ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

PROYECTO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA

TEMA:

"ESTUDIO E IMPLEMENTCION DEL SOFTWARE INFOSPHERE GUARDIUM V9.1 PARA LA PROTECCION DE LA BASE DE DATOS KDBS_SINERGY"

AUTOR: JIMMY FABIAN LUDEÑA CARRION

DIRECTOR: DR. NIKOLAI ESPINOSA.

CODIRECTOR: ING. CRISTIAN VEGA.

SANGOLQUÍ

2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

CERTIFICADO

Dr. Nikolay Espinosa.

Ing. Cristian Vega.

CERTIFICAN

Que el presente Proyecto de grado titulado: "ESTUDIO E IMPLEMENTACION DEL SOFTWARE INFOSPHERE GUARDIUM V9.1 PARA LA PROTECCIÓN DE LA BASE DE DATOS KDBS_SINERGY", desarrollado en su totalidad por el señor JIMMY FABIAN LUDEÑA CARRIÓN, con CI: 0703532242, ha sido guiado y revisado periódicamente bajo nuestra dirección, cumpliendo con las normas estatuarias establecidas en el Reglamento de Estudiantes de la ESPE.

Sangolquí, 20 de Mayo del 2015.

Atentamente:

Dr. Nikolay Espinosa.	Ing. Cristian Vega.
DIRECTOR	CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

AUTORÍA DE RESPOSABILIDAD

JIMMY FABIAN LUDEÑA CARRIÓN

DECLARO QUE:

El proyecto de grado titulado: "ESTUDIO E IMPLEMENTACION DEL SOFTWARE INFOSPHERE GUARDIUM V9.1 PARA LA PROTECCIÓN DE LA BASE DE DATOS KDBS_SINERGY", ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las citas que constan al pie de las correspondientes páginas, cuyas fuentes se encuentran en las referencias bibliográficas.

Consecuentemente el presente trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del presente proyecto de grado.

Sangolquí, 20 de Mayo de 2015.

_____

Jimmy Fabian Ludeña Carrión

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo, Jimmy Fabian Ludeña Carrión

Autorizo a la Universidad de las Fuerzas Armadas ESPE, la publicación en la biblioteca virtual de la institución el proyecto de grado titulado: "ESTUDIO E IMPLEMENTACION DEL SOFTWARE INFOSPHERE GUARDIUM V9.1 PARA LA PROTECCIÓN DE LA BASE DE DATOS KDBS_SINERGY", cuyo contenido, criterios e ideas son de mi exclusiva responsabilidad y autoría.

Sangolquí, 20 de Mayo del 2015

_____

Jimmy Fabian Ludeña Carrión

DEDICATORIA

Dedico la culminación de este trabajo a mi país Ecuador porque sé que soy un hombre de bien y deseo realizar aportes muy buenos en favor de un mejor porvenir.

AGRADECIMIENTO

Agradezco a mi padre Galo Ludeña por ser el amigo que jamás me abandona y siempre me acompaña.

Agradezco a mi tío Mario Ludeña por su gran cariño y apoyo que siempre estuvo conmigo y por él conseguí terminar la carrera.

Agradezco a mi tío Enrique Ludeña, con el pasar del tiempo valoro sus enseñanzas, las cuales han sido demasiado fuertes. Siguiendo siempre sus pasos, mi carácter es cada vez más fuerte y firme.

Agradezco a todas las fuentes de energía externa que me ayudaron a levantar el espíritu y me mantienen fuerte.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La presente tesis tiene por objeto estudiar e implementar una solución que ayude a la gestión, control y supervisión de la actividad de los usuarios con privilegios y, realizar una evaluación de vulnerabilidades de la base de datos de la empresa Sinergy Team. Dentro de la gestión se busca proteger la información sensible en la cual se puedan tomar decisiones en tiempo real cuando se intenten ejecutar comandos no autorizados sobre objetos sensibles. El despliegue de agentes S-TAP, Discovery y CAS sobre el servidor de datos ayudan gestionar, controlar y evaluar tráfico y vulnerabilidades contra la base de datos. El propósito de este trabajo es estudiar e implementar la solución IBM Infosphere Guardium para asegurar la información alojada en la base de datos como las actividades de los usuarios privilegiados o proveedores que realizan operaciones sobre la base de datos para mitigar fuga de información. Se detalla la arquitectura, instalación, configuración y resultados de la solución.

PALABRAS CLAVES

VULNERABILIDADES

BASE DE DATOS

AGENTE S-TAP

AGENTE DISCOVERY

AGENTE CAS

USUARIOS PRIVILEGIADOS.

ABSTRACT

This thesis is to study and implement a solution to help manage, control and supervision of the activities of privileged users and perform a vulnerability assessment database company Sinergy Team. Within the management seeks to protect sensitive information on which decisions can be made in real time when trying to run unauthorized commands on sensitive objects. The deployment of agents S-TAP, Discovery and CAS on the data server help manage, monitor and evaluate traffic and vulnerabilities against the database. The purpose of this work is to study and implement the IBM InfoSphere Guardium solution for securing information stored in the database as the activities of privileged users or suppliers that operate on the database to mitigate information leakage. Architecture, installation, configuration and solution results are detailed.

KEYWORDS
VULNERABILITY
DATABASE
AGENT S-TAP
DISCOVERY AGENT
AGENT CAS
PRIVILEGED USERS.

CAPÍTULO I: MARCO TEORICO

1.1. Vulnerabilidades

Realizar la protección adecuada de las bases de datos, proteger su funcionamiento y la información no es tan fácil. Las organizaciones evalúan continuamente los paquetes de su software de base de datos, analizando y determinando cual sería activado y desactivado para reducir la superficie de ataques. Controlando los campos en las búsquedas para impedir inyecciones sql y el discernimiento de la debilidad en las credenciales en el inicio de sesión.

La mitad de las siguientes vulnerabilidades están relacionadas indirecta o directamente con las endebles prácticas de gestión de parches en el entorno de base de datos. El 38% de los administradores aplican los ajustes de seguridad en sus bases de datos en el ciclo de revisión inicial de tres meses y casi un tercio de ellos toman un año o más para aplicar el primer parche. (Maulini, 2010)

Las vulnerabilidades de bases de datos más usuales:

1.- Nombre de usuario/password en blanco, por defecto o débil. Algunas veces es normal encontrar pares de usuario/password como sa/1234, esta es la primera línea de defensa y punto fundamental de la armadura de nuestra base de datos.

2.- Inyecciones SQL

Cuando el motor de base de datos falla para la desinfección de sus entradas, los atacantes son capaces de ejecutar las inyecciones SQL de forma similar como lo hacen los atacantes basados en web. Les permite elevar sus privilegios con lo cual obtienen acceso a una amplia gama de funcionalidades. Los proveedores muestran sus soluciones para eludir estos problemas, lo cual no servirá de mucho si los parches no se aplican o no se toman los correctivos correspondientes.

3.- Preferencia de privilegios de usuario por privilegios de grupo.

Las organizaciones deben garantizar que los privilegios no les den a los usuarios por asignación directa. Los usuarios deberían recibir privilegios por parte de grupos o funciones y sean manejados colectivamente, de esta forma será fácil eliminar los derechos del usuario con simplemente eliminarlo del grupo, asegurando que no queden derechos ocultos u olvidados asignados a dicho usuario.

4.- Características de base de datos innecesariamente habilitadas.

Cada base de datos viene con paquetes adicionales que rara vez son utilizados por una organización. Las empresas necesitan ubicar los paquetes que no utilizan y desactivarlos. Esto no solo reduce el riesgo de ataques, sino que también simplifica la gestión de parches.

5.- Configuración de seguridad ineficiente.

Las bases de datos tienen diferentes configuraciones y consideraciones diferentes a disposición de los administradores para ajustar el rendimiento y funcionalidades mejoradas. Las empresas deberían conseguir y desactivar aquellas configuraciones inseguras que podrían estar activadas por defecto para mayor comodidad de los DBA o desarrolladores de aplicaciones. Las configuraciones de bases de datos en producción y desarrollo deberían ser radicalmente diferentes.

6.- Desbordamiento de búfer

Las vulnerabilidades de desbordamiento de búfer son abusadas por las inundaciones de las fuentes de entrada con valores diferentes o muy superiores a los que la aplicación espera. Por eso es muy importante la actualización de los parches.

7.- Escalada de privilegios

Con frecuencia las bases de datos exponen vulnerabilidades comunes permitiendo a un atacante escalar privilegios en una cuenta de privilegios bajos hasta tener acceso a los derechos de un administrador. A medida que las vulnerabilidades son descubiertas, los proveedores las descubren y los administradores deben mantener los parches actualizados

8.- Ataque de denegación de servicio

Los atacantes pueden utilizar las vulnerabilidades de los DBMS para derribar los servidores de base de datos a través de un alto flujo de tráfico.

9.- Base de datos sin actualizar

Los administradores de base de datos a veces no aplican un parche en el momento oportuno porque tiene miedo que este dañe su base de datos. El riesgo de ser hackeado es mucho más alto que el riesgo de aplicar un parche que descomponga la base de datos.

10.- Datos sensibles sin cifrar, tanto en reposo como en movimiento.

Las organizaciones no deben almacenar los datos sensibles en texto plano en una tabla. Todas las conexiones que manejen datos sensibles deben utilizar el cifradoue

escribiendo en este formato los párrafos que tengas, con la sangría tal y como esta y con el tipo de letra tal y como está mejor dicho estoy escribiendo full para llenar un párrafo y tener de modelo para poner asi mismo en los demás párrafos de este documento por eso va a encontrar este párrafo repetido en diferentes locaciones de documento.

1.2. Modelos O Algoritmos De Protección De La Información

La información es el activo más importante, por lo cual es necesario que se asegure más allá de la seguridad física.

Codificar la información es proteger la información en todos los trayectos por los cuales se encuentre circulando y la cual se requiera proteger, más no solamente en los más vulnerables.

Dentro de la codificación de la información está la criptografía, la cual se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones.

Algoritmo – Advanced Encryption Standard

También conocido como Rijandel, es un esquema de cifrado por bloques adoptado como un estándar de cifrado.

AES permite bloquear tamaños de bloques de 128, 168,192, 224 y 256 bits. AES permite tamaños de claves de 128, 192 y 256 bits, el estándar encryption usa AES-128 donde ambos el tamaño de bloques y claves son 1298 bits. El tamaño del bloque es cómodamente denotado como Nb y el tamaño de la clave es cómodamente denotado como Nk. Nb referido para el número de columnas en el bloque donde cada línea en la columna consiste de cuatro celdas de 8 bits cada uno para AES-128.

El siguiente ejemplo presentará como la información es rota dentro del bloque. Usando AES-128 significa que cada bloque consistirá de 128 bits. Nb puede ser calculado mediante la división de 128 por 32. El 32 viene desde el número de bytes en cada columna. En este caso, Nb es 4. El texto plano original es almacenado en bytes en un bloque. Por ejemplo el texto “Esto es un texto..” se almacenará en un bloque como en la figura de abajo.

	0	1	2	3
0	T		a	s
1	h	i		t
2	i	s	t	.
3	s		e	.

