]

Se recomienda deshabilitar el acceso al portal web vía HTTP, para ello, consultar la guía de configuración del servidor de aplicaciones desplegado en la organización.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

En SailPoint IdentityIQ, las identidades (usuarios) que realizan tareas administrativas pueden ser asignados a permisos en SailPoint denominados *Capacidades*. Un Administrador puede crear y editar *Capacidades*, además de crear nuevos *Capacidades* que se adecuen a las necesidades de la organización. Para obtener más información sobre los permisos de la aplicación, se recomienda consultar la documentación asociada a la matriz de permisos de la [REF17].

Para más información de cómo generar modificar y crear nuevas *Capacidades*, consultar [REF18].

Una capacidad en IdentityIQ es el conjunto de uno o varios *SPRight.* Los permisos se otorgan a través de grupos de capacidades.

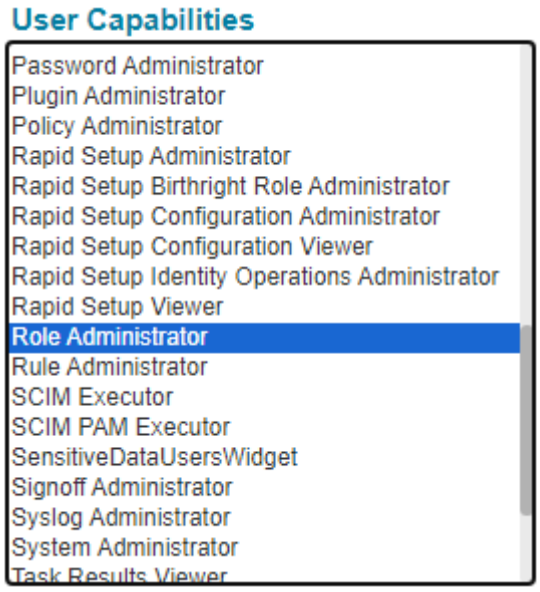


Figura 12: Listado de capacidades



Figura 13: Detalle de la herencia de capacidades

Como se ve en la imagen superior, la capacidad “Role Administrator”, está compuesto por la herencia de varias capacidades (*InheritedCapabilities*) y referencia a diferentes permisos (*RightRefs*)

La capacidad que otorga permisos para administrar toda la plataforma es el “*Role Administrator*”.

Existen otras capacidades, de forma granular, que serán otorgadas según las necesidades de la organización a la hora de administrar. Existen ya capacidades predefinidas para administrar:

a) Aplicaciones

b) Syslog

c) Sistemas

d) Administrador de Contraseñas

e) Otras

Consultar la matriz de compatibilidades [REF17]

Si no existiera un rol que se adecue a las necesidades de la organización, se podrá crear una capacidad a medida con los SPRights necesarios.

6.3.3 POLÍTICA DE CONTRASEÑAS

SailPoint IdentityIQ también actúa como punto central para la aplicación de políticas de contraseñas, al definir las políticas que las contraseñas deben cumplir. Se ha de tener en cuenta que el administrador debe asegurarse de que los sistemas externos no apliquen políticas de contraseñas más estrictas que SailPoint o, de lo contrario, la sincronización de contraseñas puede fallar debido a políticas contradictorias.

Para configurar la política de contraseñas, desde la consola Web de administración, Gear > Global Settings > IdentityIQ Configuration, pestaña Password se deben establecer los siguientes parámetros de configuración para tener una gestión de contraseñas segura:

- **Longitud mínima y máxima de la contraseña**. Se deberá configurar una longitud mínima de 12 caracteres, aunque se recomienda una longitud de 15.
- **Validez de la contraseña**. El valor recomendado para la vigencia y expiración de contraseñas es de 30 días.
- **Histórico de contraseñas**. No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas
- **Complejidad**. Las contraseñas deberán estar compuestas por una mezcla de mayúsculas, minúsculas, números y caracteres especiales (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”).

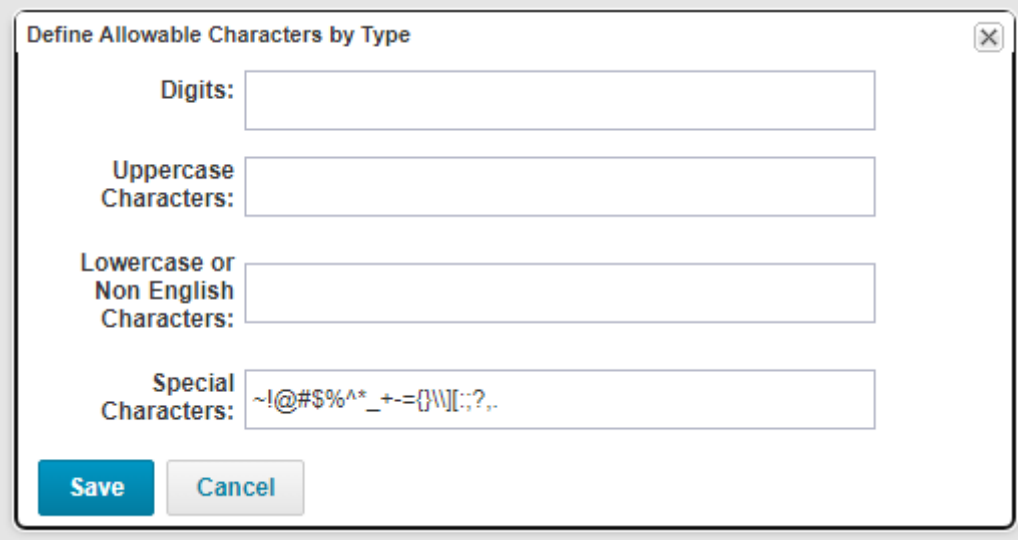


Figura 14: Pantalla de definición de caracteres permitidos en la contraseña

- **Habilitar la validación de la contraseña contra diccionario.**
- **Habilitar la validación de la contraseña contra atributos de la identidad.**

En la siguiente imagen se muestran todos los parámetros de configuración:



Figura 15: Pantalla de definición de política de contraseña

Para más información, consultar página 20 del documento IdentityIQ System [REF19].

