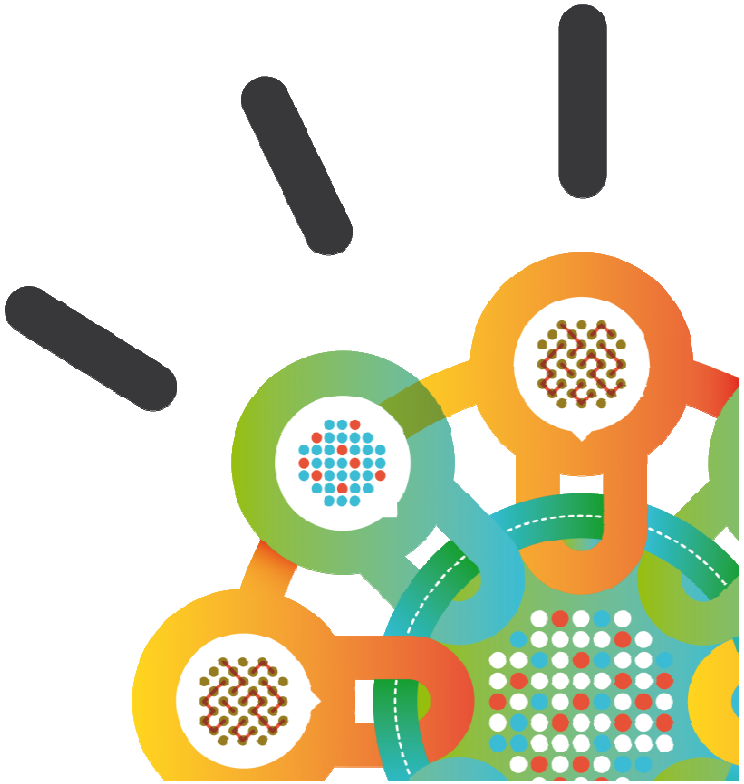
Security Intelligence.
Think Integrated.

Novedades en la gestión de Identidades y Accesos de IBM

10 Abril 2014

Juan Nemiña

juannemina@es.ibm.com



Gestión de Identidades y Accesos "Threat-Aware"
Un ambicioso lanzamiento en proceso

Nuevas capacidades para ayudar a las organizaciones a securizar la identidad corporativa como el nuevo perímetro en que se ha convertido

NEW

Simplificar la integración de directorios y silos de identidades

- Proporcionar visibilidad de todas las identidades disponibles en la empresa
- Unificar "Universos de Identidades" para la gestión de la seguridad

NEW

Prevenir las amenazas internas y el fraude asociado a la identidad

- Gestionar las cuentas privilegiadas y compartidas de la empresa
- Defender las aplicaciones frente a ataques y vulnerabilidades especificas

NEW

Proporcionar gobernanza de identidades y accesos inteligente

- Posibilitar la gestión de identidades a la Línea de Negocio
- Mejorar la monitorización de la actividad del usuario y la inteligencia en la seguridad de los dominios de seguridad

NEW

Proteger las interacciones en las redes sociales y los entornos móviles

- Validar "quién es quién" cuando los usuarios se conectan desde fuera de la red interna
- Posibilitar políticas proactivas de acceso a las redes sociales, entornos móviles y la nube

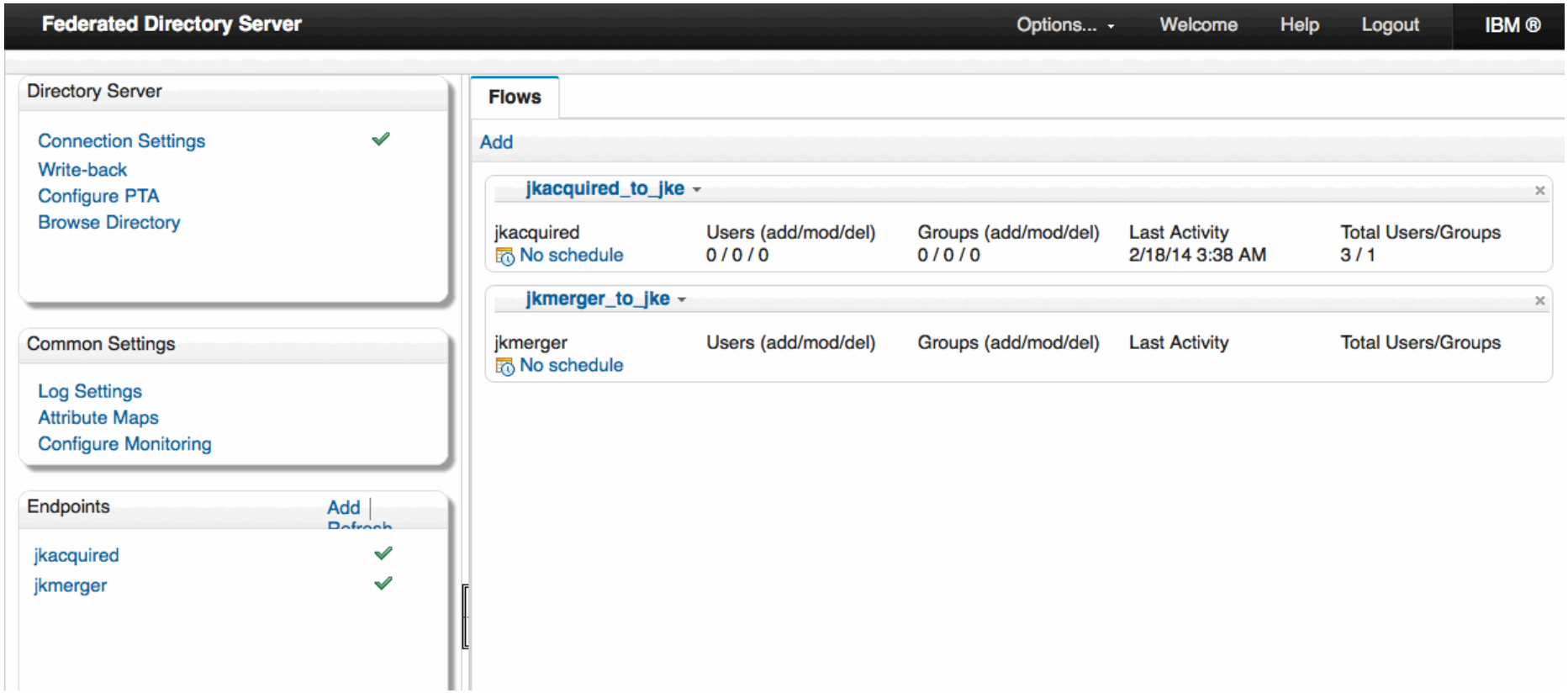
Simplificar la integración de directorios y silos de identidades

- Proporcionar visibilidad de todas las identidades disponibles en la empresa
- Unificar “Universos de Identidades” para la gestión de la seguridad

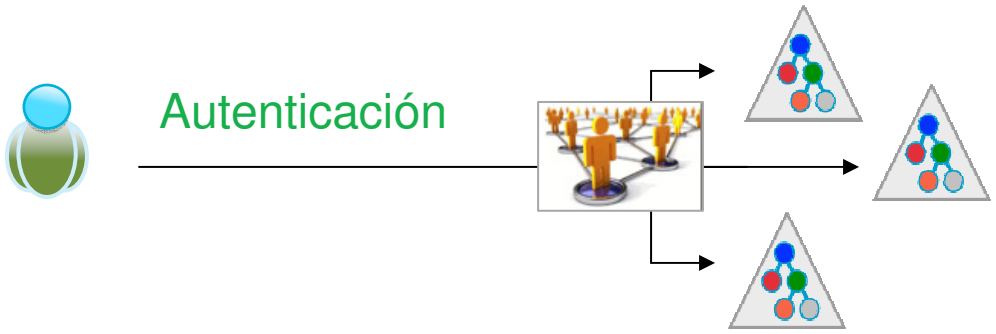
Federated Security Services

SDI 7.2 (contiene FDS)

- Disminuye dramáticamente el coste y el riesgo de los patrones de despliegue mas comunes
- Solución “Out-of-the-box” para + del 80% de los escenarios de integración de directorios

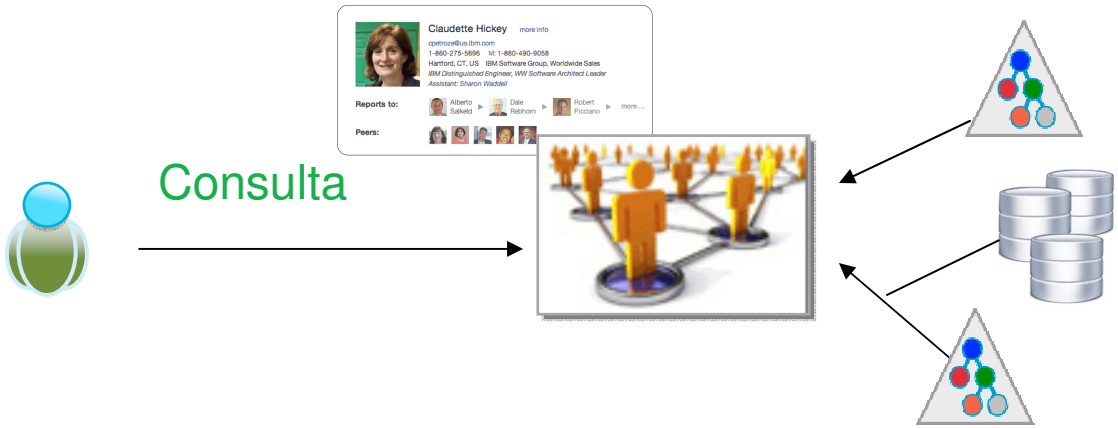


Escenarios principales de FDS :



Un único punto de contacto para la autenticación de las aplicaciones, para SSO, colaboración , etc...

Active Directory
RACF, IBM Directory
Sun/Oracle, Novell Domino, LDAPv3



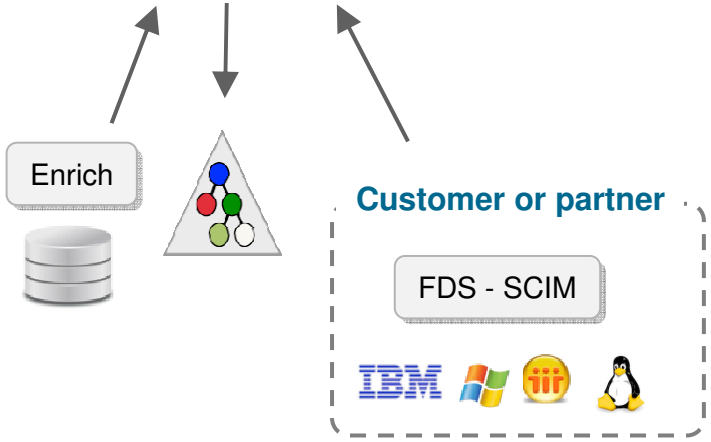
Búsqueda y vista de datos de identidad que han sido consolidados, aumentados, limpiados,…

Directorios, BBDD
Ficheros, SAP
Web services
… y muchos otros

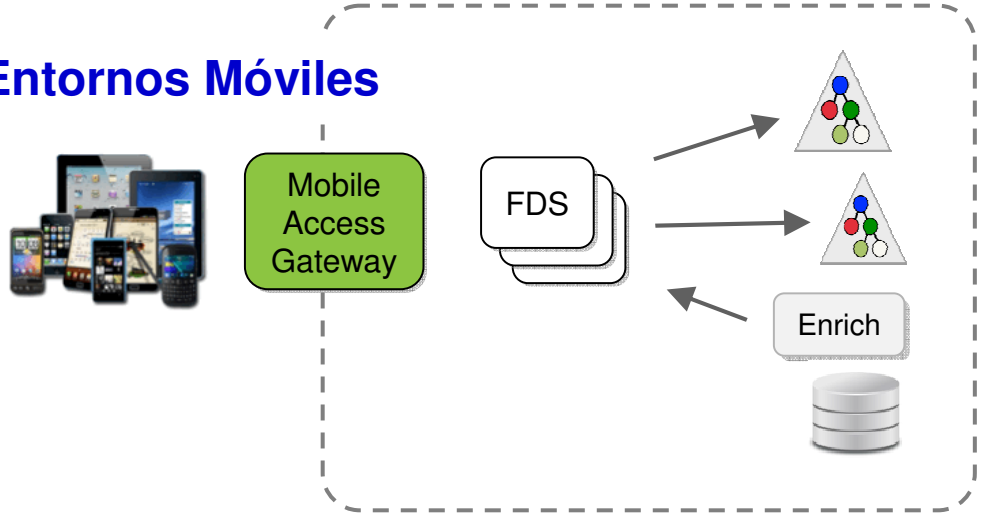
Entendemos que estos dos escenarios agrupan a la mayoría de los casos de uso

Directorio federado en la nueva empresa

Interacción con las redes sociales



Entornos Móviles



- Cuando se necesita que múltiples directorios parezcan uno
- Robusto, escalable y de alto rendimiento
- Corona, extiende y protege la infraestructura existente
- Enriquece los servicios de directorio con información de otras fuentes
- Mitiga el riesgo y el coste de integración de unidades de negocio independientes
- Interacción segura de la empresa con socios y clientes

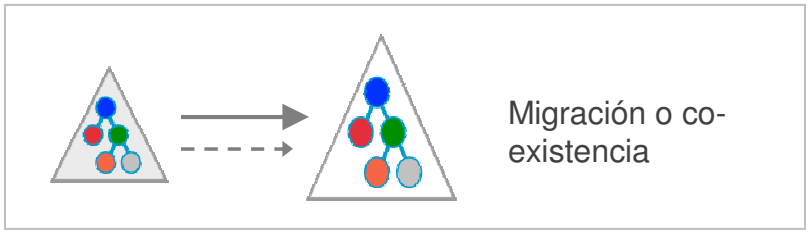
Que es FDS ?