Figure 1. El texto plano original es almacenado en bytes en un bloque

Cada carácter es almacenado en una celda del bloque, la celda en blanco que se presenta en el diagrama no está realmente blanca como se representa el espacio en el texto. Dependiendo de cómo el algoritmo es implementado los caracteres pueden ser almacenados como valores enteros, valores hexadecimal o incluso cadenas binarias. Todas las tres formas representan la misma data. La mayoría de diagramas presentan valores hexadecimales, sin embargo la manipulación de cadenas y enteros es mucho más fácil hacer cuando AES programa actualmente. La figura 1 presenta los valores como caracteres para propósitos de demostración para presentar como el texto es almacenado dentro del bloque. EL texto plano es almacenado dentro de las columnas de bloques por columna y bloque por bloque antes que todos los datos estén almacenados. En el ejemplo de arriba fueron exactamente 16 caracteres utilizados por simplicidad. Para usar el algoritmo de Rijndael la data debe ser un múltiplo del tamaño del bloque, desde todos los bloques que deben ser completados. Cuando la Data no es un múltiplo del tamaño del bloque alguna forma de relleno debe ser usada.

La última cosa que necesita antes de usar el algoritmo es la clave. La clave también conocida como la clave cifrada es también el mismo tamaño como el bloque en este

ejemplo. La mayoría de la data y transformación de la clave cifrada puede tener los valores elegidos por el diseñador sin restricciones siempre que la clave es la longitud correcta. La clave también es almacenada como un bloque similar al texto sin formato. (Wikipedia, 2015)

Algoritmo - RC4

Es el sistema de cifrado de flujo más utilizado y se usa en algunos de los protocolos más populares Transport Layer Security (TSL/SSL) (Para proteger el tráfico de internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas).

RC4 es un algoritmo sorprendentemente simple. Este consiste en 2 algoritmo: 1-Key Scheduling Algorithm (KSA) y 2-Pseudo-Random Generation Algorithm (PRGA). Ambos de estos algoritmos usan 8-by-8 S-Box, el cual es solo un array de 256 números en el cual ambos son únicos en cuanto a rango y su valor va desde 0 hasta 255. Todos los números de 0 a 255 existen dentro del array, pero están solo mesclados de diferentes maneras, el KSA se encarga de realizar la primera mezcla en el S-Box, basado en el valor de la semilla dada dentro de él, y esta "semilla" puede ser de 256 bits de largo.

Primero, el S-box array es llenado con valores secuenciales desde 0-255. Este array será llamado simplemente S. Entonces, el otro array de 256 bits es llenado con el valor de la "semilla", repitiendo como sea necesario hasta que todo el array es llenado. Este array será llamado k, entonces el array S es mezclado usando el siguiente pseudocódigo

```
j=0;
for i = 0 to 255
{
    j = ( j+S [ i ] + k [ i ]) mod 256;
    intercambia S [ i ] and S [ j ];
```

}

Una vez que es realizado, la S-box es intercambiada basándose en el valor de la "semilla". Esa es la "Key" programada para el algoritmo, algo sencillo.

Ahora cuando se necesita el keystream data, se usa el Pseudo Rnadom Generation Algorithm (PGRA). Este algoritmo tiene 2 contadores, el i y la j, en el cual ambos son inicializadores en 0 para comenzar. Después de eso, cada bit de keystream data es usado en el siguiente Pseudo-Code:

```
i = (i + 1) mod 256;
j = (j + S[ i ]) mod 256;
intercambia S[I] and S[j];
t = (S[i] + S[j]) mod 256;
Exponer valor de S[t];
```

El valor expuesto del byte de S[t] es el primer byte del keystream, repitiéndose el algoritmo descrito para conseguir bytes adicionales de keystream.

RC4 es lo suficientemente sencillo como para ser almacenado e implementado al vuelo, aunque la robustez de dicho algoritmo depende, en gran medida, de la implementación y utilización realizada, existiendo graves problemas conocidos en la implementación del sistema de cifrado WEP, diseñado para ofrecer confidencialidad en redes Wireless. (Wikipedia, 2015)

Algoritmo – Blowfish

El Blowfish es un codificador de bloques simétricos, no se han encontrado técnicas de criptoanálisis efectivas contra el blowfish. Sin embargo, se ha dado más atención de la decodificación de bloques con bloques más grandes, como AES y Twofish.

Blosfish usa bloques de 64 bits y claves que van desde los 32 bits hasta 448 bits. Es un codificador de 16 rondas Feistel y usa llaves que dependen de las Cajas-S. Tiene una estructura similar a CAST-128, el cual usa Cajas-S fijas.

Diagrama de Blowfish

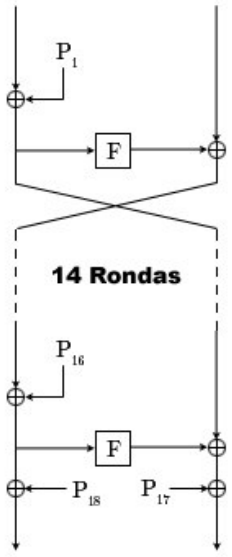


Figure 2. Diagrama de Blowfish

g El diagrama muestra la acción de Blowfish. Cada línea representa 32 bits. El algoritmo guarda 2 arrays de subclave. El array P de 18 entradas y 4 cajas-S de 256 entradas. Una entrada del array P es usada cada ronda, después de la ronda final, a cada mitad del bloque de datos se le aplica un XOR con uno de las 2 entradas del array P que no han sido utilizadas.

La función divide las entradas de 32 bits en 4 bloques de 8 bits, y usa los bloques como entradas para las cajas-S. Las salidas deben estar en módulo 232 y se les aplica un ok XOR para producir la salida final de 32 bits.

Debido a que Blowfish está en la red Feistel, puede ser invertido aplicando un XOR entre P17 y P18 al bloque texto codificado, así sucesivamente se usan las P-entradas en orden reversivo.

La generación de claves comienza inicializando los P-arrays y las cajas-S con los valores derivados de los dígitos hexadecimales de pi, los cuales no contienen patrones obvios. A la clave secreta de le aplica un XOR con las P-entradas en orden (ciclando la clave si es necesario). Un bloque de 64 bits de puros ceros es cifrado con el algoritmo como se indica. EL texto codificado resultante reemplaza a P1 y P2. Entonces el texto codificado es cifrado de nuevo con las nuevas subclaves, P3 y P4 son reemplazados por el nuevo texto codificado. Esto continúa, reemplazando todas las entradas del P-array y todas las entradas de las cajas-S. En total, el algoritmo de cifrado Blowfish correrá 521 veces para generar todas las subclaves cerca de 4KB de datos son procesados. (Wikipedia, 2014)

Algoritmo – Data Encryption Standard

Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS, cuyo uso de ha propagado ampliamente. El algoritmo DES hoy en día se considera inseguro en muchas aplicaciones, esto se debe principalmente a que el tamaño de clave de 56 bits es corto; las claves de DES se han roto en menos de 24 horas.

Existen también resultados analíticos que demuestran debilidades teóricas en su cifrado, aunque son inviables en la práctica. Se cree que el algoritmo es seguro en la práctica en su variante de triple DES, aunque existan ataques teóricos.

DES es el algoritmo prototipo del cifrado por bloques, el algoritmo al texto claro de longitud fija de bits los transforma mediante una serie de operaciones básicas en otro texto cifrado de la misma longitud. Para DES el tamaño es de 64 bits, utiliza clave criptográfica para modificar la transformación de tal manera que el descifrado sólo es realizable cuando se conoce la clave concreta utilizada en el cifrado.

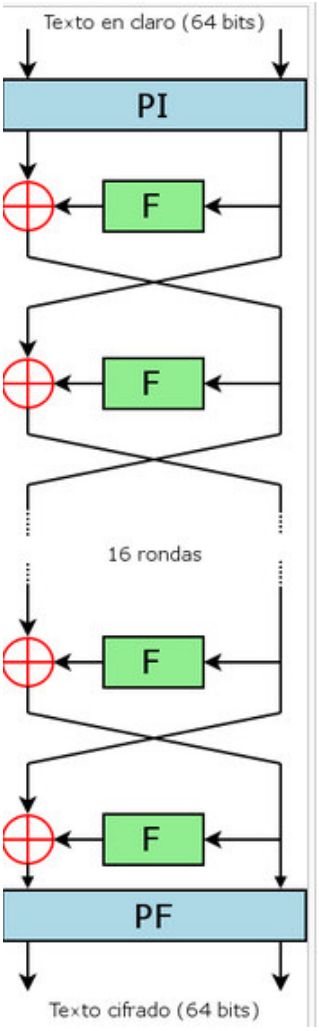


Figure 3. Data Encryption Standard

La clave mide 64 bits, aunque en realidad, sólo 56 de ellos son empleados por el algoritmo. Los ocho bits restantes se utilizan únicamente para comprobar la paridad, y después son descartados. La longitud de clave fija efectiva en DES es de 56 bits, y asi es como se especifica.

DES debe ser utilizado en el modo de operación de cifrado de bloque si se aplica a un mensaje mayor de 64 bits. (Wikipedia, 2015)

Algoritmo – Triple DES

Triple DES se le llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1998 se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, se eligió TDES para agrandar el largo de la clave sin la necesidad de cambiar de algoritmo de cifrado.

El TDES está desapareciendo lentamente, reemplazado por AES, aunque la mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo Triple DES. Por su diseño, el DES y el Triple DES con algoritmos lentos. AES puede llegar a ser hasta 6 veces más rápido y a la fecha no se ha encontrado ninguna vulnerabilidad. (Wikipedia, 2013)

Algoritmo – DSA

DSA (Digital Signature Algorithm), es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Este algoritmo como su nombre lo indica sirve para firmar y no para cifrar la información. (Wikipedia, 2015)

Algoritmo – ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) es una modificación del algoritmo DSA, emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciales que usa DSA (problema del algoritmo discreto). La principal ventaja de este esquema es que requiere números de tamaños menores para brindar la misma seguridad que DSA o RSA. (Wikipedia, 2014)

Algoritmo – International Data Encryption Algorithm

IDEA es un cifrado por bloques, fue un algoritmo propuesto para reemplazar al DES. Opera con bloques de 64 bits usando una clave de 128 bits y consiste de ocho transformaciones idénticas (cada una llamada un ronda) y una transformación de salida (llamada media ronda). El proceso de cifrar y descifrar es similar. Gran parte de la seguridad de IDEA deriva del intercalado de operaciones de distintos grupos – adición y multiplicación modular y O-exclusivo (XOR) bit a bit que son algebraicamente "incompatibles" en cierta forma.

IDEA mediante la utilización de tres operaciones en su proceso con las cuales logra la confusión, se realizan con grupos de 16 bits. (Wikipedia, 2014)

Algoritmo - ROT13

Es un sencillo cifrado césar utilizado para ocular un texto, en el cual se sustituye cada letra por la letra que está trece posiciones por delante en el alfabeto. A se convierte en N, B se convierte en O y así hasta la M, que se convierte en Z. Luego la secuencia se invierte: N se convierte en A, O se convierte en B y así hasta la Z, que se convierte en M. Este algoritmo se utiliza en foros de internet como medio para ocultar de miradas casuales, el final de un chiste, la solución a un acertijo, un spolier de una película o una historia, o algún texto ofensivo.

El ROT 13 no está pensado para los casos donde el secreto es una importancia. El efecto real es simplemente asegurarse de que el lector de un mensaje tenga que descifrarlo conscientemente, lo que normalmente suele implicar ejecutar el comando en cuestión en el software que lee el mensaje. En lugar de proteger un mensaje confidencial de los lectores no autorizados, el ROT13 salvaguarda a los lectores autorizados del material que pueden no querer leer involuntariamente. (Wikipedia, 2015)

Algoritmo – RSA

En criptografía RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública, siendo el primer algoritmo de este tipo más utilizado, válido para cifrar como para firmar digitalmente.