Para configurar el inicio de sesión, desde la consola Web de administración, Gear > Global Settings > Login Configuration, pestaña Login Settings se deben establecer los siguientes parámetros de configuración para tener una gestión de inicio de sesión segura:

- **Máximo número de logins fallidos**. Se deberá configurar el bloqueo de las cuentas al introducir, como mucho, 5 intentos erróneos.
- **Número de minutos que un usuario será bloqueado debido a un acceso indebido**: establecerlo a 60 minutos.
  a) En la siguiente imagen se muestran todos los parámetros de configuración:

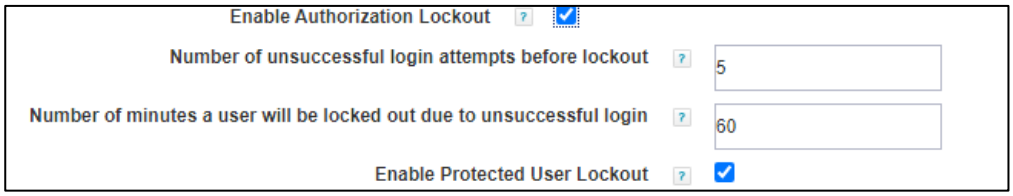


Figura 16: Parámetro de configuración de inicio de sesión

Para más información, consultar página 21 del documento IdentityIQ System Configuration [REF19].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

SailPoint proporciona canales de comunicación fiables usando TLS 1.2 para las siguientes conexiones:

- IdentityIQ y Agente capturador de contraseñas de directorio activo [REF20]
- IdentityIQ con IQService [REF3]
- IdentityIQ con el componente Connector Gateway [REF5]
- IdentityIQ con la base de datos.
  - Oracle: https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-6AD89576-526F-4D6B-A539-ADF4B840819F
  - Microsoft SQL Server : https://learn.microsoft.com/es-es/troubleshoot/sql/database-engine/connect/tls-1-2-support-microsoft-sql-server
  - IBM DB2: https://www.ibm.com/docs/en/db2/11.5?topic=transit-tls-configuration-db2
  - MySQL: https://dev.mysql.com/doc/mysql-security-excerpt/5.7/en/encrypted-connection-protocols-ciphers.html

Se deberá usar TLS 1.2 para las comunicaciones mencionadas.

Los siguientes conectores soportan conexión TLS:

- Mainframe (AS / 400, RACF, ACF2, Top Secret)
- LDAPS
- Directorio activo
- Sybase
- Salesforce
- Microsoft SQL Server
- Workday

Además, SailPoint IdentityIQ proporciona canales de comunicación confiables entre él y los sistemas basados en UNIX que utilizan SSH para la transferencia de datos de políticas. El uso de claves privadas con su correspondiente passphrase.

Para más información, consultar la lista de conectores disponibles en SailPoint IdentityIQ 8.3 [REF1]

6.5 GESTIÓN DE CERTIFICADOS

En caso de que SailPoint IdentityIQ se despliegue sobre plataforma Windows, los certificados y sus claves privadas asociadas se guardan en el almacén de certificados de Windows. Windows almacena claves privadas cifradas mediante RSA. Toda la gestión de claves es responsabilidad de los componentes criptográficos del sistema operativo en los que se basa el producto.

En caso de que SailPoint IdentityIQ se despliegue sobre plataforma Linux, los certificados y sus claves privadas asociadas se guardan en el almacén de certificados KeyStore [REF11]

6.6 SERVIDORES DE AUTENTICACIÓN

SailPoint IdentityIQ soporta diferentes métodos de autenticación como se ha visto en la sección 6.2 AUTENTICACIÓN.

Por defecto, el inicio de sesión se realiza con un identificador de usuario y contraseña local de la base de datos de IdentityIQ.

Se puede delegar la autenticación en servicios externos:

- Pass-through (PTA)
- Inicio Único (SSO)
- Local

6.6.1 AUTENTICACIÓN MEDIANTE MÉTODO DE *PASS-THROUGH* (PTA)

Con la autenticación *pass-through (PTA)*, el usuario inicia sesión en la aplicación IdentityIQ a través de la página de inicio de sesión normal de IdentityIQ, pero el sistema valida las credenciales del usuario contra una fuente externa, "pasando" el ID y la contraseña al sistema de autorización en lugar de consultar el sitio web de IdentityIQ.

Sistemas de autenticación soportados:

- Directorio Activo
- Directorio LDAP

Establecer configuración de inicio de sesión bajo la sección "*Configuración de Inicio de sesión*"

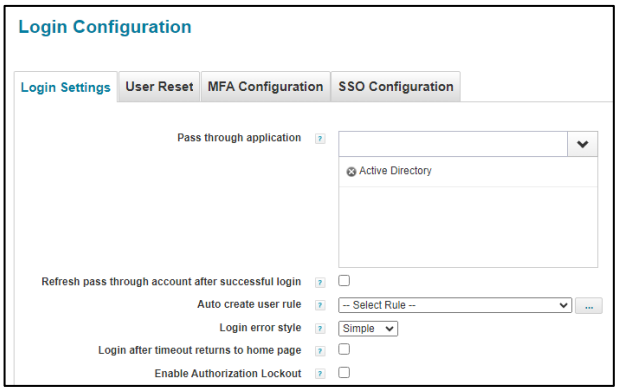


Figura 17: Pantalla de configuración de Inicio de sesión.