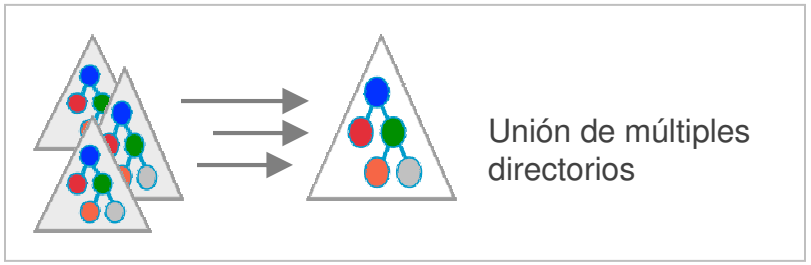
- **Desde el punto de vista comercial**
  - FDS se adquiere al adquirir SDI 7.2
  - SDI 7.2 se puede licenciar por User Value Units (Identity Edition) => el coste depende del número de usuarios o …
  - … por PVUs (General Purpose Edition) => el coste depende del número y tipo de servidores en los que se instala
  - Exactamente la misma funcionalidad en las dos ediciones (diferente en versiones anteriores)
  - **NO** está incluido en ISAM o ISIM (SDS si, FDS no)

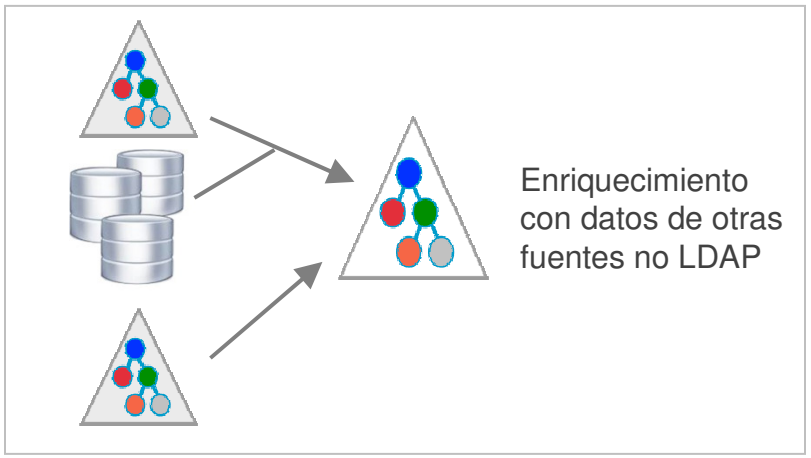
- **Desde el punto de vista técnico**
  - FDS es una aplicación basada en SDI que recupera cambios en directorios existentes y los aplica a un directorio SDS (y viceversa si se desea) => FDS incluye SDI y SDS
  - FDS puede configurarse para realizar *pass-through authentication* (PTA) en SDS => la aplicación "ve" SDS, la autenticación se realiza en el directorio original.

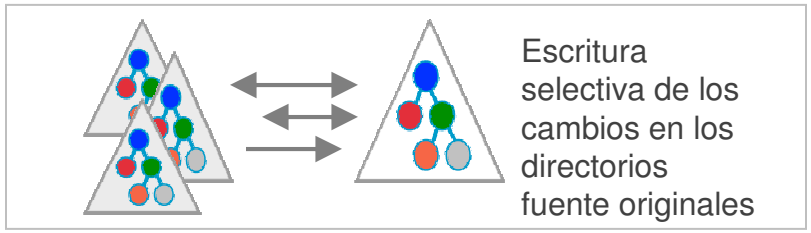
Licencia de SDI 7.2 = Licencia de SDI + SDS + FDS

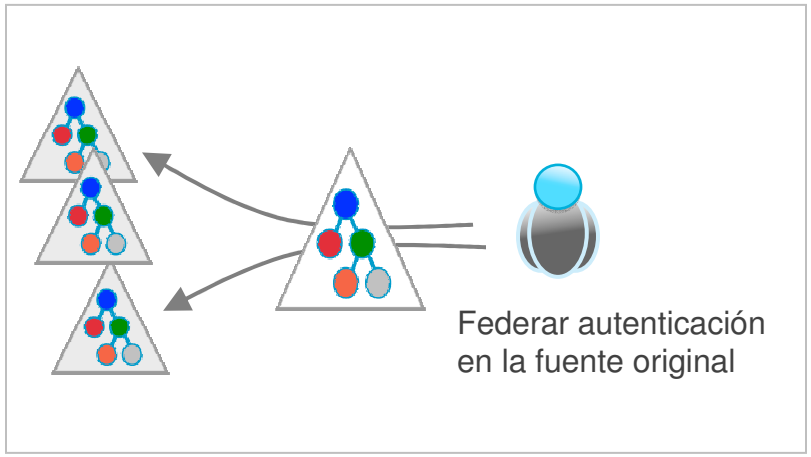
FDS => Autenticación distribuida + Consolidación de datos





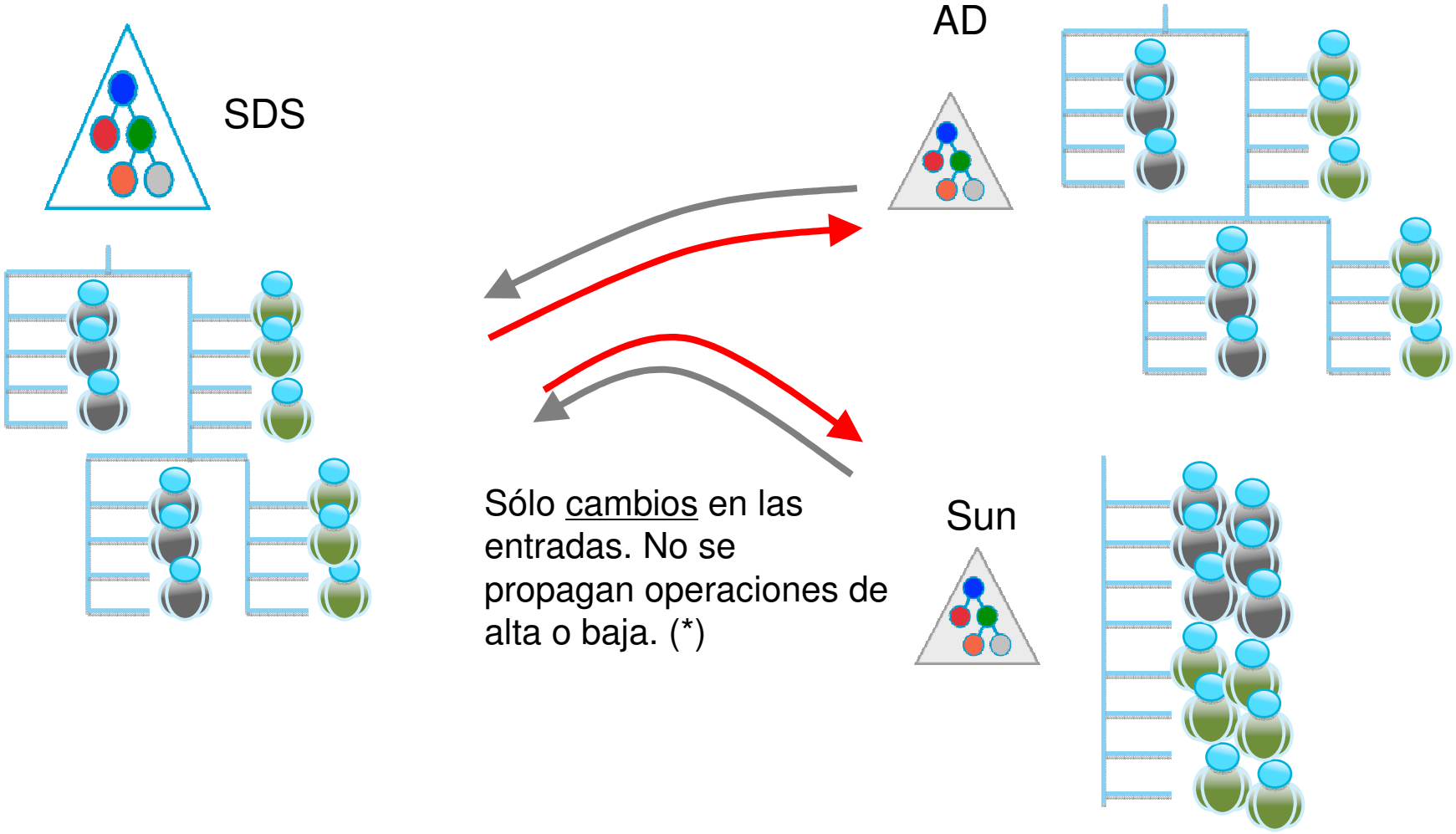




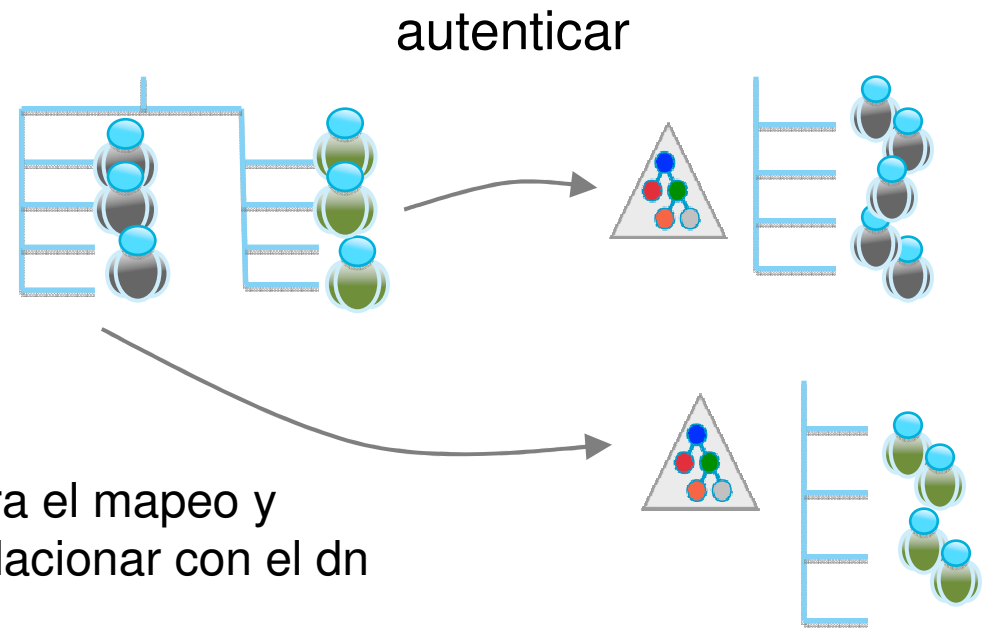


- Todas las relaciones pueden contener mapas y transformaciones de datos avanzadas.
- Incluye usuarios y grupos
- Las fuentes no se limitan a directorios

Escritura selectiva de los cambios desde SDS a las fuentes originales



Autenticación Pass-through (PTA)

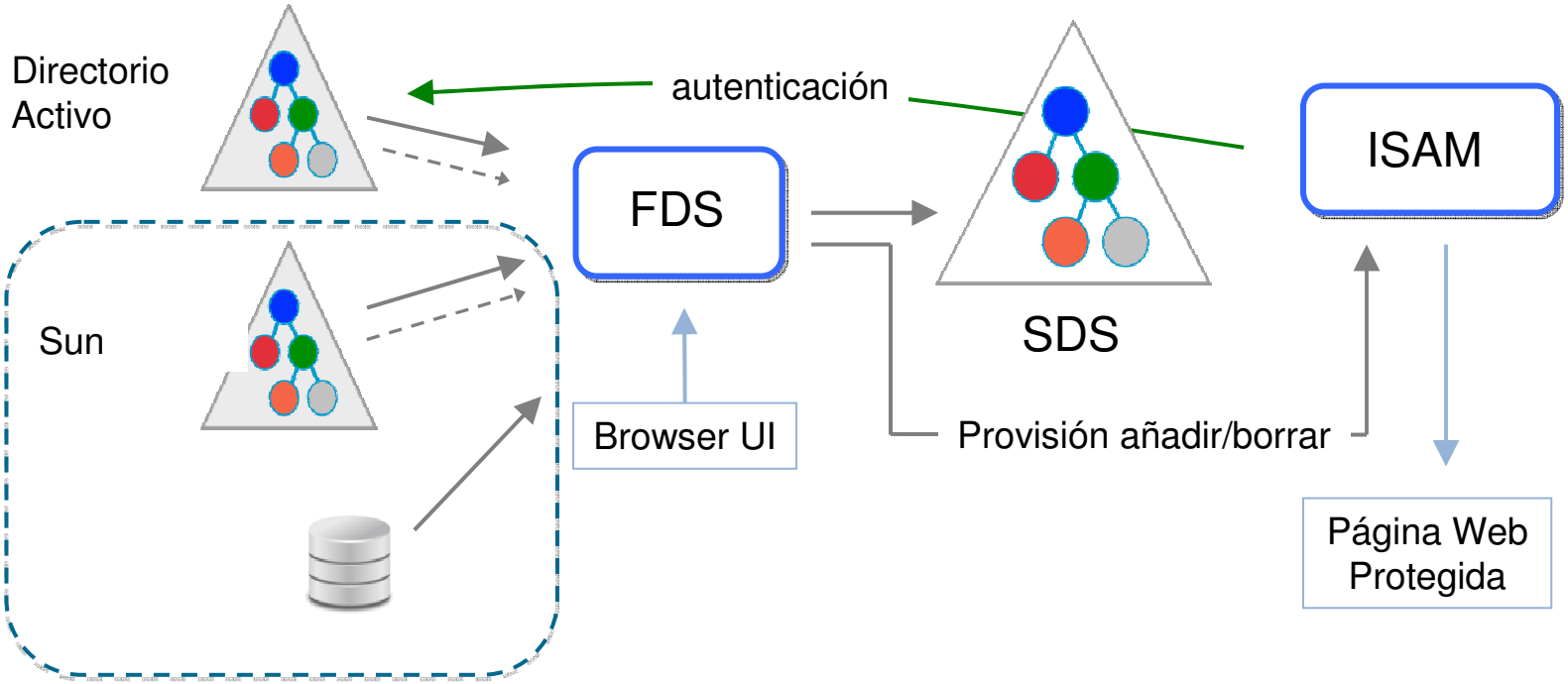


- Se define al nivel de contenedor de SDS donde serán autenticados los usuarios.