La seguridad del algoritmo radica en el problema de factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10200 y se prevé que su tamaño crezca con el aumento de la capacidad de cálculo de los ordenadores. (Wikipedia, 2015)

Algoritmo – Tiny Encryption Algorithm

TEA es un algoritmo para el cifrado por bloques notable por su simplicidad de descripción e implementación. TEA opera sobre bloques de 64 bits y usa una clave de 128 bits. Contiene una estructura de red aconsejada en 64 rondas, generalmente implementadas en parejas denominadas ciclos. Posee una generación de claves extremadamente simple, mezclando todo el contenido de la clave de la misma manera para cada ciclo. Se utilizan distintos múltiples de una constante mágica para prevenir ataques basados en la simetría de las rondas.

La más notable de las debilidades de TEA es que padece de claves equivalente, cada clave es equivalente a otras tres, y esto implica que la longitud de clave efectiva es solo de 126 bits. TEA también es susceptible de a ataques de clave relacionada que requieren 223 textos planos escogidos para un par de claves relacionadas, con una complejidad cronológica de 232.

1.3. Software Existente

Resulta difícil para las organizaciones conseguir el 100% de seguridad y control sobre que está ocurriendo en nuestras bases de datos corporativas. Para ello se hace necesario incorporar tecnologías especializadas en seguridad de base de datos que se encarguen de mirar todo el tráfico generado hacia ellas, reduciendo riesgo de actividad no permitidas, robo y/o pérdida de datos o incluso previniendo fraudes al ejecutar sentencias no autorizadas desde aplicaciones permitidas.

IBM Infophere Guardium

Se dedica a la seguridad de toda la base de datos y el cumplimiento del ciclo de vida con una consola de Web unificada, almacenamiento secundario de datos y sistema de automatización del flujo de trabajo, permitiéndole:

- Ubicar y clasificar información confidencial y errores de configuración
- Verificar si las configuraciones están bloqueadas después de implementar los cambios recomendados
- Capturar y examinar todas las transacciones de la base de datos, incluyendo acceso local por parte de usuarios privilegiados en todas las plataformas y protocolos

con un seguimiento retrospectivo seguro, no modificable que pemrite la separación de responsabilidades.

- Rastrear actividades en plataformas principales para compartir archivos
- Supervisar y reforzar las políticas de acceso a datos confidenciales, acciones de usuarios privilegiados, control de cambios, actividades de usuarios de la palicación y excepciones de seguridad, como ingresos negados.
- Automatizar todo el proceso de auditoría de cumplimiento, incluyendo la distribución de informes a los equipos de vigilancia, salidas y ascensos con informes pre-configurados para SOX, PCI DSS y privacidad de datos. Crear un único depósito centralizado de auditoría para realizar informes de cumplimiento de toda la empresa, optimización del rendimiento, investigaciones y argumentaciones.
- Aumentar fácilmente la escala de protección de una única base de datos a miles de bases de datos de centros de datos distribuidos. (IBM, s.f.)

The Vomretric Encryption Solution

Es una solución clara de entender por administración de llaves y encripción de información en reposo. Vormetric ofrece fuertes controles de seguridad de la información a través de controles y accesos basados en políticas, separación de funciones y capacidades de auditoria, las cuales pueden ser mantenidas desde una consola de administración centralizada.

La solución consiste de dos componentes

- Vormetric Data Security Manager
- Vormetric Encryption Expert Agents

El Vormetric Data Security Manager provee administración centralizada de llaves de incripción y el Vormetric Encryption Expert Agents provee protección de almacenamiento de información estructurada y no estructurada que puede incluir archivos de bases de datos y servidor de archivos, carpetas, documentos y escáner de imágenes, grabación de voz, registros y más. (Vormetric, 2015)

McAfee Vulnerabilty Manager for Databases

Ubicación exacta y grado de vulnerabilidad de todas las bases de datos. McAfee vulnerability manager for Databases da una visibilidad completa del estado de la seguridad de todas las bases de datos y proporciona una evaluación detallada de los riesgos gracias a las más de 4700 comprobaciones de vulnerabilidades que realiza. Clasifica con precisión las amenazas a la seguridad de las bases de datos en función de distintas prioridades, secuencias de comandos de reparación y recomendaciones. (Mcafee, 2014)

McAfee Database Activity Monitoring

Potencia la seguridad global de las bases de datos con una protección fiable en tiempo real frente a las amenazas externas e internas en los entornos físicos, virtuales y de internet. Los sensores de supervisión de la actividad de McAfee no requieren hardware ni cambios costosos en la arquitectura de sistemas existentes, con lo que tendrá una solución de seguridad de base de datos fácil de instalar y adaptable. Los sensores detectan inmediatamente cualquier tipo de comportamiento no autorizado o malicioso y le ponen término sin afectar de forma significativa al rendimiento general del sistema. McAfee Database Activity Monitoring significa considerablemente la gestión de la seguridad de las bases de datos y ayuda a garantizar el cumplimiento de las DSS del PCI, SOX, HIPAA/HITECJ, SAS 70 y de muchos otros tipos de normativas. (Mcafee, 2015)

McAfee Virtual Patching for Databases

McAfee Virtual Patching for Databases protege las bases de datos frente a los riesgos que entrañan las vulnerabilidades sin parche. Detecta y evita los intentos de ataque e intrusión en tiempo real, sin que sea necesario dejar inactivas las bases de

datos o realizar pruebas de las aplicaciones, lo que facilita la gestión de la seguridad de las bases de datos. (Mcafee, s.f.)

1.4. Normativa De Seguridad De La Información

La ISO27000 es una norma internacional emitida por la Organización Internacional de Normalización (ISO), describe cómo gestionar la seguridad de la información. Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. La redacción es realizada por los mejores especialistas del mundo en el tema, proporcionando una metodología para implementar la gestión de la seguridad de la información dentro de una organización.

La función de la norma es proteger la confidencialidad, integridad y disponibilidad de la información. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información, evaluando riesgos y así definir lo que es necesario hacer para evitar que estos problemas se produzcan, mitigando el riesgo.

Resolución 2148

Qué en el título II “De la organización de las instituciones del sistema financiero privado”, del libro I “Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero” de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capítulo I “Apertura y cierre de oficinas en el país y en el exterior de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros”;

Que en el título X “De la gestión integral y control de riesgos”, del citado libro I, consta el capítulo V “De la gestión del riesgo operativo”.

Que la superintendencia de Bancos y Seguros debe propender a que las instituciones del sistema financiero cuenten con fuertes medidas de seguridad en la tecnología de información y comunicaciones a fin de que los elementos tecnológicos utilizados para entregar sus productos y/o servicios sean seguros y confiables. Entre los eventos de riesgo operativo que enfrentan las instituciones supervisadas en el desarrollo de sus actividades, se encuentran el "fraude interno" y el "fraude externo" los cuales podrían ocasionarse a través del uso inseguro de la tecnología de información y comunicaciones.

Siendo de vital importancia que las instituciones del sistema financiero implementen suficientes medidas de seguridad para mitigar el riesgo de fraude por el uso de la tecnología de información y comunicaciones como elemento fundamental de una administración preventiva que reduzca la posibilidad de pérdidas e incremente su eficiencia, siendo parte de una adecuada gestión de riesgos. (Junta Bancaria del Ecuador , 2012)

CAPÍTULO II: SEGURIDAD DE LAS BASES DE DATOS

2.1. Generalidades

SINERGY TEAM durante su trayectoria, aumentado su cartera de clientes y un reconocimiento en el mercado, manejando desarrollando e implementando proyectos para diferente clientes como Retail, Gobierno, Servicios, Producción y Finanzas. Los proyectos, clientes, proveedores y ventas, cuentas bancarias que es almacenada en las bases de datos, la cual es administrada por profesionales que rotan de la empresa, después con el tiempo deciden desplazarse a otras empresas que pueden ser, de la competencia, es por lo cual se ha notado la falta de control de esa información.

Actualmente la empresa se encuentra protegida por un firewall que administra los accesos web y un directorio activo para la administración de los usuarios, con lo cual se autentican para ingresar a los servidores donde se encuentran alojadas las bases de datos. La seguridad en las bases de datos es un mecanismo fundamental ya que todo sistema informático está expuesto a cualquier tipo de amenazas de daño enormes y desastrosas como pequeñas y leves pero que de una manera u otra causan pérdida de confidencialidad.

La protección de la base de datos es proteger la información contra la revelación no autorizada, alteración no autorizada, destrucción intencional o involuntaria, está orientada a usuarios que no tienen derechos y a los que tienen derechos de acceso limitados a ciertas acciones. La información alojada en la base de datos es el activo más valioso de una empresa, recurso que podría ser valioso para la competencia, razón por la cual la necesidad de la empresa en controlar y administrar cuidadosamente la información. Por esto es necesario tener herramientas que permitan controlar y proteger la información en las bases de datos.igue escribiendo en este formato los

párrafos que tengas, con la sangría tal y como esta y con el tipo de letra tal y como está mejor dicho estoy escribiendo full para llenar un párrafo y tener de modelo para poner asi mismo en los demás párrafos de este documento por eso va a encontrar este párrafo repetido en diferentes locaciones de documento.

2.2. Seguridad De La Base De Datos

Infosphere Guardium es una solución tecnológica avanzada que permite supervisar de forma continua el acceso a bases de datos e impedir que se realicen actividades no autorizadas por parte de los usuarios internos finales a fin de detectar posibles fraudes, sin realizar cambios en las bases de datos ni en las aplicaciones y sin que esto afecte el rendimiento y eficiencia en el servicio.

Sinergy Team, realizó la adquisición e implementación de una solución de monitoreo y seguridad IBM Infosphere Guardium para la base de datos KDBS_SINERGY.igue escribiendo en este formato los párrafos que tengas, con la sangría tal y como esta y con el tipo de letra tal y como está mejor dicho estoy escribiendo full para llenar un párrafo y tener de modelo para poner asi mismo en los demás párrafos de este documento por eso va a encontrar este párrafo repetido en diferentes locaciones de documento.

2.2.1. Sensibilidad

A medida que el tamaño y la organización de la base de datos corporativa crece, la información sensible como números de tarjetas de crédito y transacciones o datos financieros. Esto ocurre con frecuencia en las empresas que han experimentado las fusiones y adquisiciones y en las empresas de más edad, donde los sistemas de legado han sobrevivido a sus dueños originales. Incluso en el mejor de los casos, los proyectos

de integración y de mejora entre los sistemas dispares pueden dejar fácilmente los datos sensibles desconocido y sin protección.

Guardium® proporciona la función de clasificación para descubrir y clasificar datos confidenciales, por lo que usted puede hacer y hacer cumplir las decisiones efectivas de política de acceso.

Una política de clasificación es un conjunto de normas destinadas a descubrir y elementos de etiquetas sensibles de datos (tablas de bases de datos o archivos). Una acción podría ser la de generar una alerta de correo electrónico, o para añadir un miembro a un grupo (Guardium). Cada vez que una regla se cumple, que se registra el suceso, y por lo tanto se puede informar sobre (a menos que se especifica IGNORE como la acción a tomar, en cuyo caso no hay ningún registro de esa norma).

Una fuente de datos identifica una instancia de base de datos específica, y su definición en el sistema Guardium puede opcionalmente información de la cuenta tienda y otros parámetros necesarios para acceder a la base de datos. Definiciones de origen de datos pueden ser compartidos, y pueden ser utilizados por otras aplicaciones además de la clasificación.

2.2.2. Vulnerabilidades

El Proceso de evaluación de Guardium evalúa la salud de su entorno de base de datos y recomienda la mejora a través de:

- La evaluación de la configuración del sistema con las mejores prácticas y la búsqueda de vulnerabilidades o amenazas potenciales a los recursos de bases de datos, incluyendo la configuración y los riesgos de comportamiento.