6.6.2 AUTENTICACIÓN MEDIANTE INICIO ÚNICO (SSO)

El inicio de sesión único (SSO) permite que los usuarios inicien sesión en IdentityIQ utilizando el estándar Security Assertion Markup Language (SAML). Este permite el intercambio de información, tanto de autenticación como de autorización entre diferentes partes: un proveedor de identidad y un proveedor de servicios

Existen dos tipos de autenticación Single Sign-On (SSO) soportadas por IdentityIQ:

- Basado en regla
- La regla tiene implementar la validación de cabeceras (firma de campos que identifiquen al usuario) y el mapeo de la cuenta a la identidad.

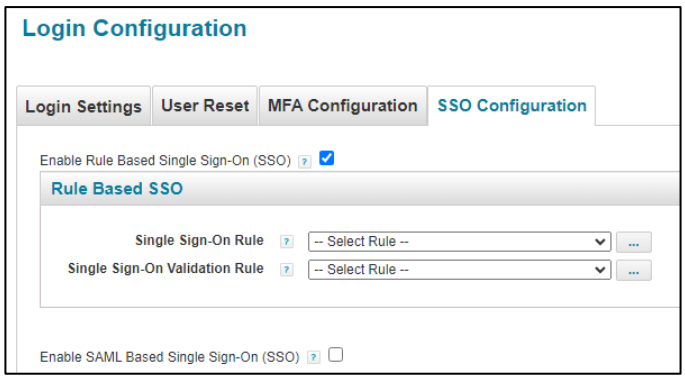


Figura 18: Pantalla de configuración de SSO basado en regla

- SAML SSO

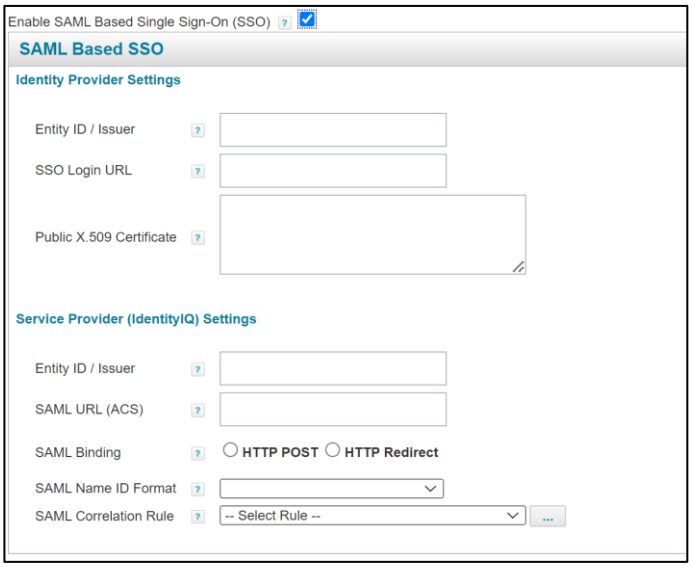


Figura 19: Pantalla de configuración de SSO basado en SAML

6.6.3 AUTENTICACIÓN MEDIANTE CUENTA LOCAL

Por defecto, la autenticación de IdentityIQ es con usuario y contraseña local.

6.6.4 ORDEN DE PROCESAMIENTO DEL MÉTODO DE AUTENTICACIÓN

Dado que SailPoint IdentityIQ permite configurar múltiples repositorios para el inicio de sesión, el orden de procesamiento es:

a) Inicio de sesión único (SSO) / basado en regla

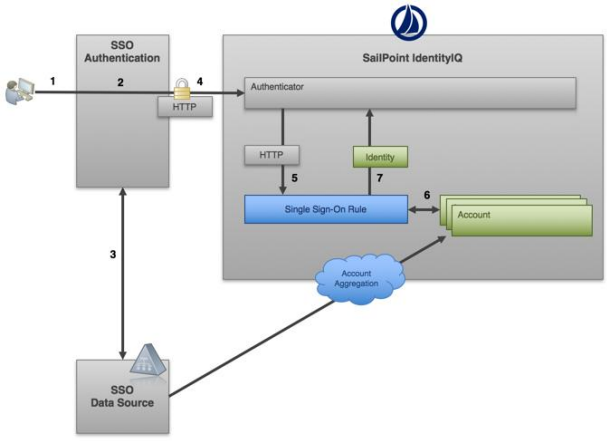


Figura 20: Diagrama de inicio de sesión único (SSO)

b) Autenticación *pass-through (PTA)*

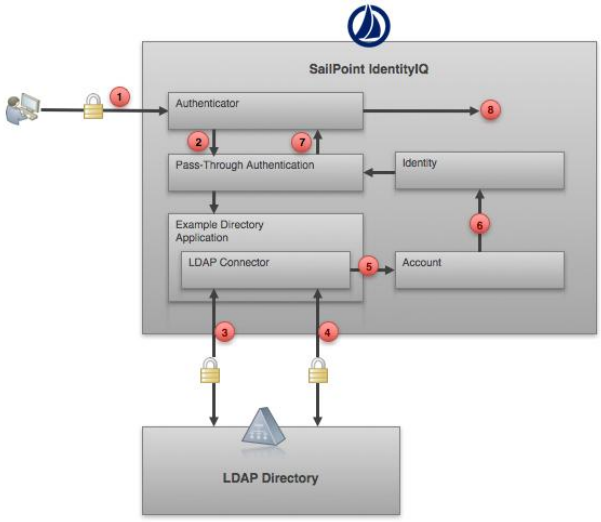


Figura 21: Diagrama de Autenticación pass-through

c) Autenticación local (base de datos)

Si la organización requiere un nivel adicional de autenticación para algunos o todos los usuarios de la organización, SailPoint IdentityIQ permite integración nativa con múltiples proveedores de autenticación (MFA).