- Se dispone de diversas opciones para el mapeo y cualquier atributo en SDS se puede relacionar con el dn para la autenticación (bind).

- Se elimina la necesidad de almacenar contraseñas en SDS y la problemática de la sincronización.

Ejemplo de uso ISAM + FDS



ISAM utiliza SDS como repositorio , pero la autenticación tiene lugar en realidad en AD
FDS consolida la información del usuario en AD, Sun y tablas SQL en SDS para el perfilado en ISAM
FDS realiza operaciones adicionales en ISAM para cada operación de alta o baja (mediante una línea de ensamblaje “post operación” que utiliza el conector ISAM para llamar a la API ISAM).

Las líneas de puntos indican que el escenario podía ser mas simple , para un usuario que , por ejemplo, no desea que se modifique se Directorio Activo. Con FDS se puede desplegar ISAM, mantener AD sin modificaciones y mantener la administración original en AD

Prevenir las amenazas internas y el fraude asociado a la identidad

- Gestionar las cuentas privilegiadas y compartidas de la empresa
- Defender las aplicaciones frente a ataques y vulnerabilidades especificas

Privileged Identity Manager

IBM Security Privileged Identity Manager

- Elimina la necesidad de compartir contraseñas para usuarios privilegiados y cuentas compartidas mediante una gestión automatizada de identidades privilegiadas.
- Proporciona soporte a los procesos de conformidad y auditoria mediante la grabación de sesión.
- Soporta la integración con la autenticación fuerte y proporciona SSO para el acceso a las cuentas de alto riesgo.
- Reducción del TCO y el “time to value” mediante el factor de forma Appliance Virtual que acelera el despliegue de la solución.

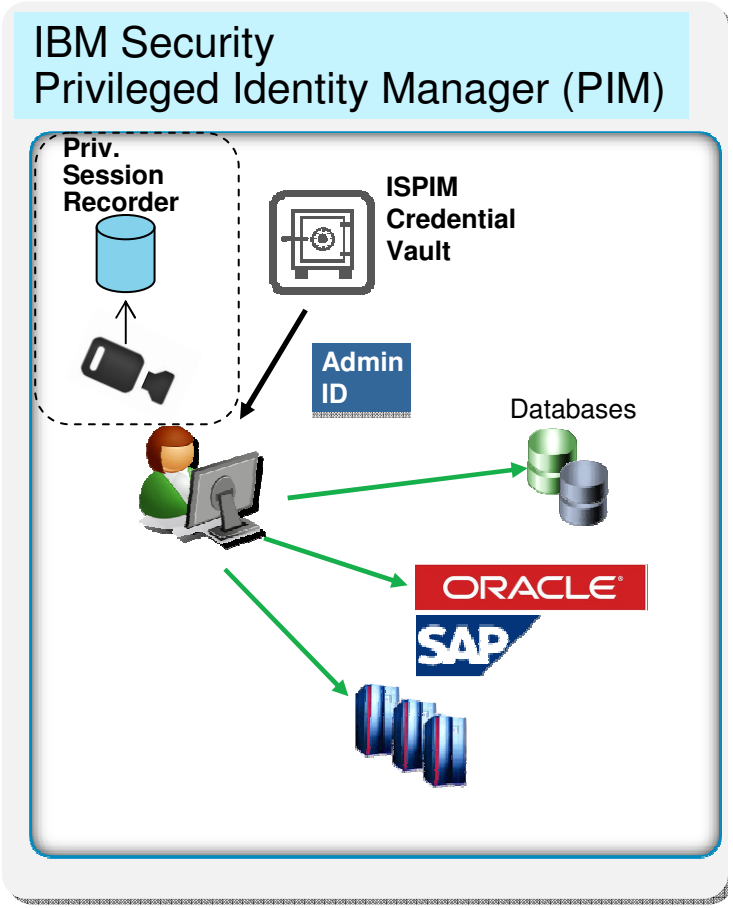
ISPIM Capacidades Actuales

ISPIM 1.0 final 2012

- **Controlar los accesos compartidos a uids sensibles**
  - Check-in / check-out , manual y automático basado en vault de credenciales
- **Solicitar, aprobar y revalidar accesos privilegiados**
- **Seguimiento del uso de las identidades compartidas**
- **Automatización de la gestión de contraseñas**

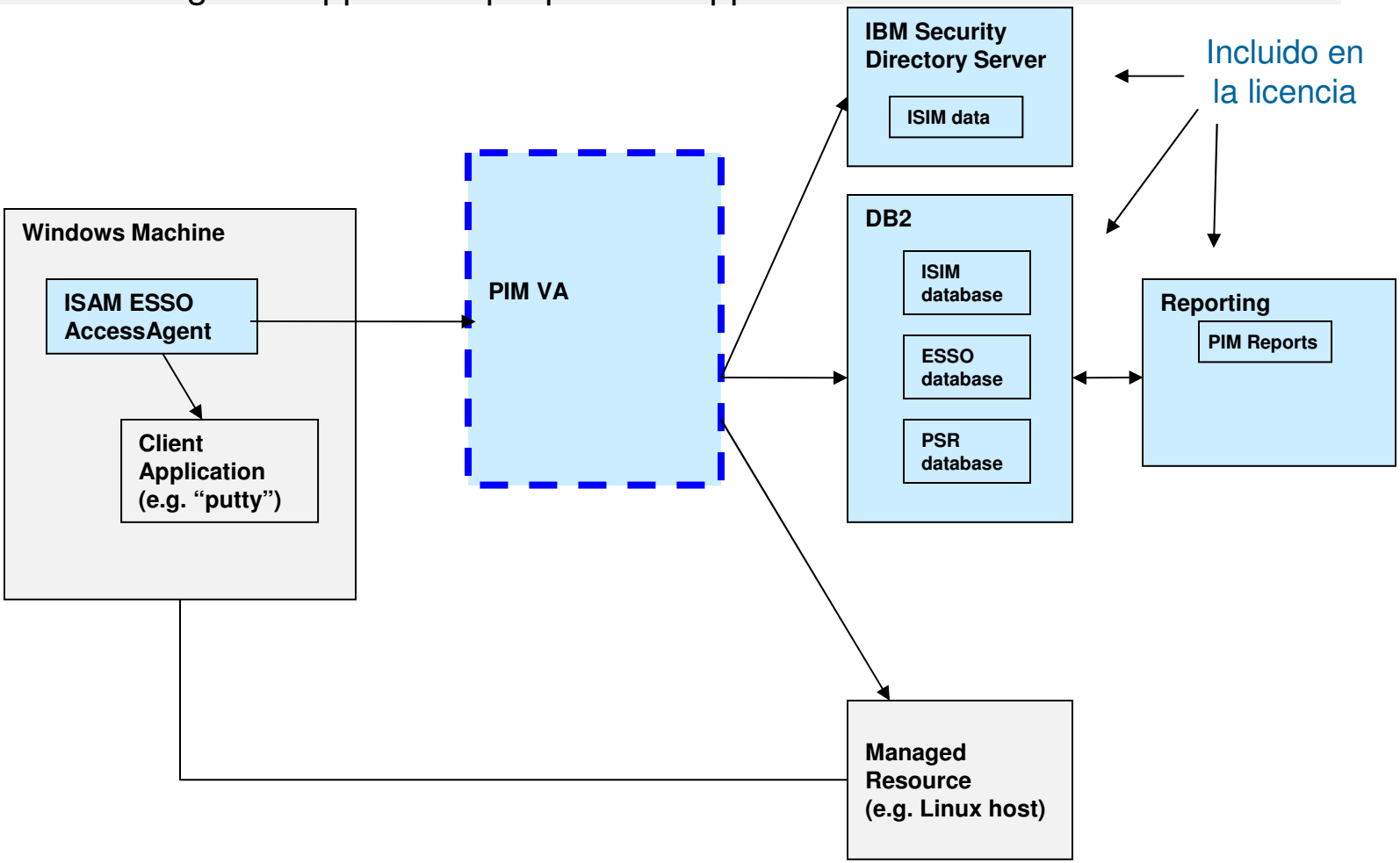
ISPIM 1.0.1 final 2013

- **Virtual Appliance**
  - Simplificación del despliegue y mejora del “time to value”
- **Grabación de sesión**
  - Capacidad de registrar, reproducir y realizar búsquedas en las sesiones establecidas con PIM
- **UI simplificada para administradores de IDs privilegiados**
  - Más facilidad de administración
- **Simplificación de la carga de usuarios**
  - Simplificación del despliegue y mejora del “time to value”
- **Soporte de Citrix XenApp**
  - PIM para escritorios no Windows



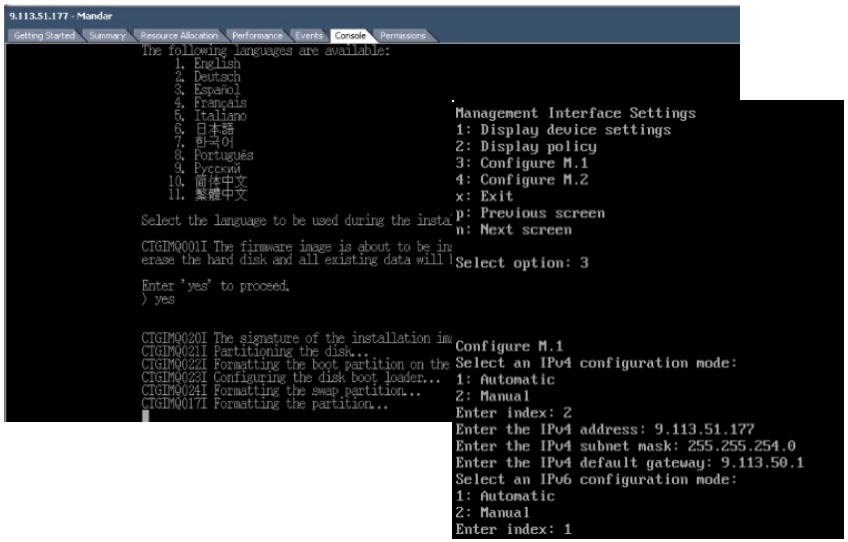
Arquitectura para el despliegue de PIM Virtual Appliance

- Rápido de desplegar y fácil de mantener
- Se requiere la capa de datos externa (DB2 and LDAP) (TDS, DB2 incluido en la licencia pero no en la imagen)
- Misma tecnología de appliance que para los appliances Web GW ó los IPSs

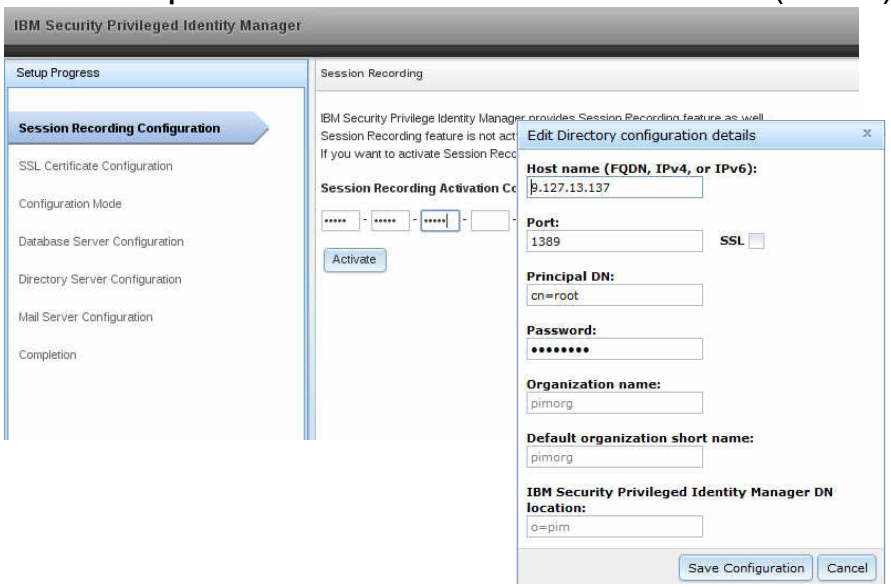


PIM 1.0.1 VA: Despliegue y configuración rápida

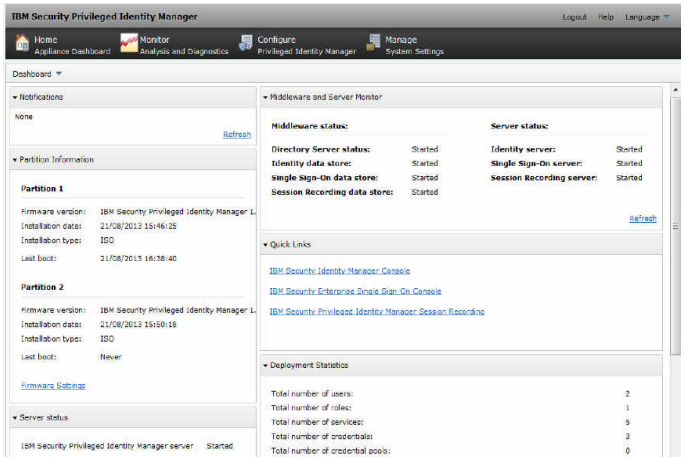
1. Instalación en una nueva VM en ESXi



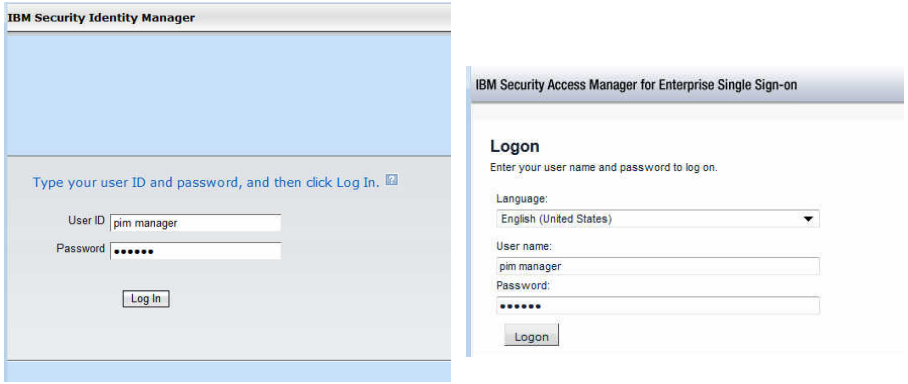
2. Primeros pasos de conf via consola Web (“JMI”)