- Encontrar las vulnerabilidades inherentes presentes en el entorno de TI, como parches de seguridad ausentes,
- Recomendar y dar prioridad a un plan de acción basado en las zonas descubiertas de la mayoría de los riesgos críticos y vulnerabilidades. La generación de informes y recomendaciones proporcionan directrices sobre la forma de responder a los cambios de cumplimiento y elevar la seguridad del entorno de base de datos evaluados
- Evaluación de la vulnerabilidad de base de datos de Guardium combina tres métodos de prueba esenciales para garantizar la profundidad y amplitud de la cobertura. Aprovecha las múltiples fuentes de información para elaborar un cuadro completo de la salud de la seguridad del entorno de base de datos y los datos.
- Vulnerabilidades de detección-Descubriendo pasivos mediante la observación del tráfico de red.
- Escaneo-Interrogar un punto final en la red a través del acceso con credenciales.

Incluido en la vulnerabilidad Guardium y solución de gestión de amenazas son:

Base de datos de descubrimiento automático -performs una red de auto-descubrimiento del entorno de base de datos y crea una representación gráfica de las interacciones entre los clientes de bases de datos y servidores.

Content Database Clasificador manera automática descubre y clasifica los datos confidenciales, como números de tarjetas de crédito de 16 dígitos y Seguridad Social de 9 dígitos números ayudar a las organizaciones a identificar rápidamente los negocios defectuoso o los procesos de TI que almacenan datos confidenciales.

Evaluación de la vulnerabilidad de base de datos -scans la infraestructura de base de datos en busca de vulnerabilidades y proporciona una evaluación de la base de datos y la seguridad de los datos de salud, con el tiempo real y las mediciones históricas.

CAS (Configuración del Sistema de Auditoría) -tracks todos los cambios en los elementos tales como las estructuras de bases de datos, controles de acceso y seguridad, valores de datos críticos, y los archivos de configuración de base de datos.

Cumplimiento Workflow Automation -automates todo el proceso de cumplimiento a través de comenzar con la evaluación y el endurecimiento, monitorización de la actividad al informe de auditoría, la distribución de informes, y sign-off por las principales partes interesadas.

CAS (Sistema de Auditoría de Configuración) desempeña un papel importante en la identificación de vulnerabilidades y amenazas. Guardium pre-configurado y plantillas CAS definidos por el usuario se puede utilizar en la prueba de Evaluación y llevar una visión holística del entorno de base de datos del cliente; Con CAS, Guardium puede identificar vulnerabilidades a la base de datos en el nivel de sistema operativo, como los permisos de archivos, la propiedad y las variables de entorno. Estas pruebas pueden ser visto a través del panel de CAS conjunto de plantillas Definición y tener la palabra 'Evaluación' en su nombre.

Vulnerability Assessment (VA) y Configuración del Sistema de Auditoría (CAS) sólo se admiten en Inglés.

Vulnerabilidades y Exposiciones Comunes (CVE®) es un diccionario de nombres comunes (es decir, Identificadores CVE) para las vulnerabilidades de seguridad de información de conocimiento público. Identificadores comunes de CVE hace que sea más fácil compartir datos a través de bases de datos y herramientas de seguridad de red separados, y proporcionar una línea de base para evaluar la cobertura de tal manera

que, si un informe incorpora CVE Identificadores, los usuarios pueden acceder de forma rápida y precisa fijar la información en compatible CVE-independiente uno o más bases de datos para remediar el problema.

Numerosas organizaciones han hecho sus productos de seguridad de la información y servicios "compatible con CVE" mediante la incorporación de identificadores CVE. Guardium monitorea constantemente las vulnerabilidades y exposiciones comunes (CVE) de la Corporación MITRE y agregar estas pruebas para las vulnerabilidades relacionadas con bases de datos pertinentes.

Para ayudar en el descubrimiento de las vulnerabilidades individuales mientras ve los nombres CVE para bases de datos específicas, el usuario, al configurar las pruebas a través de Evaluación de Seguridad Builder, puede seleccionar el botón de radio CVE para la base de datos deseada y luego seleccionar y agregar el identificador CVE apropiado. Información adicional siempre se puede encontrar en la copia maestra de la lista mantenida por el CVE MITRE Corporation.

Para mantenerse al día CVEs dentro de la solución Guardium, Guardium descargará y utilizar la base de datos CVE más actual para rellenar una tabla de base de datos con todas las entradas CVE actuales y candidatos. Guardium compara la programación los datos CVE descargados con los datos CVE ya están en el repositorio de Evaluación de la Vulnerabilidad Guardium; producir una lista de nuevas CVEs para su revisión. Base de datos Guardium Equipo de Seguridad revisa manualmente estos candidatos a la vulnerabilidad de Conocimientos Guardium, los prueba y añade las pertinentes a la vulnerabilidad GA Guardium Evaluación de Conocimientos. Estas pruebas están etiquetados con el número CVE apropiado, y una vez en el repositorio GA, estas pruebas pueden ejecutarse de forma automática mediante la aplicación de Evaluación de Vulnerabilidad Guardium. (IBM, s.f.)

2.2.3. Endurecimientos

La administración de vulnerabilidades y amenazas es el inicio para la gestión del ciclo de vida de seguridad y cumplimiento para cualquier entorno de TI. Un conjunto predefinido y personalizado, junto con un flujo de trabajo de procesos, permiten a las organizaciones a identificar y vulnerabilidades de bases de datos de direcciones en una infraestructura de forma proactiva para mejorar configuraciones y endurecimiento automatizados.

El clasificador de manera automática descubre y clasifica los datos confidenciales, ayuda a las organizaciones a identificar rápidamente los negocios defectuosos o los procesos de TI que almacenan datos confidenciales.

La aplicación de Evaluación de Vulnerabilidad Guardium permite a las organizaciones identificar y vulnerabilidades de bases de datos de direcciones de forma consistente y automatizado. Proceso de evaluación de Guardium evalúa la salud de su entorno de base de datos y recomienda la mejora a través de:

La evaluación de la configuración del sistema con las mejores prácticas y la búsqueda de vulnerabilidades o amenazas potenciales a los recursos de bases de datos, incluyendo la configuración y los riesgos de comportamiento. Por ejemplo, la identificación de todas las cuentas por defecto que no han sido personas con discapacidad; comprobar privilegios públicos y métodos de autenticación elegida, etc.

Encontrar las vulnerabilidades inherentes presentes en el entorno de TI, como parches de seguridad ausentes,

Recomendar y dar prioridad a un plan de acción basado en las zonas descubiertas de la mayoría de los riesgos críticos y vulnerabilidades. La generación de informes y recomendaciones proporcionan directrices sobre la forma de responder a los cambios de cumplimiento y elevar la seguridad del entorno de base de datos evaluados

Evaluación de la vulnerabilidad de base de datos de Guardium combina tres métodos de prueba esenciales para garantizar la profundidad y amplitud de la cobertura. Aprovecha las múltiples fuentes de información para elaborar un cuadro completo de la salud de la seguridad del entorno de base de datos y los datos.

Agente - El uso de software instalado en cada punto final (por ejemplo, servidor de base de datos). Ellos pueden determinar los aspectos del punto final que no se pueden determinar de forma remota, como el acceso de administrador a los datos sensibles directamente desde la consola de base de datos.

Vulnerabilidades de detección - Descubriendo pasivos mediante la observación del tráfico de red. (IBM, s.f.)

2.2.4. Auditoria

La solución Guardium organiza los datos que recoge en un conjunto de dominios. Cada dominio contiene un tipo diferente de información relativa a un área concerniente a: el acceso a datos, excepciones, violaciones de política, y así sucesivamente.

Todos los dominios y sus contenidos se describen en los Dominios, Entidades y Atributos apéndice.

Hay un generador de consultas independiente para cada dominio, y el acceso a cada generador de consultas se controla a través de las funciones de seguridad. Sin importar el dominio, la misma herramienta de consulta-constructor de uso general se utiliza para crear todas las consultas.

Además del conjunto estándar de dominios, los usuarios pueden definir dominios personalizados para contener la información que se puede cargar en el aparato Guardium. (IBM, s.f.)

2.2.5. Pistas de Auditoria

La solución de manera continua crea pistas de auditoría muy detalladas de todas las actividades referente a la bases de datos que son analizada constantemente y filtradas en tiempo real para implementar controles proactivos y producir la información específica requerida por los auditores.

Los reportes muestran el cumplimiento, entregando visibilidad detallada a todas las actividades de la base de datos tales como: claves erróneas, asignación de privilegios, cambios en el esquema, acceso en horas prohibidas o en aplicaciones no autorizadas y el acceso a tablas con información sensible. El sistema debería monitorear:

- Excepciones de seguridad tales como errores SQL y contraseñas fallidas.
- Comandos DDL tales como CREATE/ DROP/ALTER TABLE que pueden cambiar las estructuras de las bases de datos y que son particularmente importantes para las regulaciones de la gestión de datos tales como SOX.

- SELECT queries, que son especialmente importantes para las regulaciones de privacidad de datos como PCI.
- Comandos DML (INSERT, UPDATE, DELETE) incluyendo variables ocultas
- Comandos DCL que controlan las cuentas, los roles y los permisos (GRANT, REVOKE).
- Lenguajes de procedimientos soportados por cada plataforma DBMS tales como PL/SQL (Oracle) y SQL/PL (IBM).
- XML ejecutados por la base de datos.

Esta clase de soluciones no son invencibles, por lo que requieren que cada organización pueda crear dentro de su cultura al menos un departamento de auditorías de acceso a la información y uno de seguridad de acceso a aplicaciones y a los datos, siendo éste último el encargado de dictar las reglas de gobernabilidad de la información para cada rol dentro y fuera de la organización.igue escribiendo en este formato los párrafos que tengas, con la sangría tal y como esta y con el tipo de letra tal y como está mejor dicho estoy escribiendo full para llenar un párrafo y tener de modelo para poner así mismo en los demás párrafos de este documento por eso va a encontrar este párrafo repetido en diferentes locaciones de documento. (IBM, s.f.)

2.2.6. Autenticación

La gestión de usuarios y roles es generalmente reservado para el administrador de acceso: el usuario Guardium que se le asigna el nombre de usuario accessmgr.

Definición y modificación de usuarios implica decidir tanto que van a utilizar el sistema de Guardium y en qué roles que serán asignados. Un rol es un grupo de

usuarios, todos los cuales se otorgan los mismos privilegios de acceso. Para obtener más información sobre las funciones, consulte Administrar funciones.

Definiciones de usuario pueden ser importados desde un servidor LDAP, a la vista o en un horario. Para obtener más información, consulte Importar usuarios desde LDAP.

Independientemente de cómo los usuarios se definen en el aparato Guardium, el administrador Guardium puede configurar el dispositivo para autenticar a los usuarios a través de Guardium, LDAP o Radio.

En nuestros primeros pasos con un dispositivo Guardium, una importante tarea temprano es identificar qué grupos de usuarios van a utilizar ese aparato, y cuál será su función. Por ejemplo, un grupo de seguridad de la información puede utilizar Guardium para alertar y solucionar problemas; un grupo de administradores de base de datos puede utilizar Guardium de información y control. Al decidir quién acceder al sistema Guardium, tenga en cuenta que los datos confidenciales de la empresa pueden ser recogidos por el sistema. Por lo tanto, ser muy conscientes de que será capaz de acceder a esos datos. (IBM, s.f.)