Más información y detalle del proceso de configuración en el documento de Identity IQ Login Configuration [REF21].

6.7 ACTUALIZACIONES

La actualización de SailPoint IdentityIQ consiste en la actualización de la base de datos y de la aplicación web desplegada sobre los servidores de aplicación.

Dichas actualizaciones están disponibles en la web de soporte de SailPoint, y se puede descargar y comprobar su integridad de la misma manera que se descarga el software para la instalación inicial.

Antes de realizar cualquier proceso de actualización, se deberá realizar una copia de **seguridad de la base de datos de SailPoint IdentityIQ** así como de los ficheros de configuración y extensiones del producto que hayan sido modificados o personalizados durante el proceso de configuración.

Se deberá tener permisos administrativos tanto en el servidor donde está alojado SailPoint IdentityIQ como en el motor de base de datos para poder realizar la actualización de forma correcta.

Para más información acerca de las actualizaciones, los pasos exactos que se deben seguir para realizar la actualización de los componentes de SailPoint IdentityIQ, y las diferentes recomendaciones a tener en cuenta durante la actualización, se recomienda consultar la sección Updating SailPoint IdentityIQ de la guía de instalación de IdentityIQ [REF2].

6.8 ALTA DISPONIBILIDAD

SailPoint IdentityIQ se puede desplegar en alta disponibilidad, principalmente basada en el balanceo de los componentes web (aprovisionamiento e interfaz de usuario), por medio de balanceadores de tráfico, junto con las opciones de balanceo y alta disponibilidad del motor de base de datos utilizado, tal y como se muestra en la imagen siguiente:

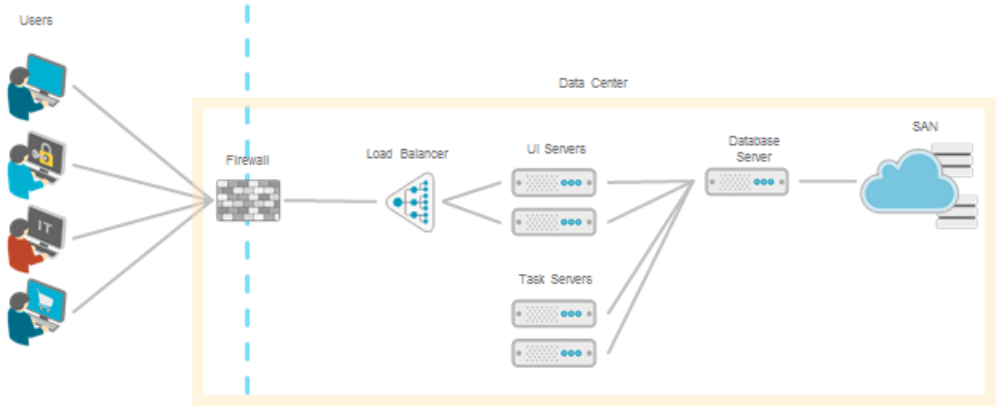


Figura 22: Arquitectura para instalaciones en Alta disponibilidad

Para obtener más detalle consultar la siguiente documentación relativa a recomendaciones de Arquitectura [REF22]

Para el almacenamiento de los datos se deberá disponer de replicación SAN. Esta replicación permite obtener una redundancia de los discos en caso de desastres mediante la replicación del almacenamiento mediante tecnologías propias de las cabinas de discos.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

SailPoint IdentityIQ mantiene los datos de auditoría en la base de datos. Todos los objetos, atributos, acciones y clases son susceptibles de ser auditados.

No todos los eventos auditables dan lugar a la generación de registros de auditoría. Para extender la auditoría y recopilar información adicional, se realiza a través del interfaz gráfico de usuario como se muestra en la siguiente imagen:

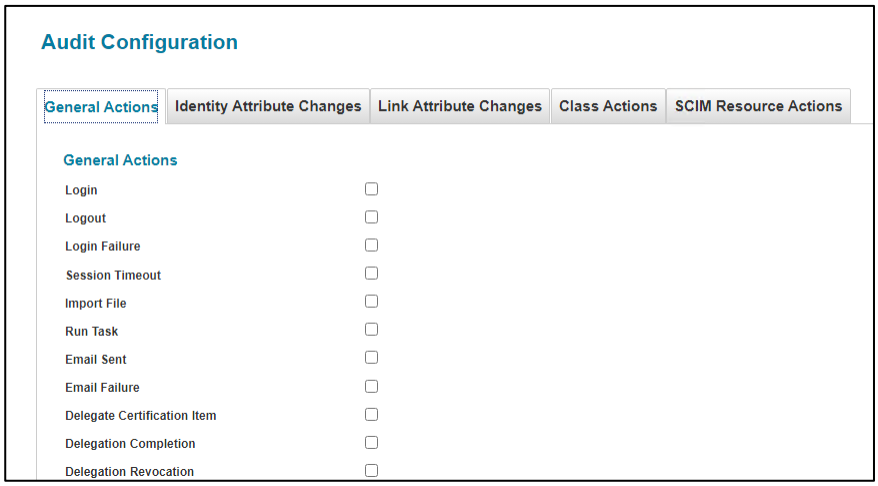


Figura 23: Interfaz de configuración de Auditoria

Para la visualización de los datos recuperados por la auditoría, se utiliza el interfaz gráfico en la sección análisis avanzado.