3. Configuración y monitorización de VA

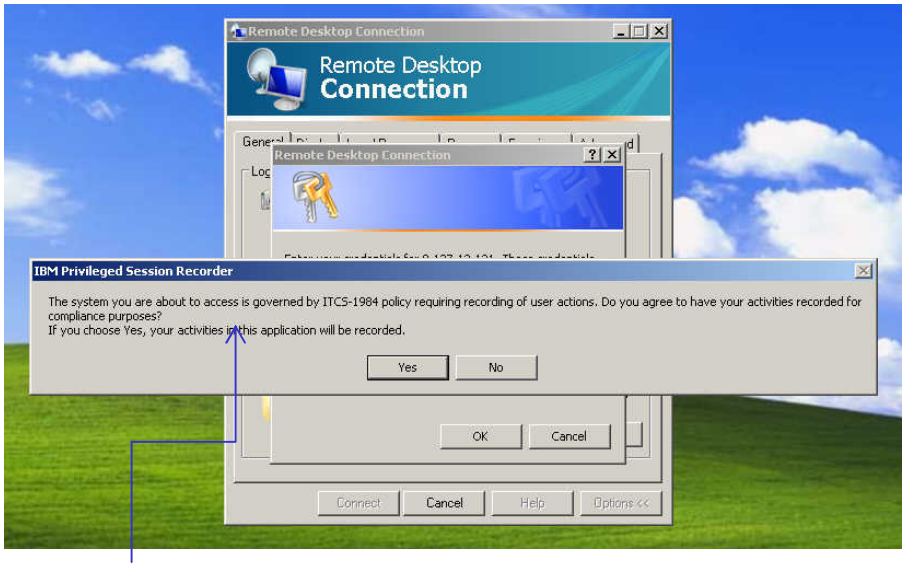


4. PIM listo para administración y carga de usuarios y credenciales



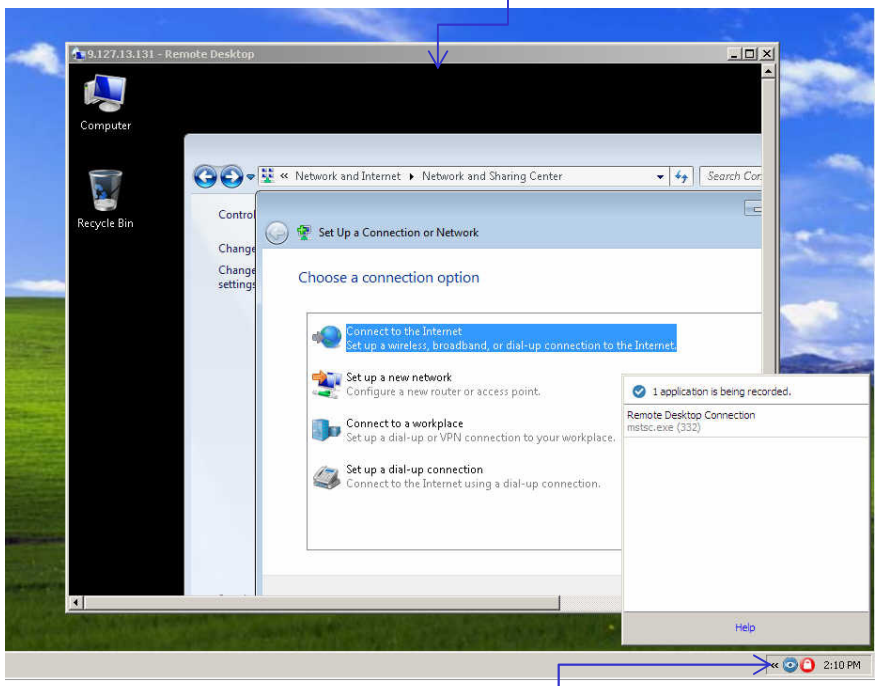
PIM 1.0.1: Privileged Session Recorder

- Disponible cuando se inicia la sesión mediante el cliente SSO
- Graba solo la sesión privilegiada, respetando el resto de la actividad del usuario por cuestiones de privacidad



Pompt configurable – anterior al checkout del ID, antes de iniciar la sesión- Si respondes “NO” no se inicia la sesión. Cumple una función legal y disuasoria

Logon automático a la sesión con ID de PIM

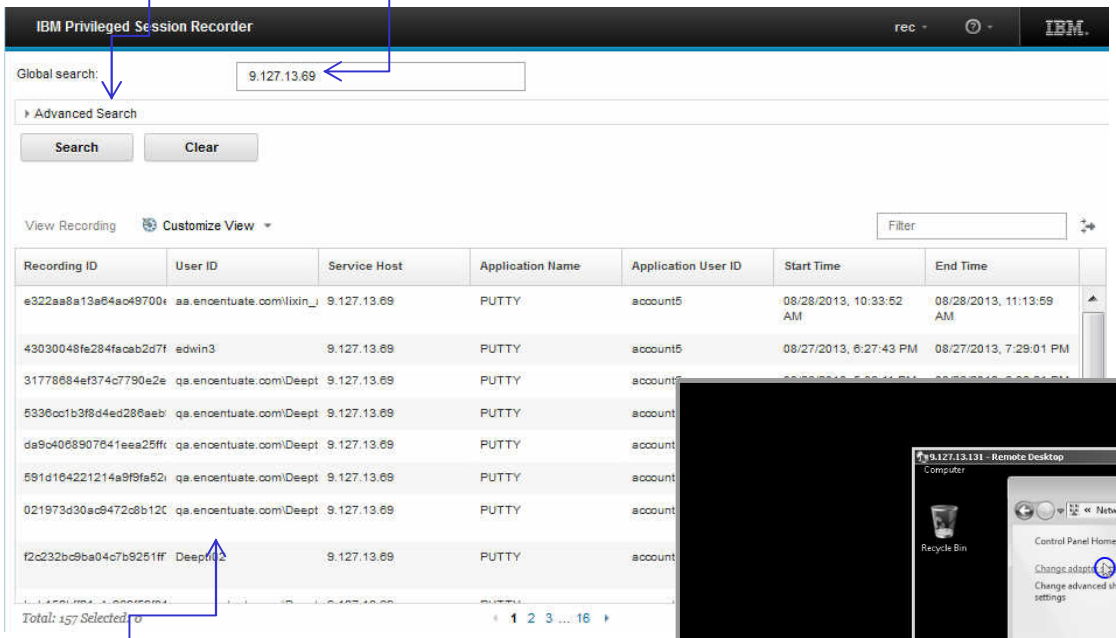


Icono del PSR en la bandeja del escritorio Win. Informa al usuario de las sesiones que están siendo grabadas

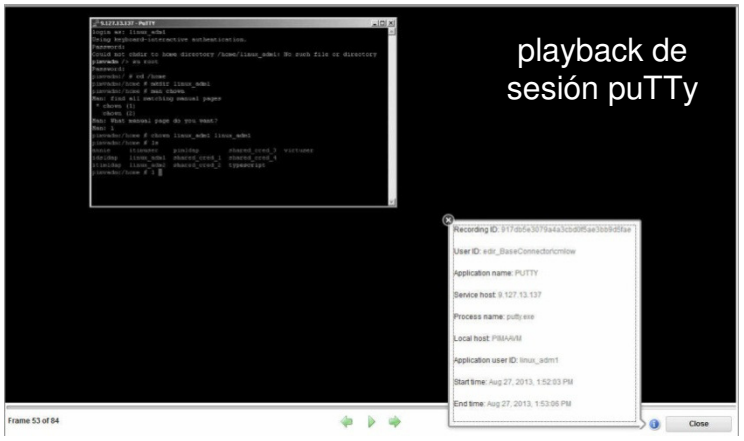
PIM 1.0.1: Privileged Session Recorder Reproducción

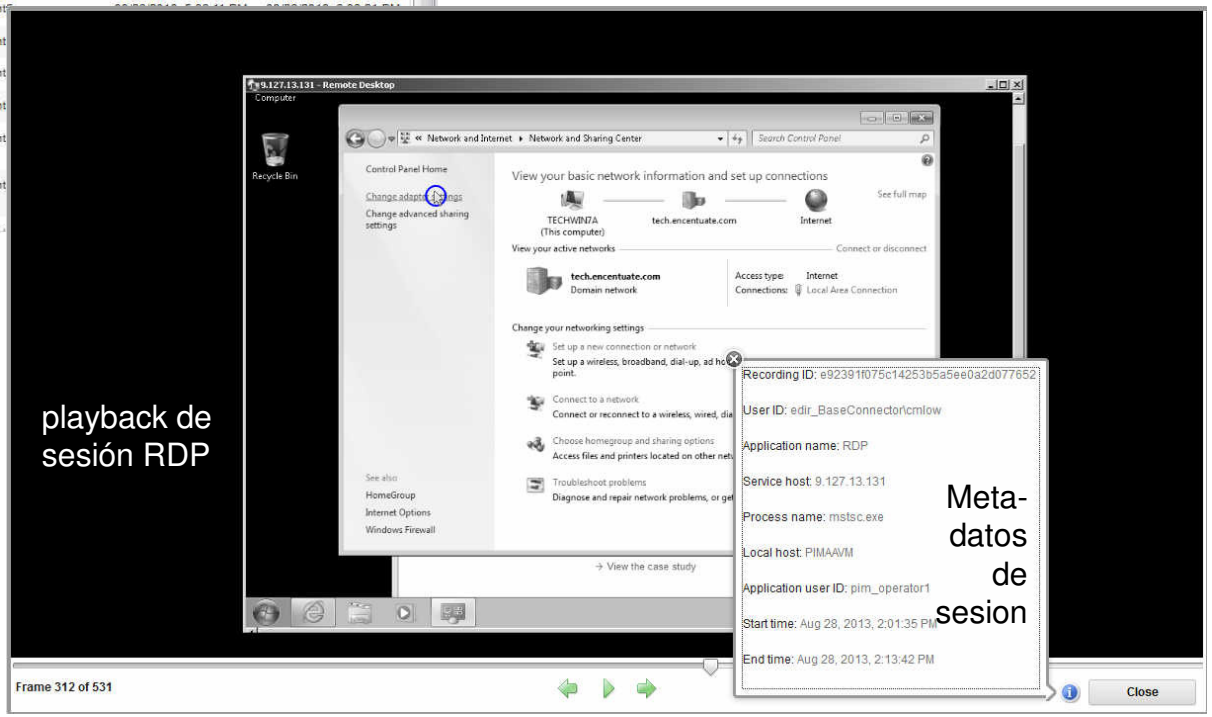
Búsqueda avanzada

Búsqueda rápida



Resultados de la búsqueda - lista de sesiones

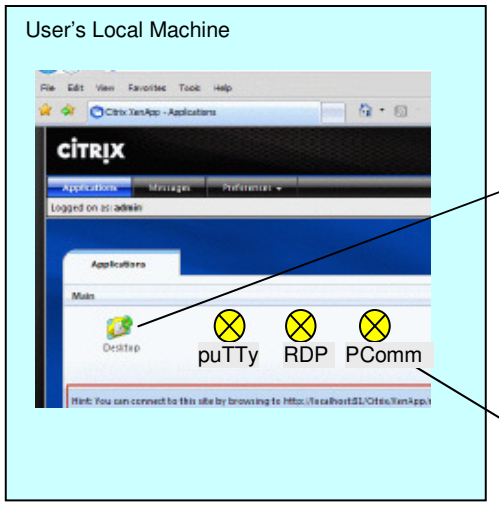




Imágenes grabadas en B&N o color

Experiencia de usuario PIM con Citrix XenApp

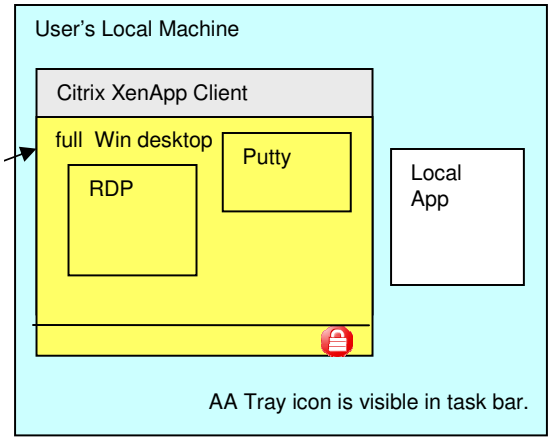
Paso 1. Logon a la interface Citrix Web Interface, lanzar una aplicación publicada o una sesión de escritorio.