Seguridad de la cuenta de usuario

Varios ajustes se pueden modificar para proporcionar seguridad adicional para las cuentas de usuario. Puedes activar o desactivar esta configuración con el espectáculo y almacén de contraseñas comandos CLI (ver cuentas de usuario, contraseña y comandos de la CLI de autenticación en la referencia de la CLI).

De forma predeterminada, la validación de contraseña está activada. Esto significa que se requiere un mínimo de ocho caracteres y la contraseña debe tener al menos un carácter de cada una de las siguientes categorías:

Las letras mayúsculas: A-Z
Letras minúsculas: a-z
Dígitos: 0-9
Caracteres especiales: @ # $% ^ &; - + = _.!

De forma predeterminada, la caducidad de contraseña está activada. Las contraseñas se pueden configurar para expirar después de un número determinado de días.

De forma predeterminada, el bloqueo de cuenta tras un número determinado de intentos fallidos de conexión está activada. De bloqueo se puede configurar para producir después de un número fijo de intentos en un tiempo determinado, o después de un número total de intentos para la vida de la cuenta. (IBM, s.f.)

Cuentas bloqueadas

El gestor de acceso Guardium puede habilitar una cuenta de usuario deshabilitada desde el panel de mantenimiento del usuario.

Si la cuenta de usuario administrador se bloquea, utilice el comando CLI de administración de desbloqueo para desbloquearla (consulte Instalación y comandos de la CLI de control en la referencia de la CLI).

2.2.7. Control de Acceso

Un rol es un grupo de usuarios Guardium, los cuales tienen los mismos privilegios de acceso.

El gestor de acceso define las funciones, y los asigna a los usuarios y aplicaciones. Cuando se asigna un papel a una aplicación o la definición de un elemento (una consulta específica, por ejemplo), sólo aquellos usuarios Guardium que también se asignan ese rol pueden acceder a ese componente.

Si no hay funciones de seguridad se asignan a un componente (un informe, por ejemplo), sólo el usuario que define ese componente y el usuario administrador puede acceder a él. En el tiempo de instalación, Guardium está configurado con un conjunto predeterminado de papeles, y un conjunto predeterminado de cuentas de usuario.

Cuando definiciones de usuario se importan desde un servidor LDAP, los grupos a los que pertenecen, opcionalmente, se pueden definir como roles. Para obtener más información.

igue escribiendo en este formato los párrafos que tengas, con la sangría tal y como esta y con el tipo de letra tal y como está mejor dicho estoy escribiendo full para llenar un párrafo y tener de modelo para poner asi mismo en los demás párrafos de este documento por eso va a encontrar este párrafo repetido en diferentes locaciones de documento.

2.2.8. Gestión de Derechos

Cada rol por defecto viene con un diseño predeterminado. Cuando un usuario inicia una sesión por primera vez, la disposición inicial de dicho usuario está determinada por las funciones asignadas. Después de la entrada inicial, agregar o quitar funciones no alterarán la disposición del usuario. Después de retirar un papel, si el usuario intenta acceder a los informes o las aplicaciones que ya no están autorizados, se producirá un mensaje de "no autorizado". (IBM, s.f.)

2.3. Tipos De Ataques A Las Bases De Datos

Inyección por SQL. Un ataque de este tipo puede dar acceso a alguien y sin ningún tipo de restricción a una base de datos completa e incluso copiar o modificar la información. Acciones como las siguientes.

- Descubrimiento de la información (information disclosure): Las técnicas de inyección SQL pueden permitir a un atacante modificar consultar para acceder a registros y/o objetos de la base de datos a los que inicialmente no tenía acceso
- Elevación de privilegios: Todos los sistemas de autenticación que utilicen credenciales almacenadas en motores de base de datos hacen que una vulnerabilidad de inyección SQL pueda permitir a un atacante acceder a los identificadores de usuarios más privilegiados y cambiarse las credenciales.
- Denegación de servicio: La modificación de comandos SQL puede llevar a la ejecución de acciones destructivas como el borrado de datos, objetos o la parada de servicios con comandos de parada y arranque de los sistemas. Asimismo, se pueden inyectar comandos que generen un alto cómputo en el motor de base de datos que haga que el servidor no responda en tiempos útiles a los usuarios legales.

- Suplantación de usuarios: Al poder acceder al sistema de credenciales, es posible que un atacante obtenga las credenciales de otro usuario y realice acciones con la identidad robada o “spoofeada” a otro usuario

Malware y spear phishing. Se trata de una técnica combinada que usan los cibercriminales, hackers patrocinados por estados o espías para penetrar en las organizaciones y robar sus datos confidenciales.

Es una variante del phishing y consiste en el envío de mensajes, generalmente por correo electrónico, específicos y personalizados a un grupo de personas determinado. Esta es la principal diferencia respecto al phishing tradicional por email, que consistía en el envío de un mismo correo electrónico de forma masiva y al azar a millones de usuarios.

El medio de distribución más utilizado es el mismo en ambos casos, el correo electrónico. Se envía un correo supuestamente legítimo con una invitación para abrir un archivo adjunto que contiene un malware, un enlace que dirige a una página para la descarga de un programa malicioso o un enlace que dirige a un formulario con el objetivo de obtener información confidencial.

Con el envío de mensajes específicos, para los que previamente se suele haber realizado una búsqueda de información del objetivo, a un grupo limitado de usuarios seleccionados expresamente, generalmente de una misma empresa e incluso de un departamento en concreto, y con información muy precisa y personalizada se persigue obtener habitualmente:

- Información altamente confidencial propia de la organización.
- Datos de clientes, información bancaria, etc.
- Información de otras organizaciones con las que trata la organización víctima.

(Vergara, 2012)

2.4. Daños y Perjuicios Por Los Atacantes

El 96% de los datos sustraídos durante 2012 provenían de bases de datos, según un informe de Verizon (Data Breach). Además, durante el año pasado, 242 millones de registros resultaron potencialmente comprometidos, indica la Open Security Foundation. Se trata de dos preocupantes datos que la compañía Imperva, especializada en seguridad, recuerda en un informe que ha elaborado sobre las diez principales amenazas que existen contra las bases de datos y en el que se pone de manifiesto que éstas son el objetivo prioritario para hackers e insiders maliciosos.

En el informe asevera que esto es así debido a que las bases de datos representan el corazón de cualquier organización, ya que almacenan registros de clientes y otros datos confidenciales del negocio. Y afirma además que esta vulnerabilidad de las bases de datos mejoraría si no hubiera la actual falta de inversión en soluciones de seguridad adecuadas para protegerlas. Y es que, como señala IDC, menos del 5% de los 27.000 millones de dólares invertidos en 2011 en productos de seguridad se destinaron a la salvaguarda de los centros de datos.

Éste es, según Imperva, el top 10 en amenazas en el entorno de bases de datos:

Privilegios excesivos e inutilizados.

Abuso de Privilegios.

Inyección por SQL.

Malware y spear phising.

Auditorías débiles.

Exposición de los medios de almacenamiento para backup.

Explotación de vulnerabilidades y bases de datos mal configuradas. Los atacantes saben cómo explotar estas vulnerabilidades para lanzar ataques contra las empresas.

Datos sensibles mal gestionados. Los datos sensibles en las bases de datos estarán expuestos a amenazas si no se aplican los controles y permisos necesarios.

Denegación de servicio (DoS). En este tipo de ataque se le niega el acceso a las aplicaciones de red o datos a los usuarios previstos. Las motivaciones suelen ser fraudes de extorsión en el que un atacante remoto repetidamente atacará los servidores hasta que la víctima cumpla con sus exigencias.

Limitado conocimiento y experiencia en seguridad y educación. Muchas firmas están mal equipadas para lidiar con una brecha de seguridad por la falta de conocimientos técnicos para poner en práctica controles de seguridad, políticas y capacitación.

Para la firma de seguridad, la clave para evitar estas amenazas es una defensa multicapa que permita localizar y evaluar dónde se ubican las vulnerabilidades en la base de datos y en qué sitio residen los datos críticos; gestionar los derechos de usuario para identificar derechos excesivos sobre los datos sensibles; hacer monitorización y bloqueo para proteger las bases de datos de ataques, pérdida de datos y robo; realizar auditorías y proteger los datos.

2.5. Posicionamiento del Software en el mercado

IBM posee la solución a estas necesidades, recientemente con la adquisición de la empresa Guardium (www.guardium.com). IBM se ha posicionado como líder en el aspecto de seguridad de acceso a las bases de datos, soportando todo tipo de marcas de bases de datos y plataformas, con capacidades inclusive de registrar los accesos de usuarios privilegiados (DBAs) a datos sensitivos y no solamente de registrarlos, sino de bloquear su acceso en el preciso instante que una regla es violada.

Existen en el mercado otras soluciones que tratan de competir con IBM Guardium, sin embargo ninguna de ellas incluye una solución global como IBM Guardium:

- Algunas de ellas son exclusivas para una marca de base de datos y sobre una versión X hacia arriba.
- Otras no cubren aspectos de seguridad que involucran a los usuarios privilegiados y ni siquiera los toman en cuenta.
- La mayoría no incluye la capacidad de asegurar de una manera determinante quién es el usuario que se ha conectado a la base de datos cuando la aplicación es web y su conexión a la base de datos es a través de un pool de conexiones.
- Otras no pueden determinar usuarios registrados en los directorios LDAP de las organizaciones y compararlos con los usuarios registrados en la base de datos, siendo esto un factor de seguridad muy importante.
- Otras soluciones requieren de varios componentes para poder tratar de dar una solución como la que IBM Guardium ofrece.
- Algunas de estas soluciones que tratan de competir requieren que se activen lo logs nativos de las bases de datos.
- No son multiplataforma.

No generan alertas en tiempo real.

2.6. Componentes de la Arquitectura

2.6.1. Equipos

Appliance

El appliances incluye las siguientes subcategorías:

– Colector: El colector es el equipo que se utiliza para la captura en tiempo real y analizar la actividad de la base de datos

– Agregador: El equipo agregador se utiliza para descargar la actividad de reporte desde los colectores y para proveer informes consolidados desde múltiples colectores.

– Administrador Central: El administrador central (CM) es una función especializada que está habilitada en un equipo Agregador. La función del CM se utiliza para gestionar y controlar múltiples equipos Colectores Guardium.

2.6.2. Agentes

Los agentes incluyen la siguiente subcategoría:

– Agente Software TAP (S-TAP®): El agente S-TAP es instalado sobre el servidor de base de datos y se utiliza para monitorear y transmitir la actividad de la base de datos al equipo colector Guardium.

– Agente Guardium Installation Manager (GIM): El agente GIM se instala sobre el servidor de base de datos y se utiliza para facilitar la instalación del agente y la modificación y actualización de los agentes.

– Agente Change Audit System (CAS): El agente CAS se instala sobre el servidor de base de datos y se utiliza para capturar información de cambio de auditoría de archivos de configuración y más en el servidor de base de datos.

– Agente Instance Discovery: El agente instance discovery se instala sobre el servidor de base de datos y se utiliza para obtener información del puerto y motor de la base de datos.

2.7. Módulos

2.7.1. Database Auto-Discoverys

Algunas veces introducen bases de datos en el entorno de producción lejos de los mecanismos de control. La nueva base de datos podría ser parte de un paquete de aplicación de un proveedor de software. Cuando las instalaciones son grandes, otras veces las bases de datos pueden ser abandonadas, u olvidadas sin control, porque sus datos y/o actividades no representan riesgo cuando se implementó la base de datos.

Incluso un DBA podría crear una base de datos y hacer con ella diferentes actividades sin ser supervisado.