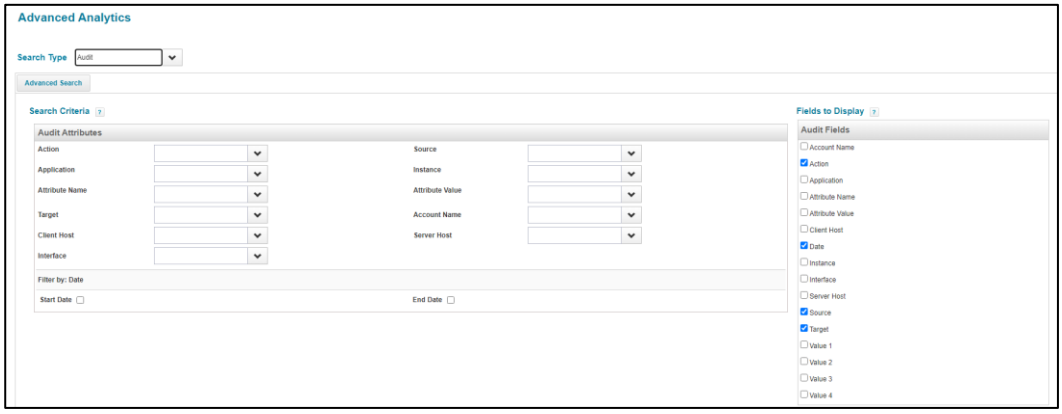


Figura 24: Interfaz de configuración de Analítica avanzada.

Como se muestra en la imagen superior, los datos que se pueden previsualizar (nombre de la cuenta, acción, aplicación, nombre del atributo, valor del atributo, fecha, instancia, interfaz, origen, destino, valor1, valor2, valor3 y valor4), será seleccionados por el usuario.

Para más información con respecto a auditoría, se recomienda revisar la documentación de configuración de Auditoria [REF23]

Los ficheros logs generados por IdentityIQ se basan en el mecanismo que provee Apache Log4J 1.2. La trazabilidad se configura mediante un fichero de propiedades ubicado en la siguiente ruta *WEB-INF/classess/log4j.properties*. En este archivo se configura el registro de salida y qué información se registra.

El contenido del formato, ver imagen inferior, de los ficheros logs generados, por defecto, cumplen con el siguiente patrón: %d{ISO8601} %5p %t %c{4}:%L - %m%n , para obtener más información sobre el significado de los parámetros de configuración consulte el siguiente enlace: https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html

En la siguiente imagen, se muestra el contenido del fichero logs de SailPoint IdentityIQ aplicando el patrón descrito con anterioridad.

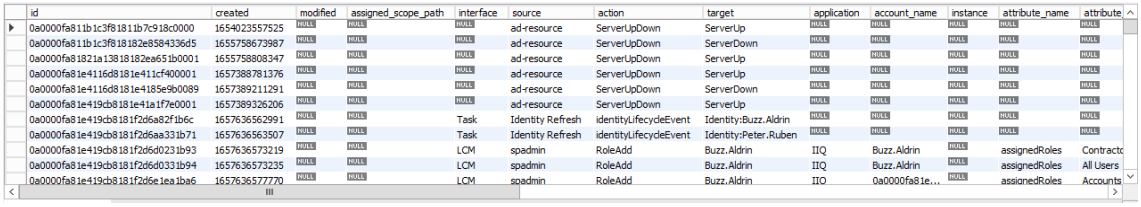


Figura 25: ejemplo de fichero logs de SailPoint IdentityIQ aplicando el patrón descrito con anterioridad.

Para más detalle sobre la configuración de logs de SailPoint IdentityIQ, consultar la [REF24]

6.9.2 ALMACENAMIENTO LOCAL

Los registros de auditoría se almacenan en SailPoint IdentityIQ como objetos *AuditEvent* y se almacenan en la tabla *spt_audit_event* de la base de datos.



id	created	modified	assigned_scope_path	interface	source	action	target	application	account_name	instance	attribute_name	attribute
0a0000fa811b1c3f81811b7c918c0000	1654023557525	NULL	NULL	NULL	ad-resource	ServerUpDown	ServerUp	NULL	NULL	NULL	NULL	NULL
0a0000fa811b1c3f818182e8584336d5	1655758673987	NULL	NULL	NULL	ad-resource	ServerUpDown	ServerDown	NULL	NULL	NULL	NULL	NULL
0a0000fa81821a13818182ea651b0001	1655758808347	NULL	NULL	NULL	ad-resource	ServerUpDown	ServerUp	NULL	NULL	NULL	NULL	NULL
0a0000fa81e4116d8181e411cf400001	1657388781376	NULL	NULL	NULL	ad-resource	ServerUpDown	ServerUp	NULL	NULL	NULL	NULL	NULL
0a0000fa81e4116d8181e4185e9b0089	1657389211291	NULL	NULL	NULL	ad-resource	ServerUpDown	ServerDown	NULL	NULL	NULL	NULL	NULL
0a0000fa81e419cb8181e41a1f7e0001	1657389326206	NULL	NULL	NULL	ad-resource	ServerUpDown	ServerUp	NULL	NULL	NULL	NULL	NULL
0a0000fa81e419cb8181f2d6a82f1b6c	1657636562991	NULL	NULL	Task	Identity Refresh	identityLifecycleEvent	Identity:Buzz.Aldrin	NULL	NULL	NULL	NULL	NULL
0a0000fa81e419cb8181f2d6aa331b71	1657636563507	NULL	NULL	Task	Identity Refresh	identityLifecycleEvent	Identity:Peter.Ruben	NULL	NULL	NULL	NULL	NULL
0a0000fa81e419cb8181f2d6d0231b93	1657636573219	NULL	NULL	LCM	spadmin	RoleAdd	Buzz.Aldrin	IIQ	Buzz.Aldrin	NULL	assignedRoles	Contracto
0a0000fa81e419cb8181f2d6d0331b94	1657636573235	NULL	NULL	LCM	spadmin	RoleAdd	Buzz.Aldrin	IIQ	Buzz.Aldrin	NULL	assignedRoles	All Users
0a0000fa81e419cb8181f2d6e1ea1ba6	1657636577770	NULL	NULL	LCM	spadmin	RoleAdd	Buzz.Aldrin	IIQ	0a0000fa81e...	NULL	assignedRoles	Accounts