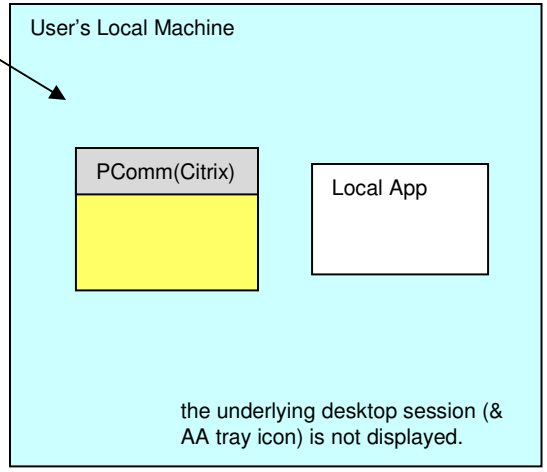


usuario lanza escritorio

Usuario lanza aplicación

Paso 2. El escritorio o la aplicación publicados se presentan en una ventana local. El usuario se loga en el sistema desde esa ventana.





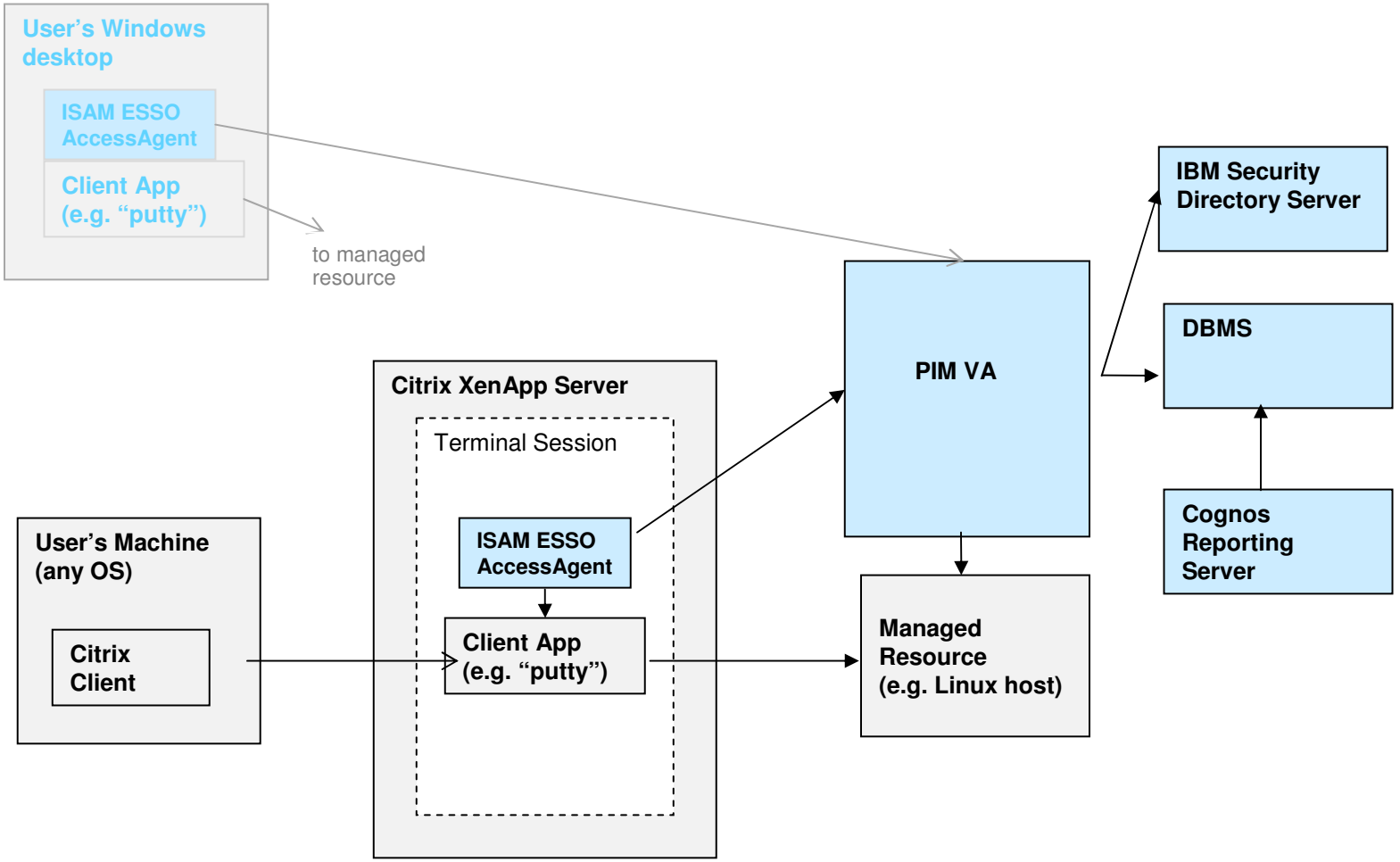
Auto-CICO & SSO Y Grabación de Sesión soportados

No se soporta CICO ni SSO ni Grabación de Sesión

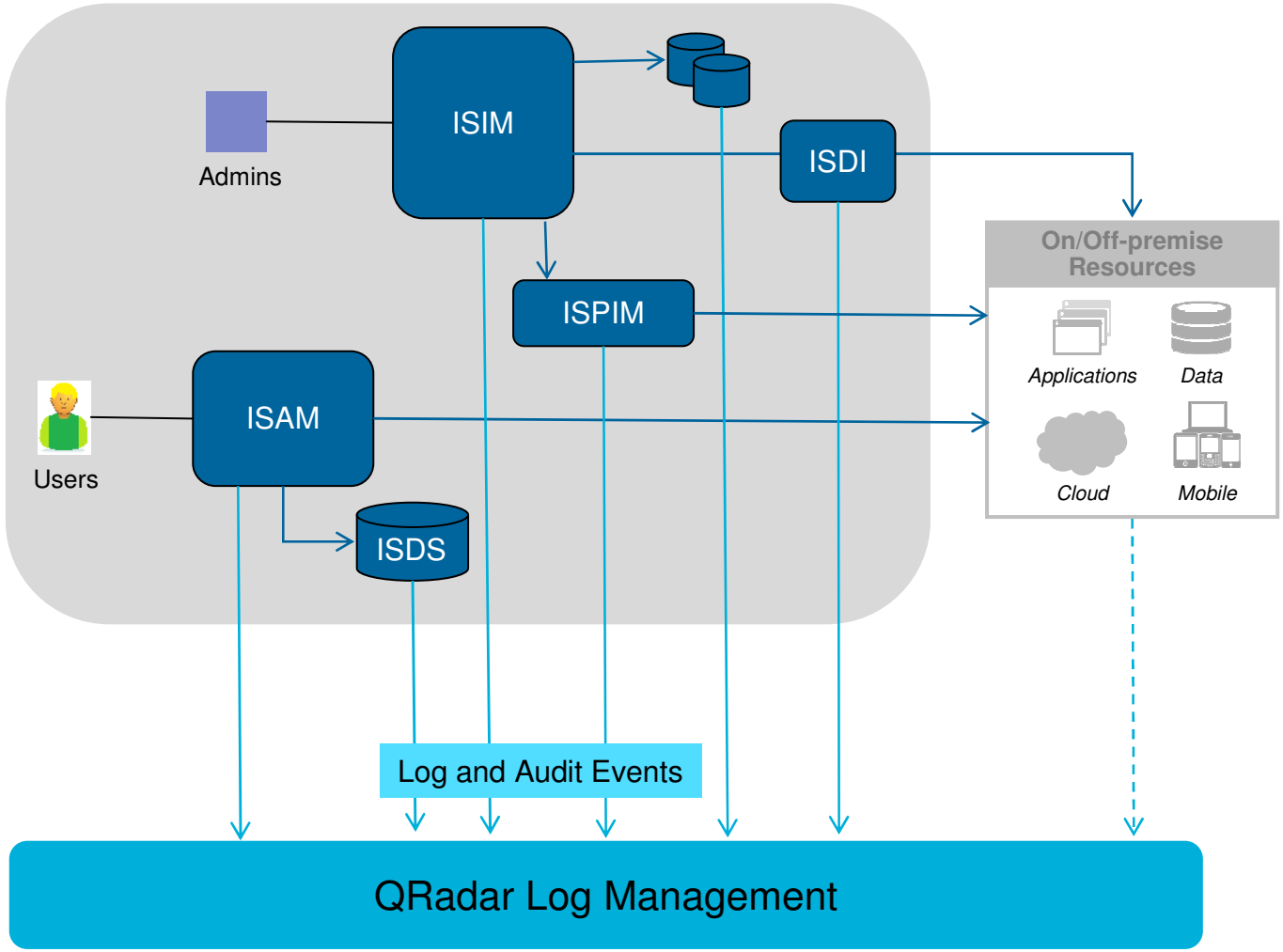
La máquina del usuario puede ser de cualquier OS (e.g. Linux, Windows, MacOS, iOS, Android) soportado para el cliente Citrix

PIM 1.0.1: Arquitectura con Citrix XenApp Server

Posibilita el soporte de escritorios no-Windows



Gestión de Logs IAM con QRadar



Ejemplo: Actividades Usuario/Sistema de un usuario privilegiado con PIM

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin

Search... ▼ | Quick Searches ▼ | Add Filter | Save Criteria | Save Results | Cancel | False Positive | Rules ▼ | Actions ▼ | Quick Filter...

Viewing real time events | View: Select An Option: | Display: Default (Normalized)

Using Search: PIM Activity Monitor

Current Filters:

Log Source Group is PIM (Clear Filter)

Event Name	Log Source	Even Coun	Tim	Low Level Category	Source IP	Sou Por	Destination IP	Des Por	
Authentication Authenticate SUCCESS	ISIM Server	4	2...	General Authentication Successful	9.127.13.178	0	9.127.13.178	0	linuxadmin
CredentialLeaseManagement Checkin S...	ISIM Server	1	2...	Information	9.127.13.178	0	9.127.13.178	0	linuxadmin
PIM_CHECK_IN	PIM IMS	1	2...	Privilege Escalation Succeeded	9.187.3.103	0	9.127.13.227	0	qa.encentuate.com\Deepti03
Successful PIM Logon	Custom Rule Engine...	1	2...	Host Login Succeeded	9.127.13.178	5...	9.127.13.69	0	root
Done with connection	Linux Server	1	2...	SSH Closed	9.127.13.178	10	9.127.13.69	0	N/A
PAM Session Closed	Linux Server	1	2...	Auth Server Session Closed	9.127.13.69	0	9.127.13.69	0	root
Root Login	Linux Server	1	2...	Admin Login Successful	9.127.13.178	5...	9.127.13.69	0	root
Session Started for user	Linux Server	1	2...	Session Opened	9.127.13.69	0	9.127.13.69	0	root
Password Changed	Linux Server	1	2...	Password Change Succeeded	9.127.13.69	0	9.127.13.69	0	account8
PAM Session Closed	Linux Server	1	2...	Auth Server Session Closed	9.127.13.69	0	9.127.13.69	0	account8
Authentication Authenticate SUCCESS	ISIM Server	19	2...	General Authentication Successful	9.127.13.178	0	9.127.13.178	0	linuxadmin
Successful PIM Logon	Custom Rule Engine...	1	2...	Host Login Succeeded	9.187.3.103	6...	9.127.13.69	0	account8
Accepted Password for User	Linux Server	1	2...	Host Login Succeeded	9.187.3.103	6...	9.127.13.69	0	account8
Session Started for user	Linux Server	1	2...	Session Opened	9.127.13.69	0	9.127.13.69	0	account8
PIM_CHECK_OUT	PIM IMS	1	2...	Privilege Escalation Succeeded	9.187.3.103	0	9.127.13.227	0	qa.encentuate.com\Deepti03

Proteger las interacciones en las redes sociales y los entornos móviles

- Validar "quien es quien" cuando los usuarios se conectan desde fuera de la red interna
- Posibilitar políticas proactivas de acceso a las redes sociales, entornos móviles y la nube

Security Access Manager V8

IBM Security Access Manager 8.0

Appliances “Todo-en-uno” con gestión de accesos motorizada por X-Force, integrada conTrusteer , QRadar y Worklight

- **Permitir accesos seguros a aplicaciones web y móviles** con SSO, gestión de sesión y soporte integrado de IBM Worklight
- **Protección de aplicaciones web y móviles** frente a los vectores de ataque más comunes, incluyendo la lista de los 10 mayores riesgos identificados por OWASP mediante la integración del PAM de X-Force
- **Control de acceso basado en el contexto** mediante identificación del dispositivo móvil, geo-localización, IP Reputation y la integración con Trusteer Mobile SDK
- **Mejora de la Inteligencia de Seguridad y la conformidad** mediante la integración con QRadar
- **Reducción del TCO y el “time to value”** con appliances “todo-en-uno" que permiten un despliegue flexible de las capacidades que se necesiten

ISAM V8 Diseño Modular

- Hardware Appliance:
  - Intel i7-2600 processor
  - 32GB memory
  - 6 network interfaces
  - 800GB solid state disk

- Virtual Appliance:
  - VMWare ESX/ESXi
  - Distribuido como un ISO instalable
  - Configuración HW Pre-definida, pero se puede variar la memoria y el número de CPUs

ACTIVAR **ACTIVAR**

LICENCIAR **LICENCIAR**

IBM Security Access Manager

ISAM for Web	ISAM for Mobile
Web Single Sign-On y gestión de sesión	Mobile Single Sign-On y gestión de sesión
Web Application Protection (Firewall)	Servicio de Autenticación con soporte de OTP incorporado
Highly-scalable Reverse Proxy	(RBA) Context-, Risk-based Access
Policy Server	Integración de Trusteer Mobile SDK / Secure Browser
Autorización de “grano grueso”	Integración con Worklight para acceso basado en el riesgo