El Auto-descubrimiento puede ser configurado para sondear la red, búsqueda y presentación de informes sobre todas las bases de datos descubiertos.

Cuando el proceso de auto-descubrimiento ha iniciado, se lo puede programar para una ejecución periódica. Hay dos tipos de trabajos que se pueden programar para cada proceso:

Un trabajo de escaneado escanea cada host, y compila una lista de puertos abiertos de la lista de puertos especificados para ese host. Un trabajo de digitalización se debe ejecutar antes de ejecutar el segundo tipo de trabajo.

Un trabajo de investigación utiliza la lista de puertos abiertos compilados durante la última exploración única completado. El trabajo de la sonda determina si hay servicios de bases de datos que se ejecutan en esos puertos. Puede ver los resultados de este trabajo en las bases de datos Descubierto informe predefinido. (IBM)

2.7.2. Classifier

La información sensible puede ser presentada en múltiples locaciones sin el actual conocimiento de los actuales propietarios de esta información, o puede tener cualquier propietario en absoluto.

A medida que la organización aumenta el tamaño de la base de datos crece, información sensible como números de tarjetas de crédito y transacciones o datos financieros personales, puede estar presente en varias ubicaciones, sin el conocimiento de los actuales propietarios de esos datos. Generalmente sucede en empresas de más edad, o empresas que has sufrido fusiones y adquisiciones, donde los sistemas de legado han sobrevivido a sus dueños originales. Incluso en el mejor de los casos, los proyectos de integración y de mejora entre los sistemas dispares pueden dejar fácilmente los datos sensibles desconocida y sin protección.

Guardium proporciona la función de clasificación para descubrir y clasificar los datos sensibles, de modo que se puedan hacer cumplir las decisiones efectivas de política de acceso.

Una política de clasificación es un conjunto de normas destinadas a descubrir elementos sensibles de la etiqueta de datos (tablas de bases de datos o archivos). Se puede definir un conjunto de acciones que deben tomarse para cada regla. Una acción podría ser la de generar una alerta de correo electrónico. Cada vez que una regla se cumple, que se registra el suceso, y por lo tanto se puede informar al (a menos que ignore se especifica como la acción a tomar, en cuyo caso no hay ningún registro de esa regla).

Un proceso de clasificación define un trabajo que consiste en una política de clasificación de una o más fuentes de datos. El proceso puede ser presentado para ser ejecutado una vez, o puede ser programada para ejecutarse de forma periódica, como una tarea en un proceso de automatización del flujo de trabajo de cumplimiento. (IBM)

CAPÍTULO III: IMPLEMENTACION Y APLICACIÓN DE LA SOLUCION

3.1. Introducción

La empresa Sinergy Team Cia. Ltda requiere asegurar la información alojada en la base de datos. Infosphere es la solución que protegerá a la base de datos de actos indebidos con el cumplimiento de normas de seguridad.

En este capítulo menciona el proceso para planear la implementación Infosphere Guardium, la solución es escalable, alta capacidad de adaptabilidad

La solución se basa en un equipo instalado en un ambiente virtual sobre el mismo segmento de red del servidor de base de datos, el cual recolecta la información observada según los procesos, políticas y reglas implementadas para efectuar acciones según corresponda.

3.2. Configuración del equipo

3.2.1. Ingreso al equipo.

El colector Guardium es un software que está implementado en un ambiente virtualizado, el ambiente de virtualización es un ESXi, accedemos por medio del cliente VMware vSphere Client con usuario root

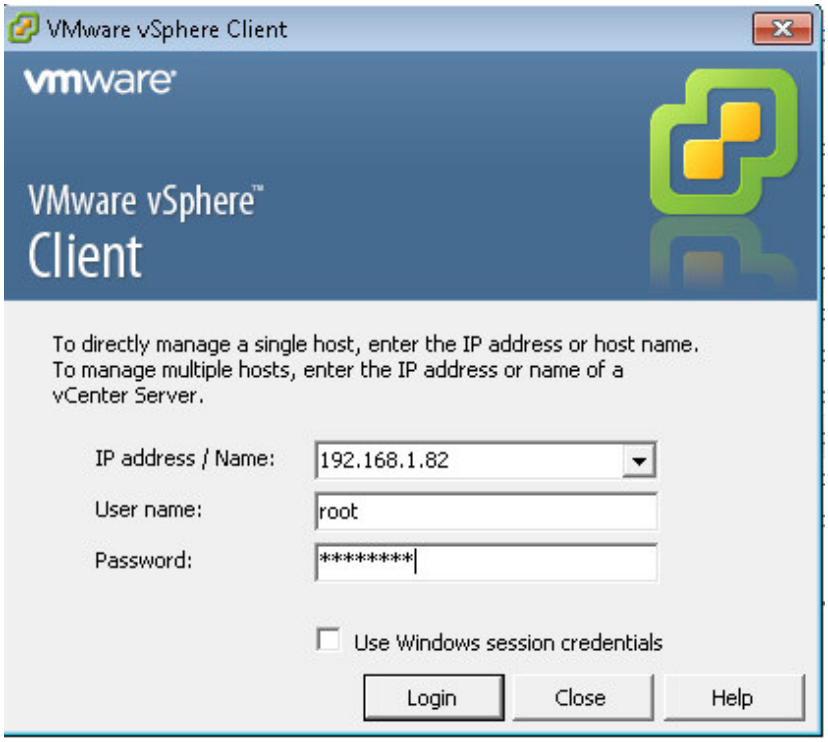


Figure 4. Acceso al ambiente de virtualización ESXi

La consola de virtualización está implementada sobre un equipo IBM System serie x3200, en este ambiente se encuentra máquinas virtuales de producción y la base de datos principal que se requiere proteger de ataques internos y externos.

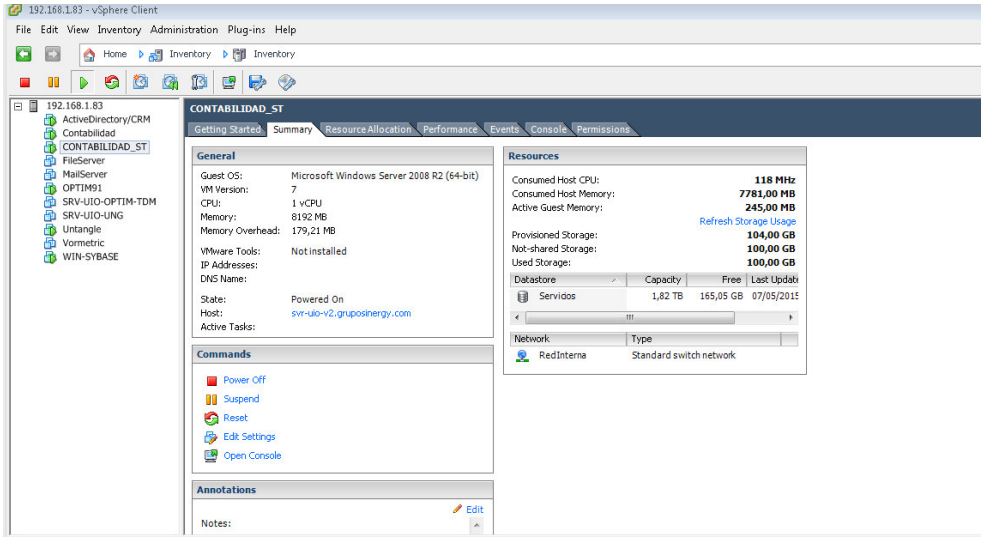


Figure 5. Consola de virtualización

La solución Guardium mantiene tres usuarios de seguridad estándar para proteger la información almacenada en el equipo. Para controlar por comandos utilizaremos el usuario “cli”

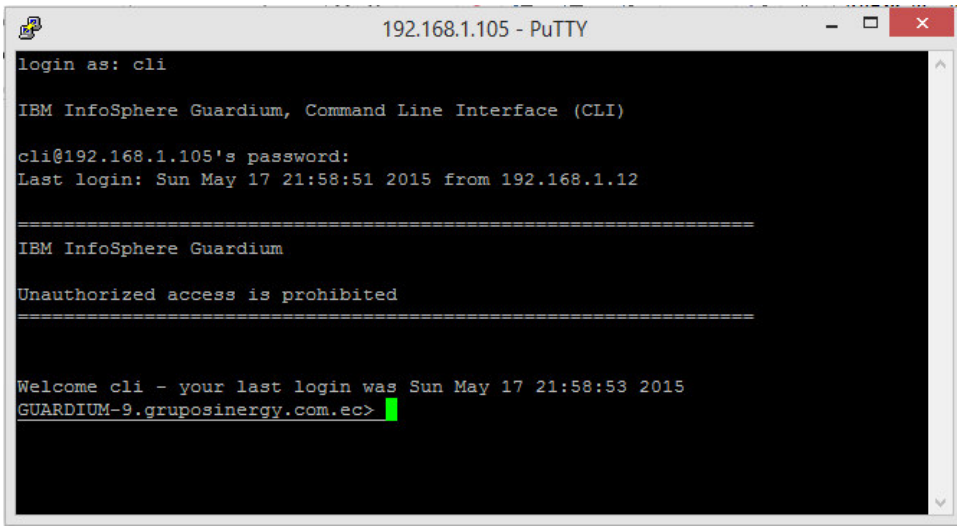


Figure 6. Consola de comandos del colector Guardium

3.2.2. Configuración de la red.

El colector tiene la figura de una caja cerrada, la cual es instalada sobre el mismo segmento de red donde se encuentra funcionando el servidor de datos y que contiene la base de datos que se requiere proteger.

Ingresamos la dirección ip para eth 0, como se presenta en la siguiente imagen por medio del comando

Store network interface ip <ip_address>

Store network interface mask <network_mask>

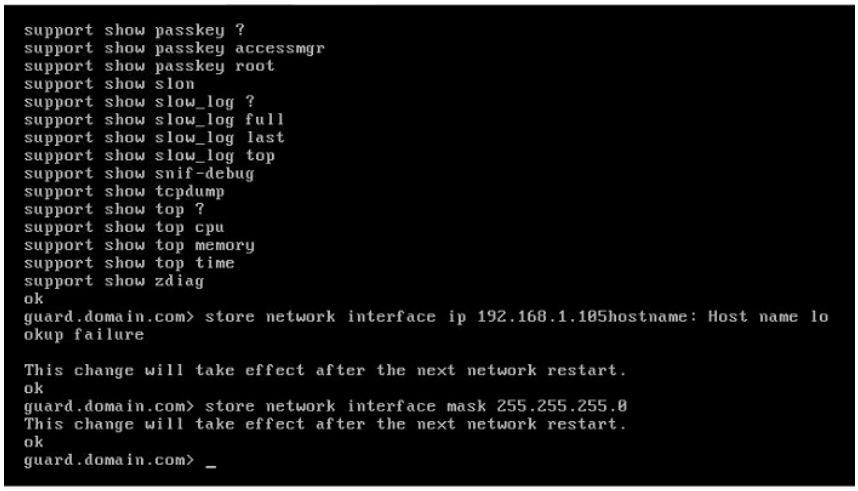


Figure 7. Ingreso de dirección ip y máscara de red

Ingresamos el Gateway de la red para la ruta por defecto, como se presenta en la siguiente imagen por medio del comando.