Figura 26: Contenido de la tabla spt_audit_event

Además de la opción de Análisis avanzado para ver los registros a través de la interfaz de usuario (visto con anterioridad), un administrador puede ver los objetos a través de:

a) Páginas de depuración.

b) Consola iiq.

c) Acceso directo a la base de datos.

6.9.3 ALMACENAMIENTO REMOTO

Los eventos de registro se almacenan en una tabla de base de datos en lugar de en archivos planos, como se ha visto con anterioridad. El syslog de IdentityIQ, tiene tres opciones de configuración:

Opción	Descripción
Habilitar Syslog	Habilitar o deshabilitar syslog
Nivel del evento que será enviado al Syslogs	Seleccionar el nivel de trazabilidad (ERROR, WARN, FATAL)

Días antes de borrar los eventos del syslogs	Establecer el número de días que se mantiene la información del evento.

Tabla 4: Almacenamiento remoto

Para la visualización de los datos recuperados por syslogs, se utiliza el interfaz gráfico en la sección análisis avanzado.

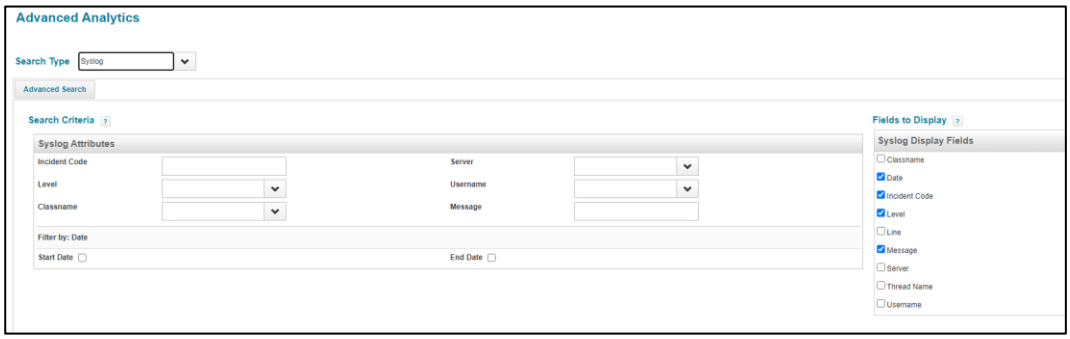


Figura 27: Interfaz de configuración de Analítica avanzada, con tipo de búsqueda Syslog.

La configuración del envío externo de la información de los eventos a un servidor de syslog, es necesario realizar la siguiente configuración adicional:

Establecer la configuración de syslog habilitada como se ha descrito con anterioridad.

Establecer un nuevo *appender* de tipo *SyslogAppender*, en el fichero de configuración de logs (*log4j.properties)* y establecer los parámetros de configuración necesario para el envío seguro de la información de los eventos al servidor de syslogs. Más información https://logging.apache.org/log4j/2.x/manual/appenders.html#SyslogAppender

6.10 BACKUP

SailPoint IdentityIQ almacena todos los datos de configuración en la base de datos por defecto. En caso de que se haya realizado personalización de IdentityIQ, y esta personalización se haya aplicado sobre el sistema de ficheros (ejemplo: cambio del logo, cambio en la configuración de colores del interfaz de usuario...etc) será necesario añadir estos cambios como parte del proceso de backup.

Si se ha establecido una nueva clave de encriptación (para más detalle de como generarla consultar la [REF22]), será necesario realizar backup de los ficheros iiq.dat e iiq.cfg ubicados en el directorio */WEB-INF/classess*

Se requiere un backup completo, con frecuencia diaria, de las bases de datos, siguiendo los procedimientos estándar del motor de base de datos utilizado y un backup, del sistema de ficheros, con una frecuencia semanal completa, donde esté desplegado la aplicación de SailPoint IdentityIQ.

Los backups de las bases de datos de SailPoint IdentityIQ deben almacenarse en un **sistema de ficheros externo a los servidores** donde se despliegan los componentes de la solución.

7 FASE DE OPERACIÓN

Durante la fase de operación de SailPoint IdentityIQ se recomienda llevar a cabo, al menos, las siguientes tareas para una gestión segura del producto:

- Comprobaciones periódicas del software para asegurar que no se ha introducido hardware o software no autorizado.
- Comprobaciones periódicas de los sistemas de antivirus desplegados en los servidores donde se han desplegado los componentes de SailPoint IdentityIQ.
- Aplicación regular de los parches de seguridad, con objeto de mantener una configuración segura en aquellos servidores donde se han desplegado los componentes de SailPoint IdentityIQ.
- Realizar copias de seguridad, al menos diarias, de las bases de datos de SailPoint IdentityIQ y en caso necesario, del servidor de ficheros.
- Realizar pruebas de restauración del servicio mediante las copias de seguridad en caso de desastre.
- Mantener los registros de auditoria en la base de datos, asegurando que el personal autorizado pueda acceder a ellos.
- Configurar el archivado de eventos y borrado en base a los criterios específicos requeridos.
- Establecer un plan de monitorización, desde la consola de Administración de SailPoint, sobre todos los componentes de SailPoint IdentityIQ además de todas las plataformas adyacentes que están siendo utilizadas.