Appliances físicos por rendimiento y seguridad

Appliances virtuales por flexibilidad en el despliegue

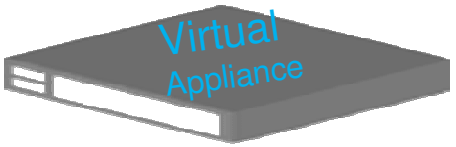
ISAM V8 Licenciamiento

Appliances fisicos:

- Coste unitario, sin restricción respecto al número de usuarios

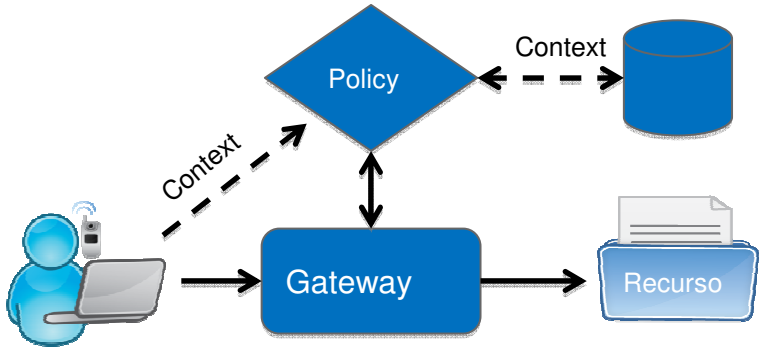
Appliances virtuales:

- Licenciamiento por Processor Value Units (PVUs)
  - ISAM for Web
  - ISAM for Mobile
- Licenciamiento por User Value Unit (UVUs)
  - ISAM for Web



- Licenciamiento de una appliance “combinado”
  - Se deben licenciar las dos opciones: ISAM for Web and ISAM for Mobile
  - Una de estas dos opciones:
    - Licenciamiento por PVU para los dos productos
    - Licenciamiento por PVU para ISAM for Mobile y por UVU para ISAM for Web

Escenarios ISAM



ISAM for Web

Web Single Sign-On y gestión de sesión
Web Application Protection (Firewall)
Reverse Proxy , Balanceador

ISAM for Mobile

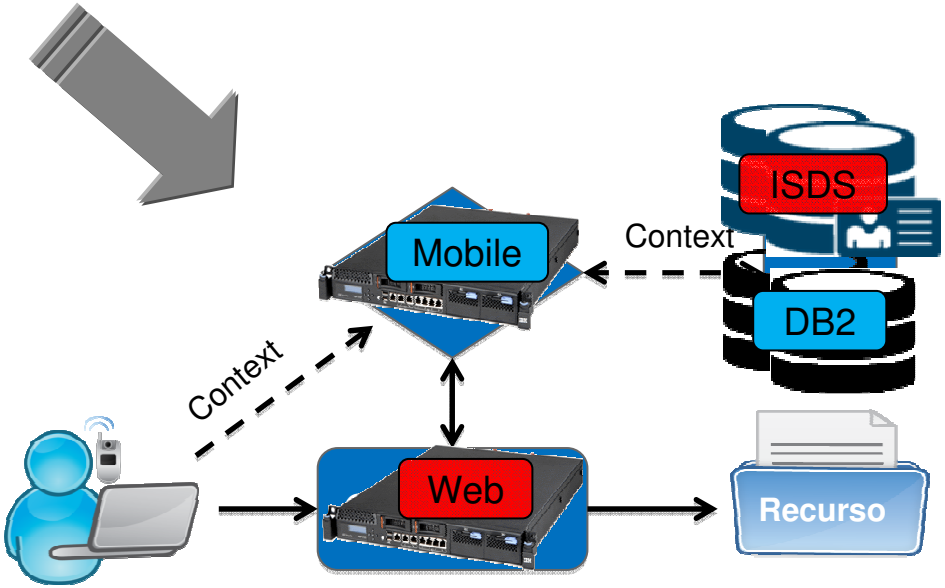
Servicio de Autenticación con soporte de OTP incorporado

(RBA) Context-Risk-based Access

Integración de Trusteer Mobile SDK / Secure Browser

Integración con Worklight para acceso basado en el riesgo

Oauth 2.0 server



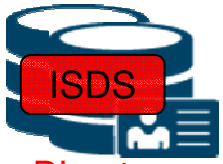
Ejemplo: Context Based Access Control + Web Application Firewall

Arquitectura de producción – mezcla de appliances físicos y virtuales

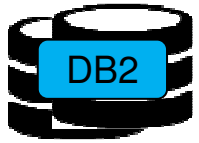
Untrusted zone

Load Balancer
Content Protection
Reverse Proxy

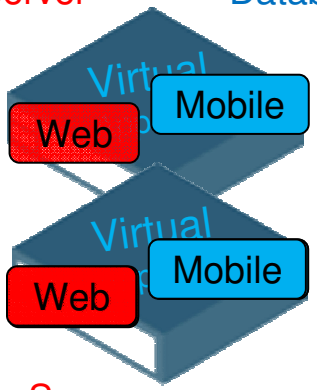
DMZ



Directory Server



Runtime Database



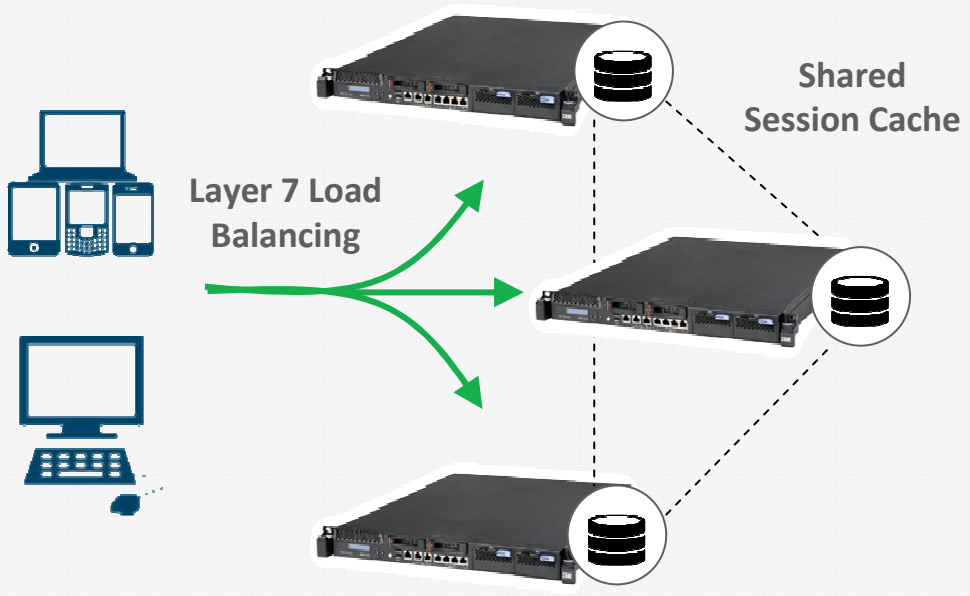
Policy Server
Distributed Session Cache
Authentication Services
Context/Risk Based Access
OAuth Authorisation Server

Application zone

ISAM for Web - Novedades

Rol de Balanceador de Carga Layer 4 y 7. Caché de sesiones compartida

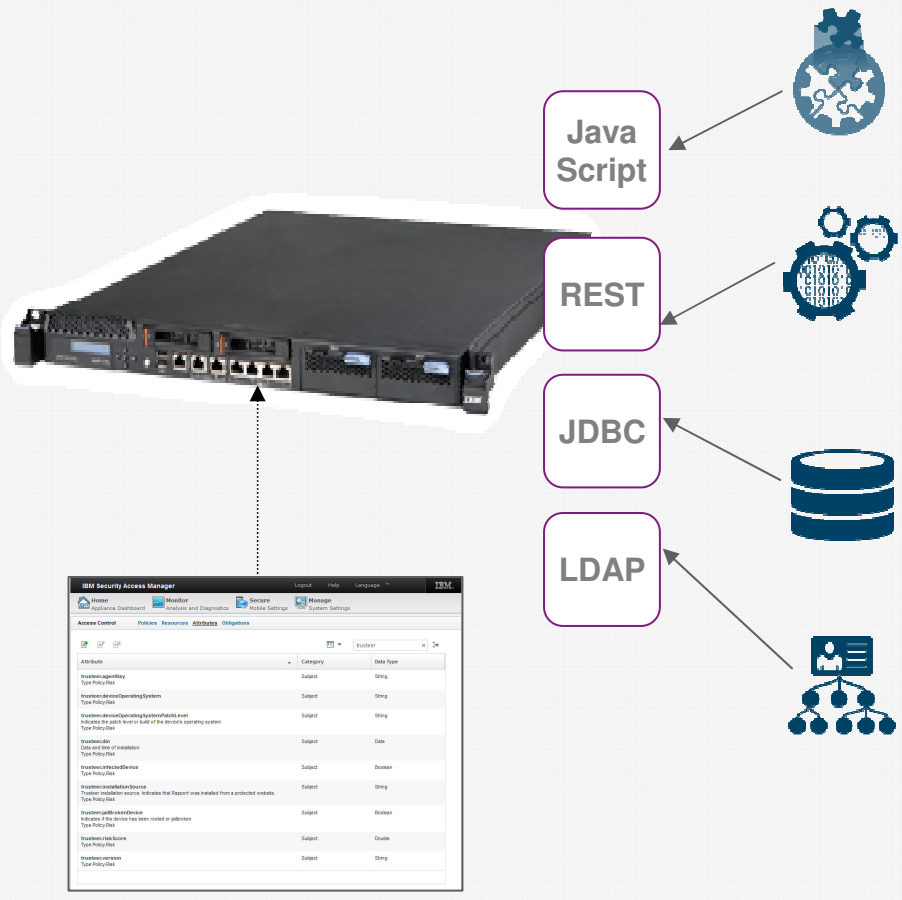
- Soporte de Layer 7 en la función de balanceador de carga (ahora soporta layer 4 y 7) lo cual permite implementar arquitecturas completas de HA para ISAM con el appliance físico
- Caché de sesiones embebida y compartida, no son necesarios servidores SMS (Session Management Server) => arquitecturas más simples y con menor coste
- Prueba y validación mejorada de las políticas de protección web en el modo de simulación del PAM (Protocol Analysis Module) de X-Force



ISAM for Mobile - Novedades

Implementación y despliegue rápido de políticas de acceso/autenticación complejas

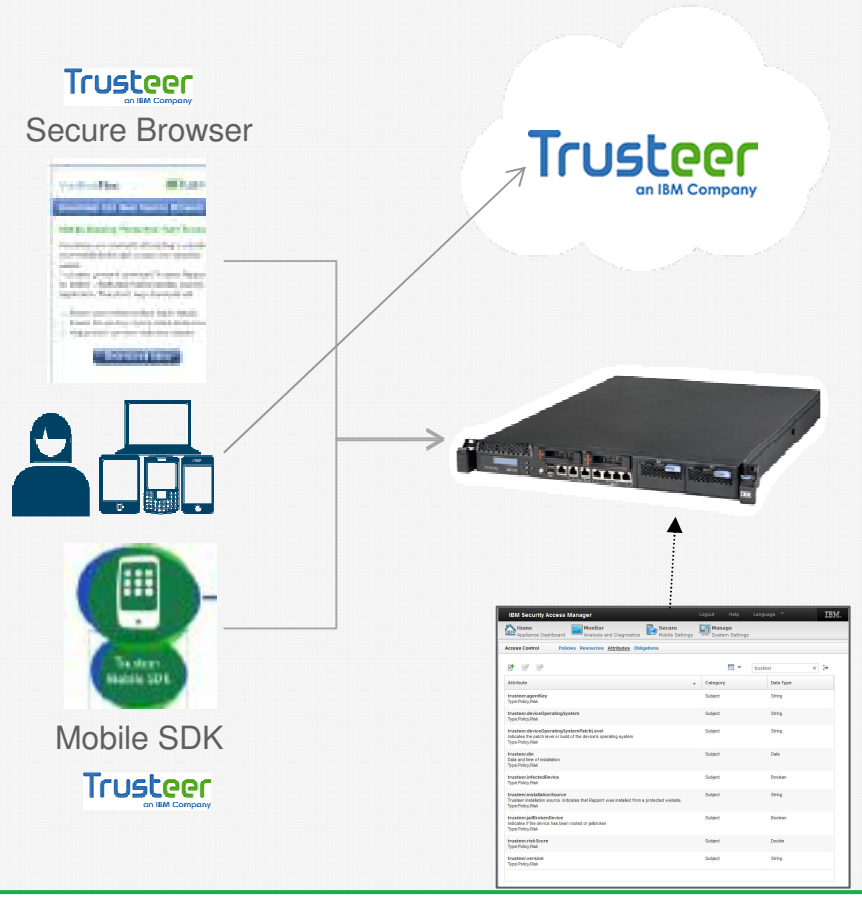
- ISAM for Mobile ofrece un nuevo editor visual fácil de usar, para la creación de políticas de autenticación multi-factor reutilizables
  - Políticas Out of the box MFA incluyendo TOTP, HOTP, etc.
  - Creación de políticas de autenticación custom
- Policy information points (PIPs) extensibles para facilitar la inclusión de datos externos como parte del contexto, para las decisiones basadas en el mismo
  - REST (XML/JSON)
  - JavaScript
  - JDBC and LDAP



ISAM for Mobile - Novedades

Detección de fraude y malware mediante la integración con Trusteer. Aplicación de políticas basadas en el contexto proporcionado por Trusteer sin necesidad de actualizar el código

- Reconocimiento Out-of-the-box de los atributos específicos que incluye Trusteer Secure Browser y Mobile SDK en las peticiones
  - Atributos del dispositivo
  - Malware
  - …
- Políticas reutilizables que pueden ser aplicadas a múltiples aplicaciones
- Imponen políticas consistentes de detección de fraude y malware sin necesidad de actualizar las aplicaciones



ISAM for Mobile

Inteligencia de seguridad en entornos móviles con la integración Out of the Box con QRadar