Store network routes def <default_route_ip>

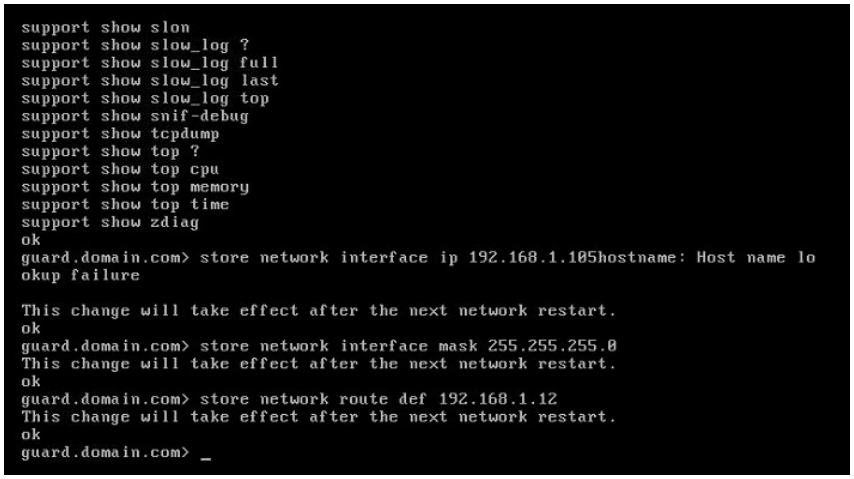


Figure 8. Ingreso del Gateway de la red

Ingresamos la dirección IP correspondientes a los DNS, como se presenta en la siguiente imagen. El primero es requerido, los otros son opcionales)

Store network resolver 1 <dns_server_ip_1>

Store network resolver 1 <dns_server_ip_2>

Store network resolver 1 <dns_server_ip_3>

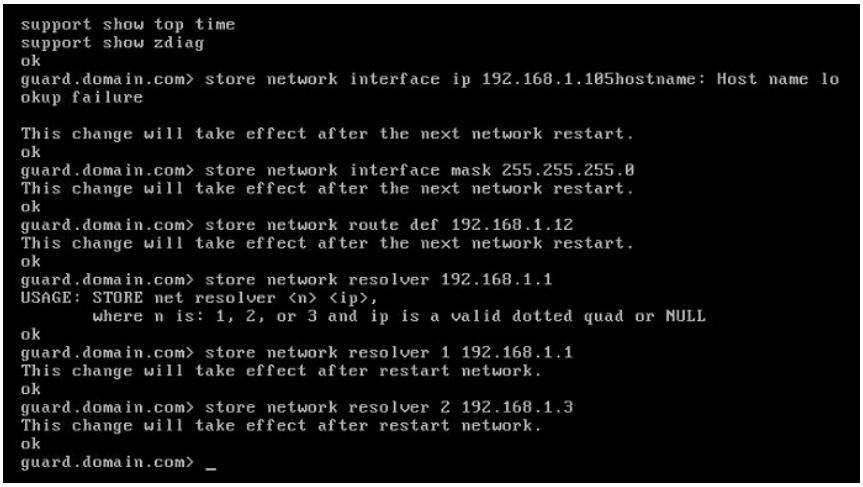


Figure 9. Ingreso de DNS

Ingresar el nombre de host y dominio, como se presenta en la siguiente imagen por medio del siguiente comando

Store System hostname <host_name>

Store System hostname <domain_name>

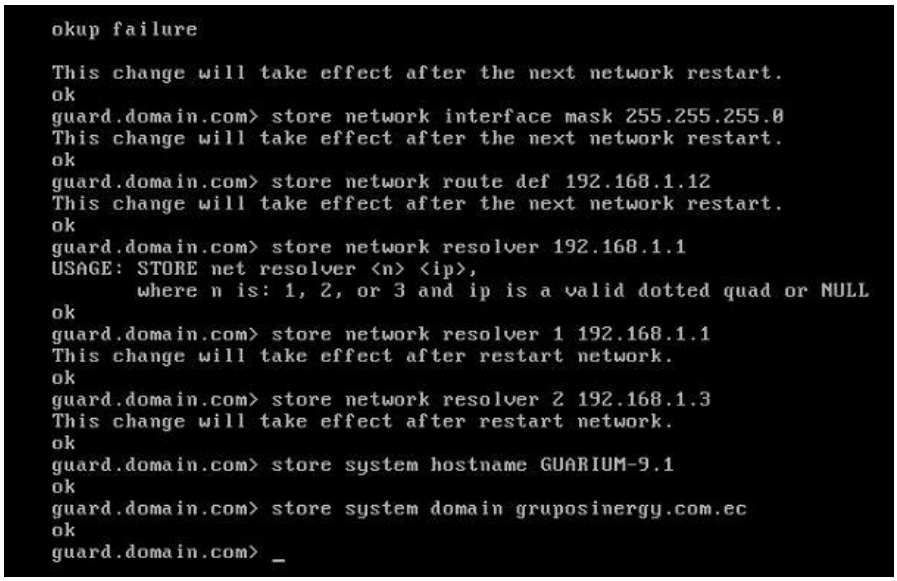


Figure 10. Nombre de host y Dominio

Ingresar la dirección IP del servidor NTP y habilite el servidor, como se ve en la siguiente imagen por medio del siguiente comando store system ntp servere

Figure 11. Activación del servidor NTP

Validación de las configuraciones de red realizadas, como se ve en la siguiente figura por medio de los siguientes comandos.

Show network interface all

Show network routes defaultroute

Show network resolver all

Show System hostname

Show System domain

Show System ntp all

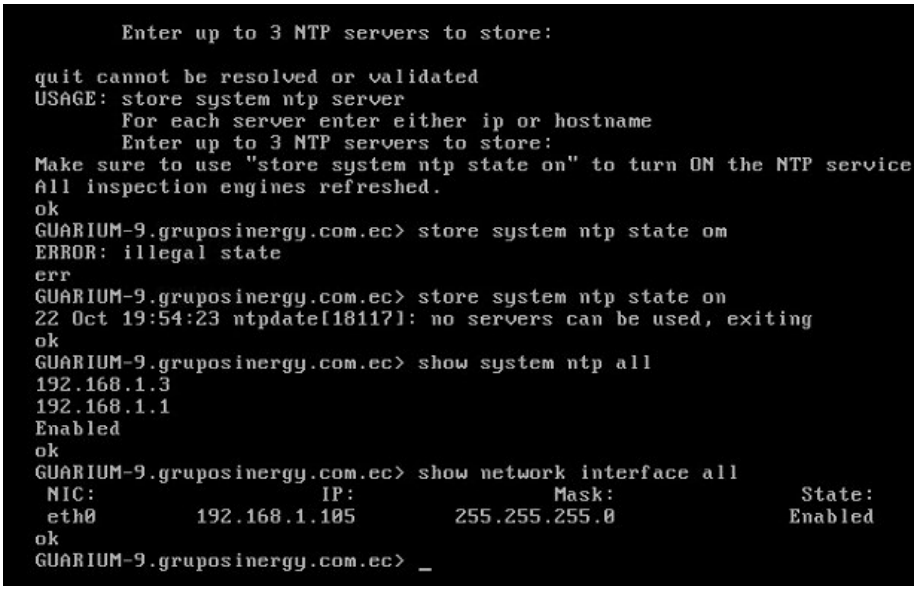


Figure 12. Validación de confirmaciones

Se realiza el reinicio del equipo Guardium para que las configuraciones se efectúen, por medio del comando

Restart system

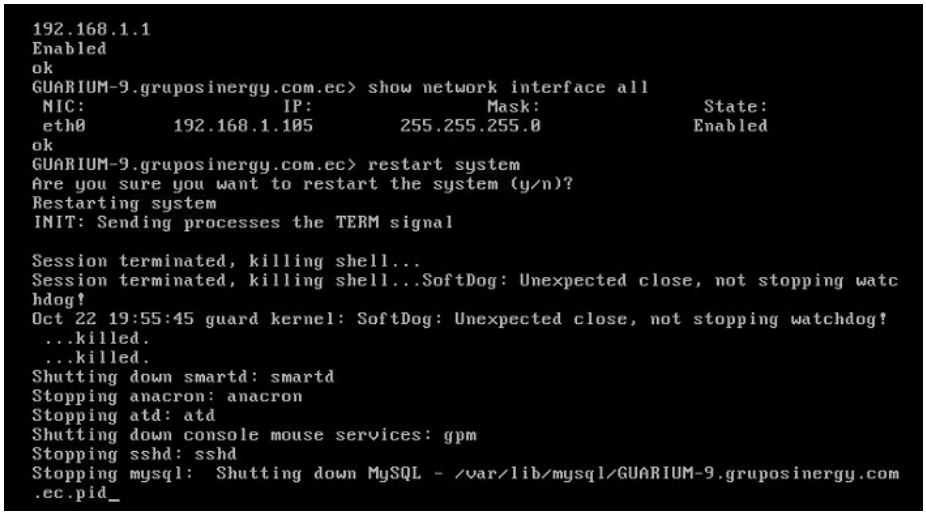


Figure 13. Reinicio del equipo Guardium

3.2.3. Configuración de fecha y hora del equipo.

El colector debe sincronizarse con la hora del servidor donde se está ejecutando para que no se presenten anomalías en la transmisión de la información y los reportes, notificaciones, alertas puedan ser observadas en el tiempo real.

Visualizamos y cambiamos zona horaría. Visualizamos la zona actual show (System clock timezone) cargada por defecto si es incorrecta desplegamos las opciones (store System clock timezone list) para escoger la correcta, así, ingresar con el comando store System clock timezone <seleccione la zona horaria>

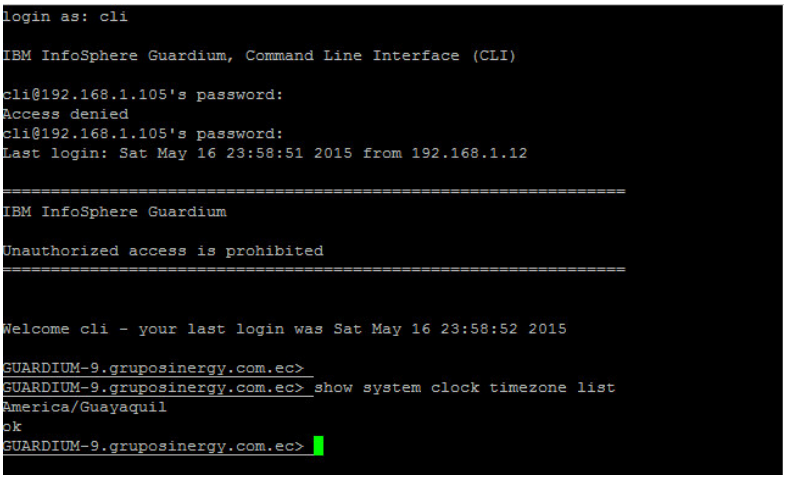


Figure 14. Establecer zona horaria en el equipo Guardium

3.3. Bases de Datos soportadas

Por su alta capacidad de adaptarse a ambientes heterogéneos y su escalabilidad, IBM Infosphere Guardium soporta una amplia lista de motores y versiones de bases de datos.

La base de datos que se protegerá es Microsoft SQL Server 2008

Table 1. Bases de Datos soportadas por Guardium. (IBM, 2015).