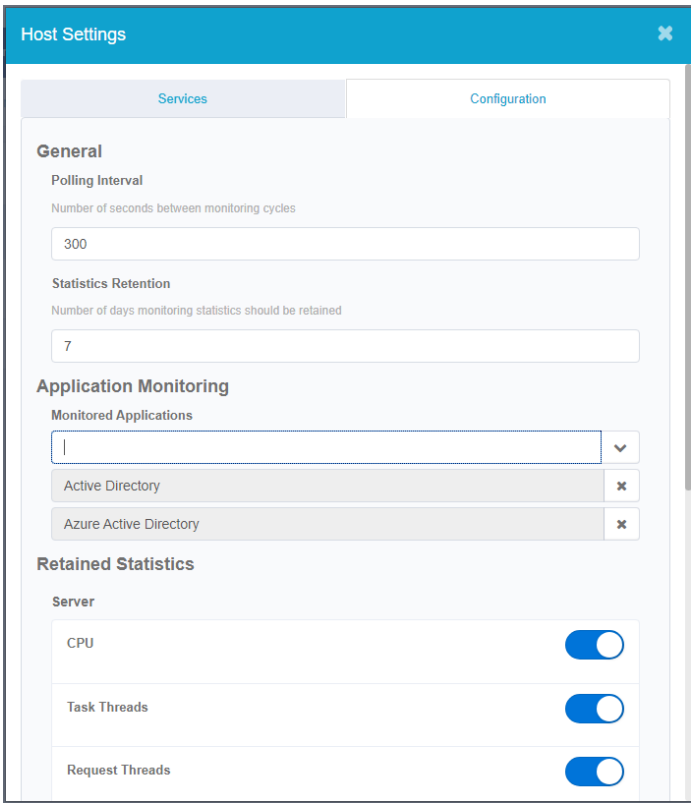


Figura 28: Pantalla para la configuración de la monitorización de aplicaciones.

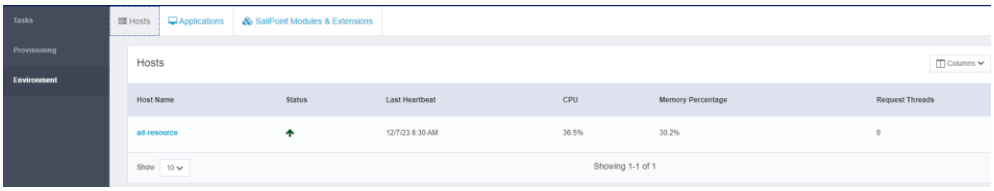


Figura 29: Estado del servidor de SailPoint IdentityIQ

- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.
- Revisión del estado de todas las tareas ejecutadas (fallo, pendientes, correctas) desde la consola de administración de SailPoint IdentityIQ

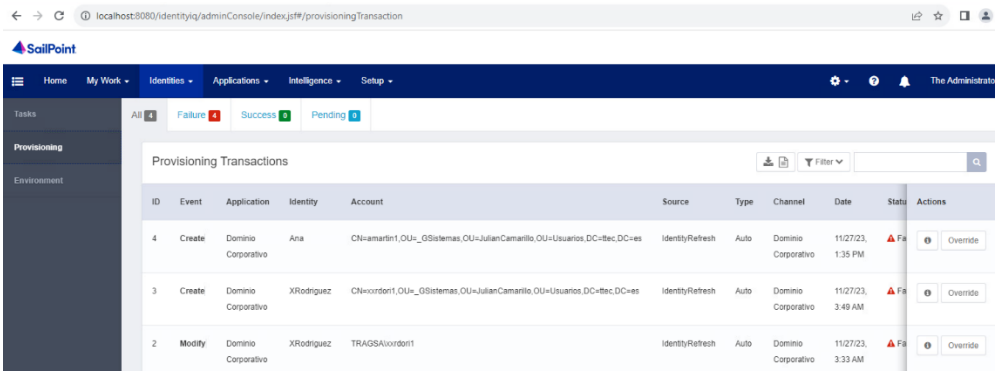


Figura 30: Listado de todas las tareas de aprovisionamiento

8 CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Configuración almacén de claves (keystore)	☐	☐	
Configuración de componentes de administración	☐	☐	
Revisar componentes adicionales de la arquitectura	☐	☐	
Configuración segura de IQService	☐	☐	
Configuración segura de Conector Gateway	☐	☐	
Configuración segura del servidor de aplicación	☐	☐	
Configuración segura del motor de base de datos	☐	☐	
Configuración de BACKUP	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Requisitos mínimos de contraseñas	☐	☐	
Configuración timeouts de sesión	☐	☐	
Configuración del método de autenticación	☐	☐	
Configuración de la auditoría	☐	☐	
Configuración del logging del tráfico relevante	☐	☐	
Configuración puertos y protocolos en modo seguro (TLS 1.2)	☐	☐	

Tabla 5: Checklist

9 REFERENCIAS

REF1 Lista de conectores
https://documentation.sailpoint.com/connectors/identityiq8_3/landingpage/landingpages/identityiq_8_3_landing.html

REF2 Guía de Instalación de SailPoint IdentityIQ
https://community.sailpoint.com/t5/IdentityIQ-Product-Guides/8-3-IdentityIQ-Installation-Guide/ta-p/214591

REF3 Guía de Instalación de IIQService
https://community.sailpoint.com/t5/IdentityIQ-Connectors/IQService-TLS-and-Client-Authentication-Configuration/ta-p/75273