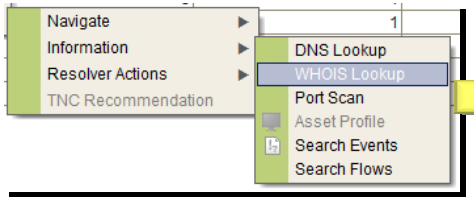
Perdida potencial de datos
Quién? Qué? Dónde?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.1[illegible].139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

Quién?
Un usuario interno

Qué?
Datos en Oracle



QRadar Has Completed Your Request

Go to APNIC results

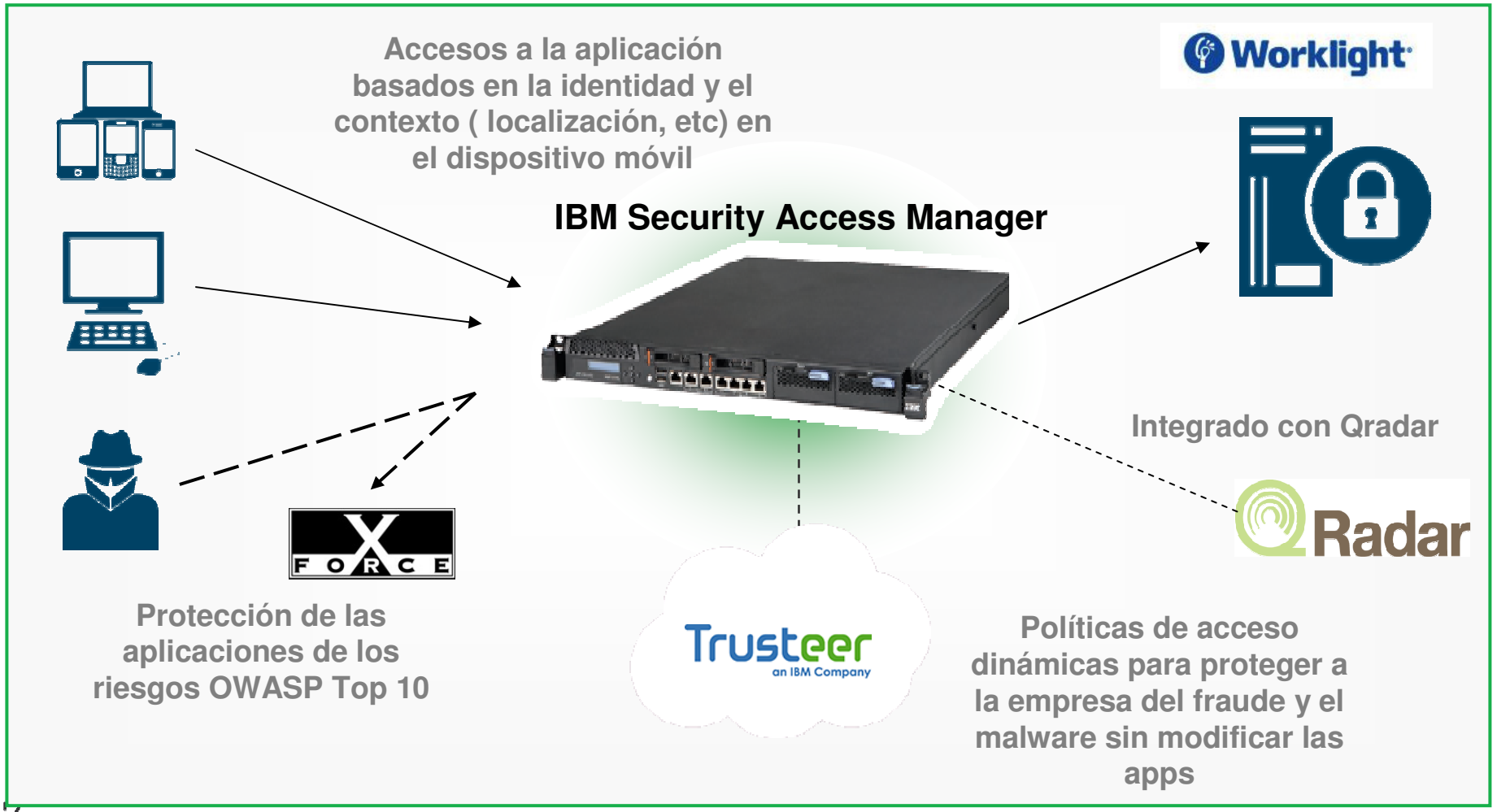
[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL

Dónde?
Gmail

Seguridad para los entornos móviles

Imposición de políticas centralizada y consistente para Acceso basado en el contexto/riesgo, protección frente a amenazas, detección de fraude y malware



Gobernanza de identidades e inteligencia en los accesos

- Posibilitar la gestión de identidades a la Línea de Negocio
- Mejorar la monitorización de la actividad del usuario y la inteligencia en la seguridad los dominios de seguridad

Security Identity Manager V6.0.0.2

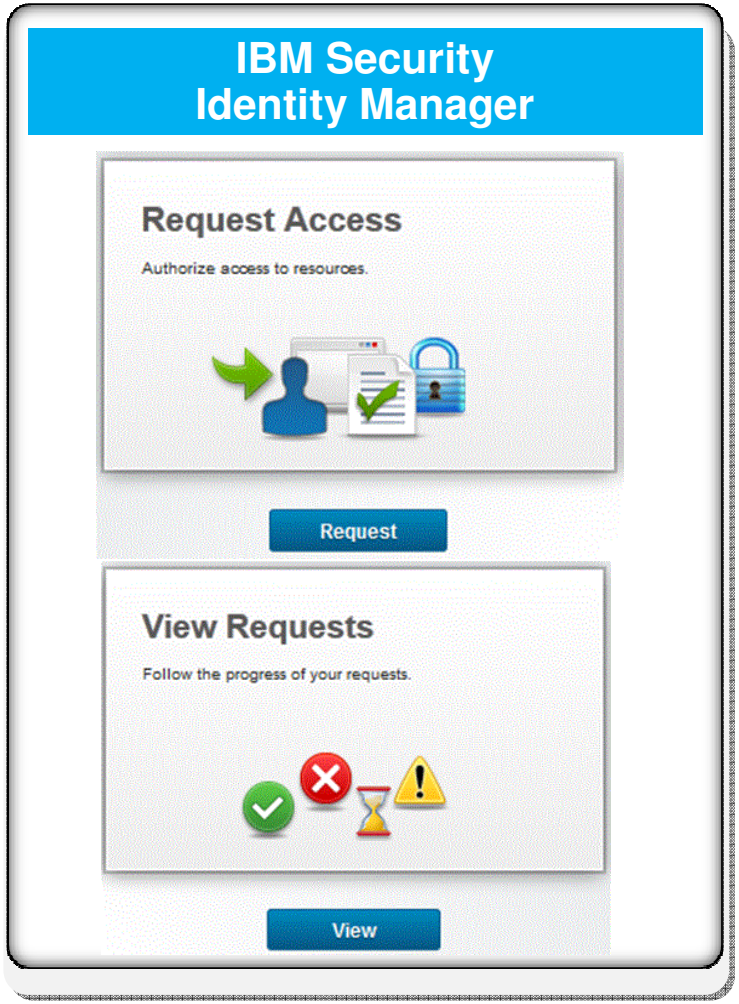
IBM Security Identity Manager v6.0.0.1

Principal novedad de la versión

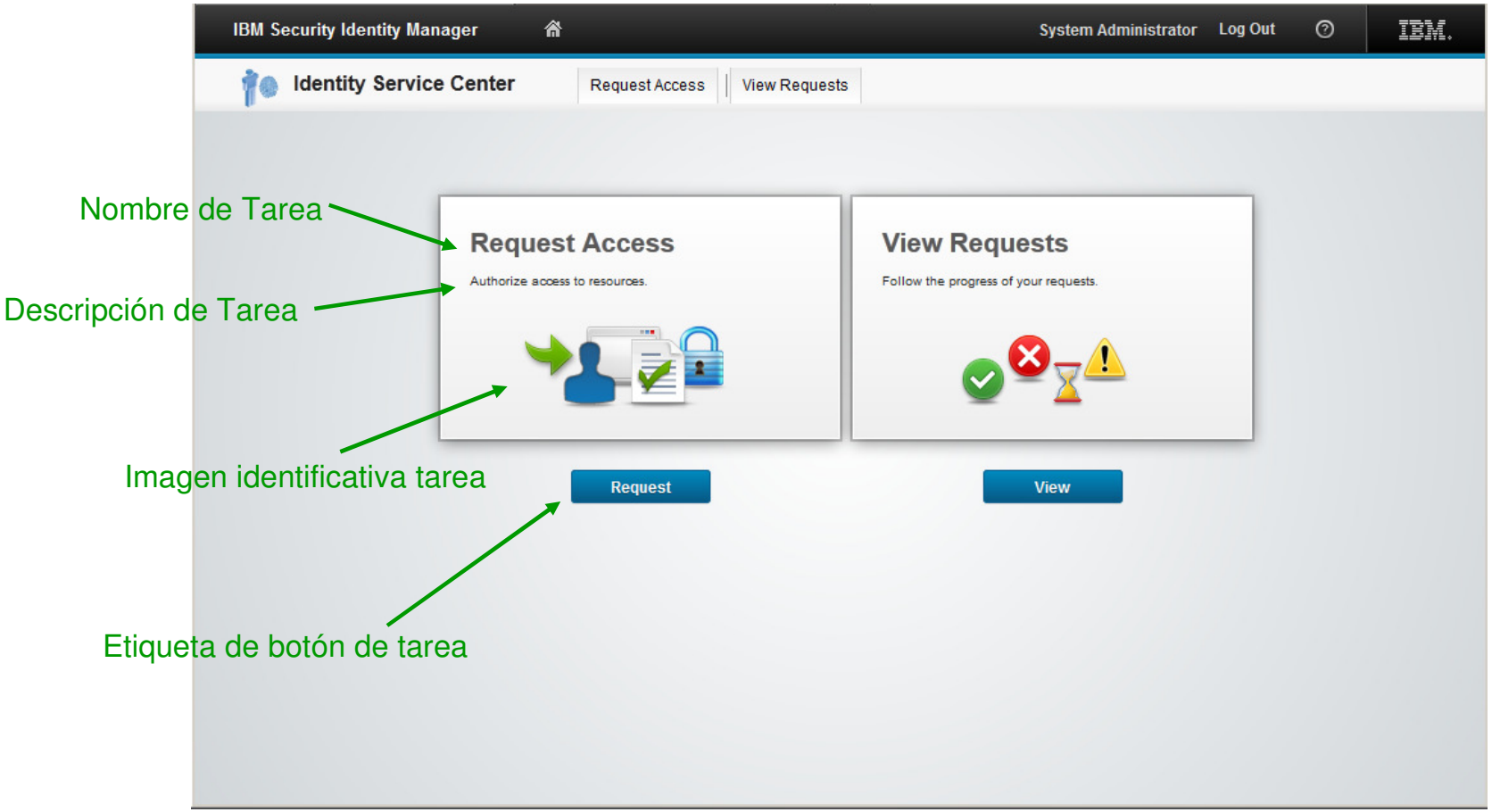
- Nueva interface Identity Service Center (Fase 1)
  - Orientada a managers inicialmente
- Soporta la petición de accesos y la consulta del status de la petición
  - Basado en los últimos paradigmas desde el punto de vista de eficiencia: carro de la compra, anticipación de escritura , etc
  - Tareas intuitivas y guiadas

Otras novedades

- Actualizaciones de adaptadores o ISIM Adapters
  - MS Office365 adapter , MS Active Directory
  - Lotus Notes, RSA Authentication Manager
  - BMC Remedy AR System
  - MS SQL Server, Oracle eBusiness Suite
  - UNIX, Linux, ISAM (ISAM Combo)
- Soporte de nuevo middleware
  - WAS 8.5, DB2 10.1



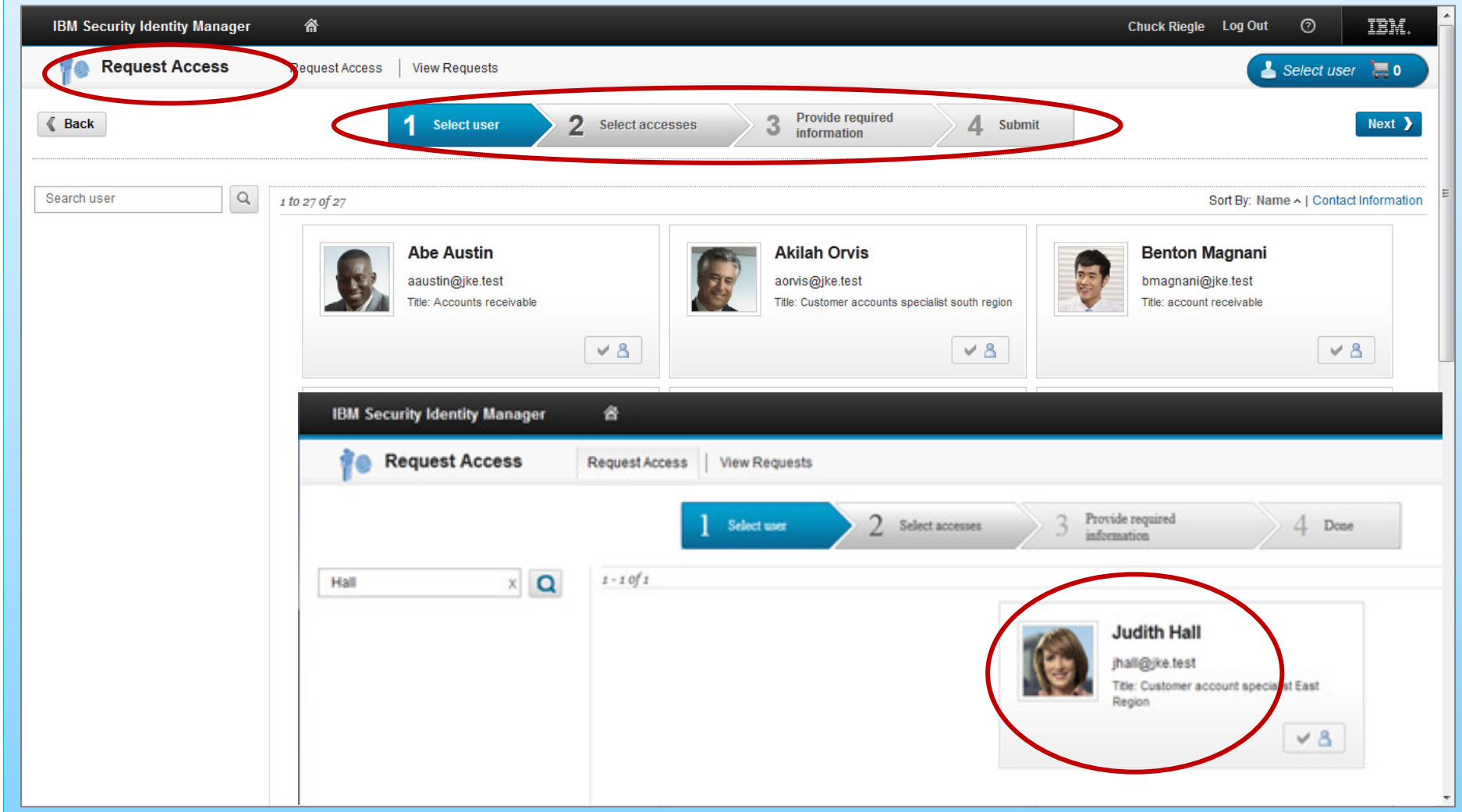
ISIM Service center



- ISIM Service center está organizado en Tareas
- Es posible incluir tareas customizadas
- Las tareas standar son altamente customizables