REF4 Guía de Instalación Cloud Gateway
https://documentation.sailpoint.com/connectors/identityiq8_3/cloud_gateway/help/cloud_gateway/introduction.html

REF5 Guía de Instalación Connector Gateway
https://documentation.sailpoint.com/connectors/identityiq8_3/ca/top_secret_mainframe/help/common/main_frame/installing_and_configuring_connector_gateway.html#top

REF6 Documento de Arquitectura de IQService
https://community.sailpoint.com/t5/IdentityIQ-Wiki/IQService-architecture-Network-ports-and-firewalls/ta-p/77385

REF7 Configuración SSL / TLS en un servidor Tomcat
https://tomcat.apache.org/tomcat-8.5-doc/ssl-howto.html

REF8 Configuración SSL en un servidor WebLogic
https://docs.oracle.com/middleware/1213/wls/SECMG/ssl_overview.htm#SECMG718

REF9 Configuración SSL en un servidor JBoss
http://docs.jboss.org/jbossweb/7.0.x/ssl-howto.html

REF10 Configuración SSL en un servidor IBM
https://www.ibm.com/developerworks/websphere/techjournal/1210_lansche/1210_lansche.html

REF11 Documento de uso KeyStore de IdentityIQ
https://community.sailpoint.com/t5/Technical-White-Papers/Using-the-IdentityIQ-Keystore/ta-p/75490

REF12 Pass-through authentication and single sign-on
https://community.sailpoint.com/t5/IdentityIQ-Wiki/Pass-through-authentication-and-single-sign-on/ta-p/72140?attachment-id=534

REF13 Arquitectura IQService: puertos de comunicación.
https://community.sailpoint.com/t5/IdentityIQ-Wiki/IQService-architecture-Network-ports-and-firewalls/ta-p/77385#jive_content_id_Encryption_of_RPC_Communications

REF14 Listado de comandos disponibles en la consola de IIQ
https://documentation.sailpoint.com/identityiq_83/help/iiqconsole/viewcommands.htm?tocpath=IdentityIQ%20Console%7C_____3

REF15 Guía de la Consola IIQ para la versión 8.3
https://community.sailpoint.com/t5/IdentityIQ-Product-Guides/8-3-IdentityIQ-Console-Guide/ta-p/214145

REF16 Páginas de depuración
https://community.sailpoint.com/t5/IdentityIQ-Articles/Debug-pages/ta-p/78660

REF17 Matriz de Permisos 8.3
https://community.sailpoint.com/t5/Technical-White-Papers/Capabilities-Matrix-8-3/ta-p/214804

REF18 IdentityIQ Permisos y capacidades – Definición
https://community.sailpoint.com/t5/IdentityIQ-Articles/IdentityIQ-Rights-and-Capabilities-Definitions/ta-p/77550

REF19 Configuración del sistema IIQ
https://community.sailpoint.com/t5/IdentityIQ-Product-Guides/8-3-IdentityIQ-System-Configuration-Guide/ta-p/214161?attachment-id=11420

REF20 Documento de instalación del agente capturador de Password. https://community.sailpoint.com/t5/IdentityIQ-Wiki/Password-Interceptor-Client-installation-and-uninstallation/ta-p/225838

REF21 Identity IQ Login Configuration https://community.sailpoint.com/t5/Technical-White-Papers/IdentityIQ-Login-Configuration/ta-p/76904

REF22 Documento de recomendaciones relativas a Arquitectura. https://community.sailpoint.com/t5/Technical-White-Papers/Recommended-IdentityIQ-Deployment-Architectures/ta-p/74263

REF23 Documento de configuración de Auditoria. https://community.sailpoint.com/t5/Technical-White-Papers/Audit-Configuration-in-IdentityIQ/ta-p/74075#toc-hId-479769136

REF24 Guía de soporte de Log4j https://community.sailpoint.com/t5/Working-With-Support-Knowledge/Log4j-Support-Guide/ta-p/137421

REF25 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

REF26 URL de descarga https://community.sailpoint.com/t5/IdentityIQ-Server-Software/IdentityIQ-8-3p5/ta-p/266932

10 ABREVIATURAS

CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN
ENS	Esquema Nacional de Seguridad.
HTTPS	Protocolo seguro de transferencia de hipertexto (Hypertext Transfer Protocol Secure). Es la versión segura del protocolo HTTP utilizado para la transmisión segura de datos en la web
IGA	Administración y Gobierno de la Identidad (en inglés Identity, Governance and Administration)
JDBC	Conector de base de datos Java (Java Database Connectivity). Es una API que permite a las aplicaciones Java interactuar con bases de datos
JRE	Entorno de ejecución de Java (Java Runtime Environment). Contiene la JVM y otros componentes necesarios para ejecutar aplicaciones Java
Log4J	Marco de registro para aplicaciones Java. Facilita el registro de eventos y mensajes en aplicaciones Java
MFA	Autenticación de Factor Múltiple (Multi-Factor Authentication). Requiere múltiples métodos de verificación para confirmar la identidad de un usuario
RAID	Conjunto Redundante de Discos Independientes. Es una tecnología que combina múltiples discos duros para mejorar la confiabilidad y el rendimiento del almacenamiento de datos
SAN	Red de Área de Almacenamiento (Storage Area Network). Es una red especializada que conecta dispositivos de almacenamiento de datos a servidores.
SSL	Capa de sockets seguros (Secure Sockets Layer). Es un protocolo de seguridad que establece un enlace cifrado entre un servidor web y un navegador, garantizando la seguridad de la información transmitida
TLS	Capa de seguridad de transporte (Transport Layer Security). Es un protocolo de seguridad que garantiza la privacidad y la integridad de los datos transmitidos a través de una red