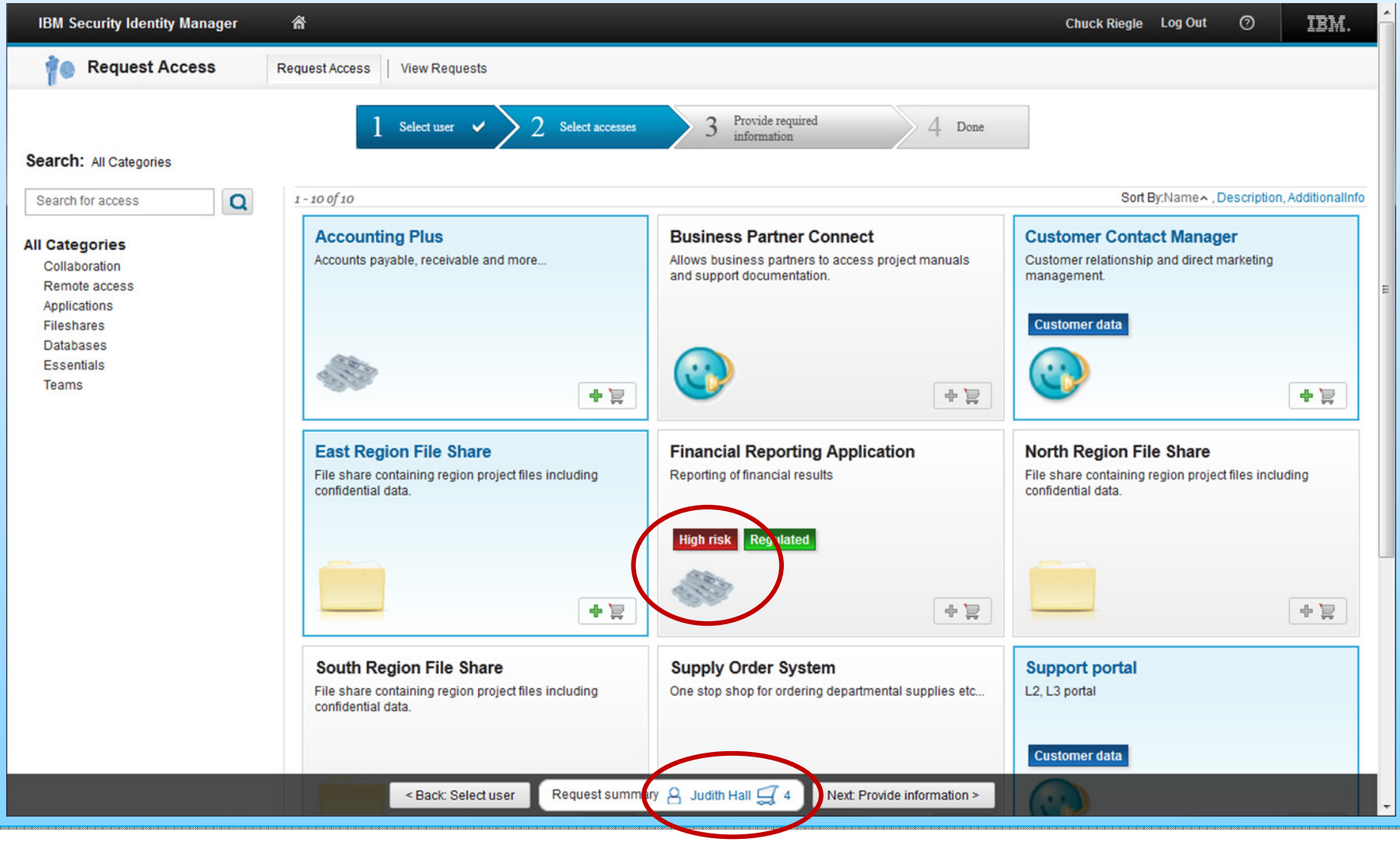
ISIM Service Center

Una vez en la tarea, se guía la actividad en distintas operaciones



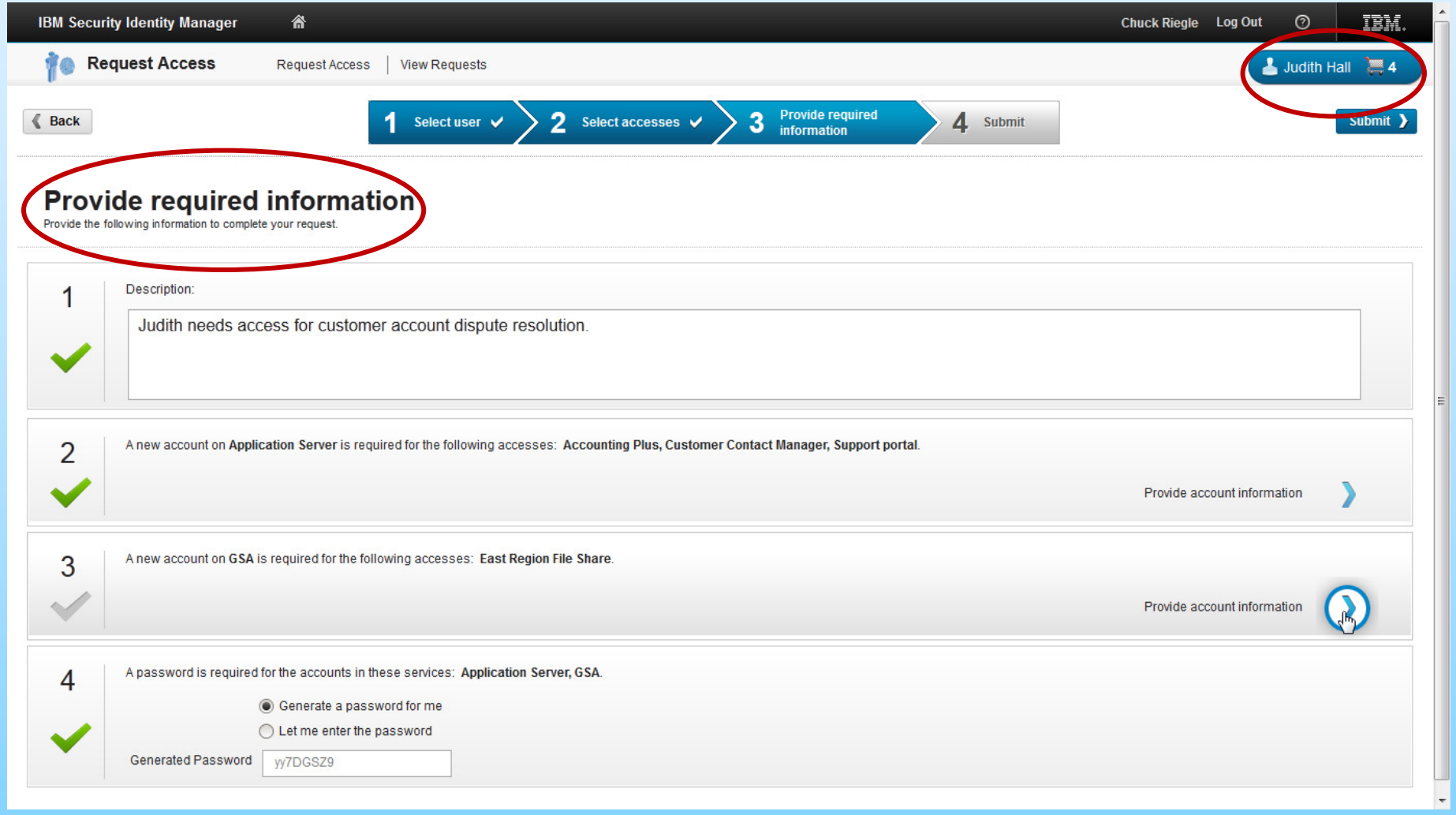
ISIM Service Center

El proceso de selección en cada operación es similar a una experiencia de compra



Identity Service Center

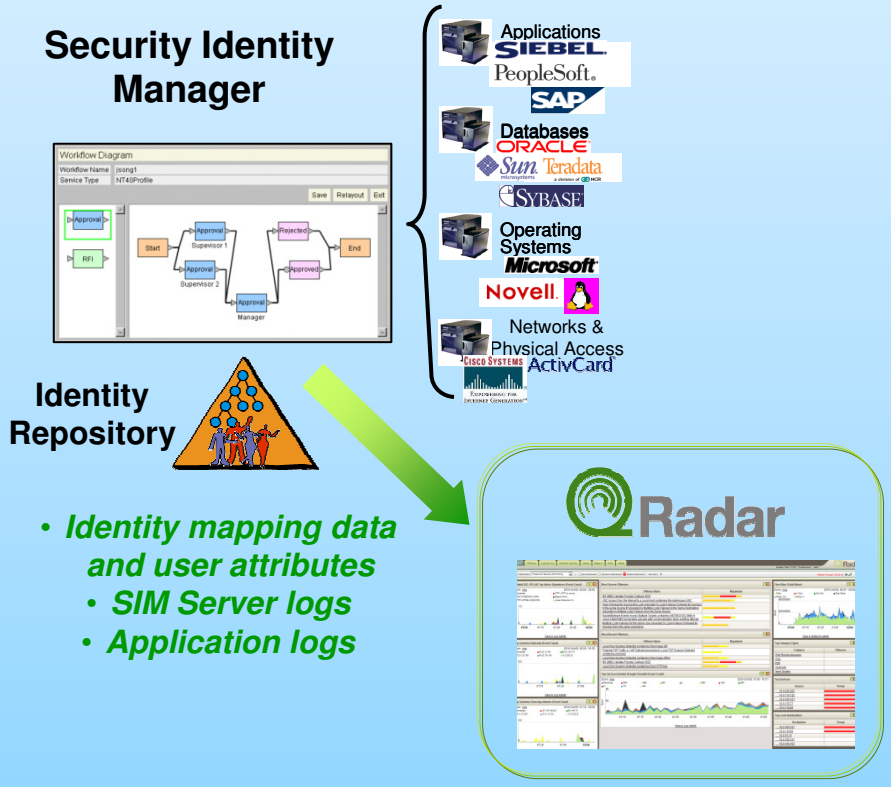
Información consolidada pero específica para cada item (acceso solicitado) información disponible en el carrito



ISIM 6.0 Mobile Identity Management en tu móvil

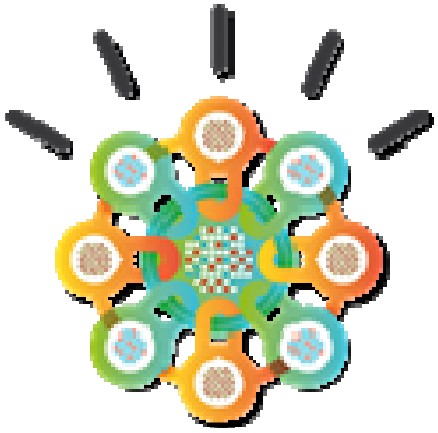
- App/interface para Android e iPhone
- Permite a managers/aprobadores revisar y aprobar peticiones de los empleados y ver la historia y el status
- Soporta cambio de contraseña y reset de contraseña olvidada
- Soporte de autenticación OAuth para aplicaciones Android e iOS

ISIM integración con QRadar



Inteligencia de seguridad enriquecida con datos de identidad:

- QRadar Device Support Module para Identity Manager
  - Reporte centralizado en QRadar de las actividades de los administradores de ISIM
- Colección de atributos de identidad del registro ISIM. Uso de los datos de identidad en conjunción con eventos de log y datos de network flows en reglas para aportar contexto de identidad a la inteligencia en seguridad
  - Mapear identidades y grupos en ISIM con actividades en aplicaciones monitorizadas con QRadar.
  - Generación de informes para asistir en la recertificación o diseño de roles
- (futuro próximo) Mapeo de UIDs: múltiples uids mapeados a un único ID, ie: pmartin y pedro.martin porque son la misma persona para una correlación completa



¿PREGUNTAS?

Gracias