Base de datos	Versiones soportadas
Oracle (including ASO/SSL)	9i, 10g (r1, r2), 11gR1, 11gR2, 12c (12c Restrictions: Monitoring support for Windows, Linux, Solaris, HP-UX, AIX only. No support for SSL encryption. ASO support available only on Linux and Solaris.)
Oracle RAC (including ASO/SSL)	10g, 11g, 11gR2, 12c (12c Restrictions: Monitoring support for Windows, Linux, Solaris, HP-UX, AIX only. No support for SSL encryption. ASO support available only on Linux and Solaris.)
Oracle Exadata (including ASO/SSL)	11gR2, 12c (12c Restrictions: Monitoring support for Windows, Linux, Solaris, HP-UX, AIX only. No support for SSL encryption. ASO support available only on Linux and Solaris.)
Microsoft SQL Server	MS SQL Cluster, 2000, 2005, 2008, 2008 R2, 2012, 2014
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, UNIX)	9.1, 9.5, 9.7, 10.1, 10.5 (including BLU acceleration)
IBM DB2 (Windows)	9.1, 9.5, 9.7, 10.1, 10.5
IBM DB2 Purescale	9.8, 10.1, 10.5

Continua

IBM PureData System for Transactions	
IBM PureData System for Operational Analytics	
IBM PureData Systems for Analytics	
IBM DB2 for z/OS	8, 9, 10, 11, 11.3
IBM DB2 for i	6.1, 7.1, 7.2
IMS	11, 12. 13
VSAM	see OS version support, part of z/OS (not separately versioned)
IBM Informix	11.50, 11.70, 12.10
Sun MySQL and MySQL Cluster	5.0, 5.1, 5.5, 5.6
Sybase ASE	15, 15.5, 15.7 (SSL encryption not supported)
Sybase IQ	15.0, 15.1, 15.2, 15.3, 15.4, 16 (Sybase IQ does not support SSL for any platform)
IBM Netezza	4.6, 4.6.8, 5,0, 6.0, 6.02, 7.0, 7.1, 7.2
PostgreSQL	8, 9, 9.1, 9.2
Teradata	12, 13, 13.10, 14, 14.10, 15

Continua

IBM InfoSphere BigInsights	1.4, 2.0, 2.1, 2.1.2, 3.0
Cloudera	CDH3 Update 2, 3, 4 CDH4.x, CDH5.x
Aster	5, 6
Cassandra	1.2.x
CouchDB	1.2.x
Greenplum DB	4.0, 4.1, 4.2, 4.3
Greenplum (Pivotal) HD	1.2, 1.5
Horton Works	1.x, 2.x, 2.2
MongoDB	2.0, 2.2, 2.4, 2.6
SAP HANA	1.0
FTP	
Window File Share (WFS)	Windows 2003, 2008
Hadoop 1.x is used with the following distributions:	Cloudera 4.x Hortonworks 1.x IBM BigInsights 2.1 Pivotal (Greenplum) HD 1.2
Hadoop 2.x is used with the following distributions:	Cloudera 5.x Hortonworks 2.x BigInsights 2.1.2 and 3.0 Pivotal 1.5

3.4. Instalación

3.4.1 Métodos de instalación.

La instalación del sistema Guardium se detallan los pasos necesarios para instalar y configurar el sistema IBM Infosphere Guardium.

IBM Infosphere Guardium está disponible como:

Hardware: Es una solución de software totalmente configurada en los equipos proporcionados por el fabricante.

Software: La solución es entregada en imágenes que se instalará en equipos físicos o virtuales.

Los pasos son:

- Se ensambla la información de configuración y el hardware necesario antes de empezar.
- La configuración del dispositivo puede ser física o virtual.
- Instala la imagen de IBM Infosphere Guardium.

Figure 15. Ventana de instalación

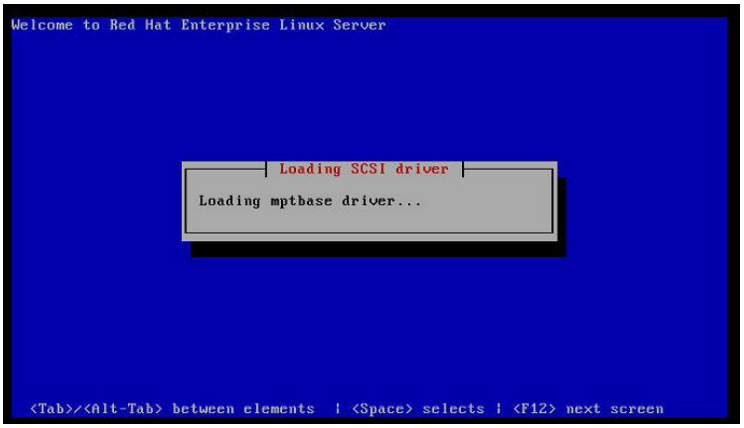


Figure 16. Cargando el driver

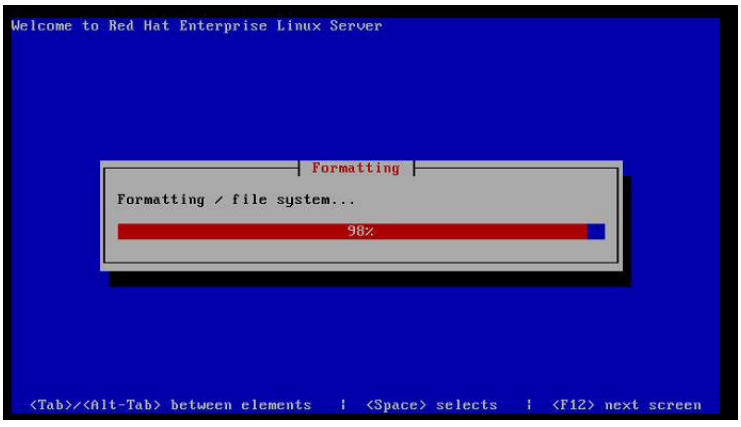


Figure 17. Formating

- Realice Configure las configuraciones iniciales y básicos.

El colector cuenta con una consola de administración gráfica, la cual es presentada por medio de un browser.

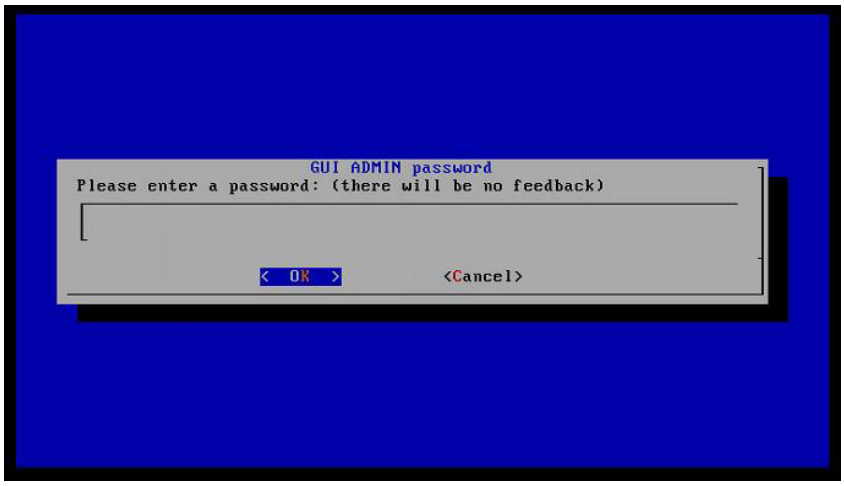


Figure 18. Clave para el usuario Admin

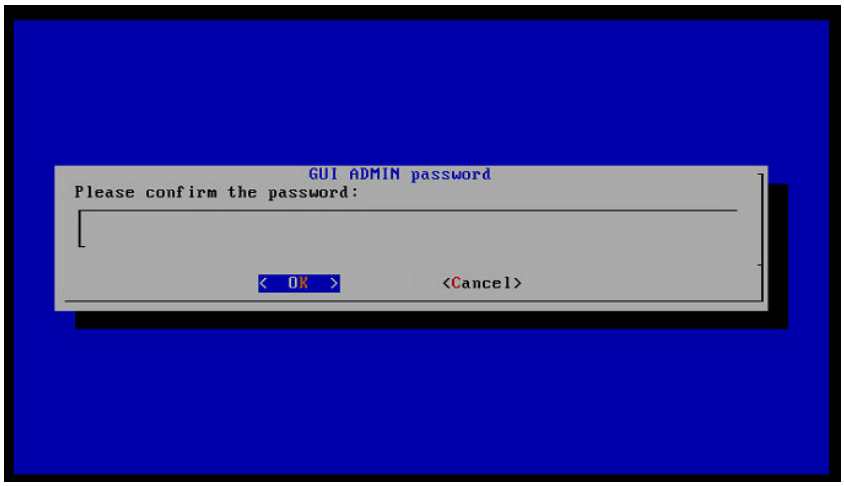


Figure 19. Confirmación de la clave para el usuario Admin

El usuario Access Manger, es un usuario donde se definirán los roles y aplicaciones a los cuales tendrán acceso los siguientes usuarios que se configuren de acuerdo a las necesidades que se vayan presentando.

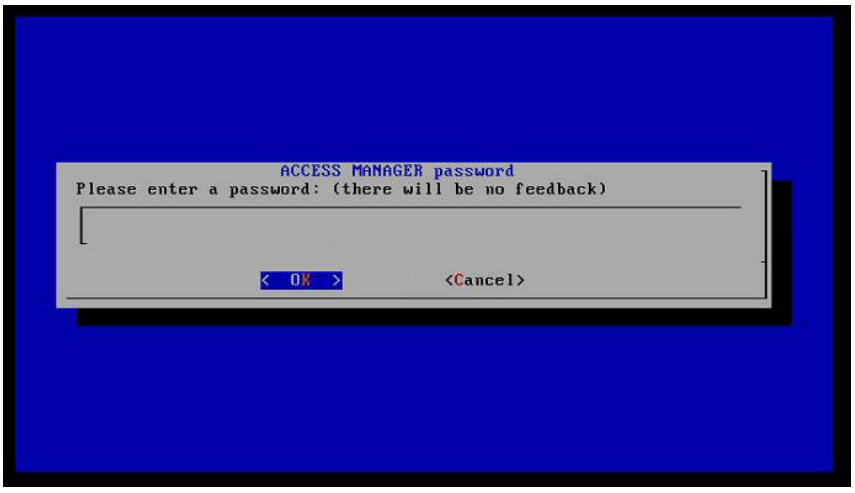


Figure 20. Clave para el usuario accessmgr

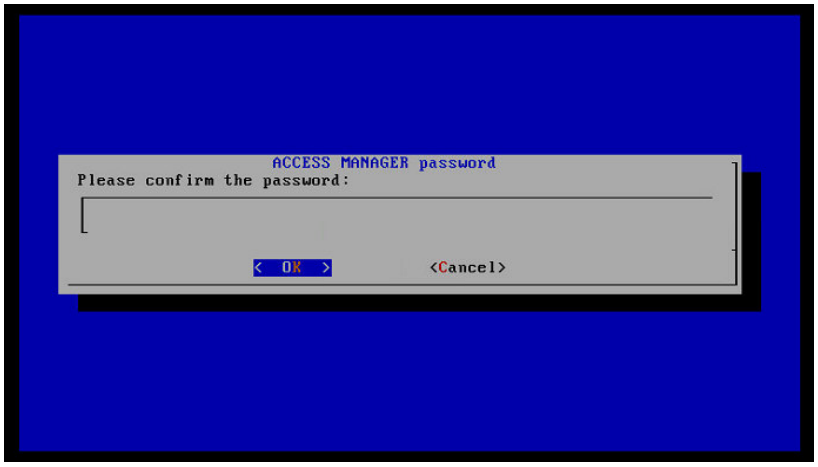


Figure 21. Confirmación de la clave para el usuario Access Manager

Guardium por su alta capacidad de adaptarse a ambientes heterogéneos, cuenta también con la escalabilidad, cuenta con funciones del tipo Colector, Agregador y Administración Central. Siendo una configuración sencilla, el equipo Guardium toma la figura de “Colector”

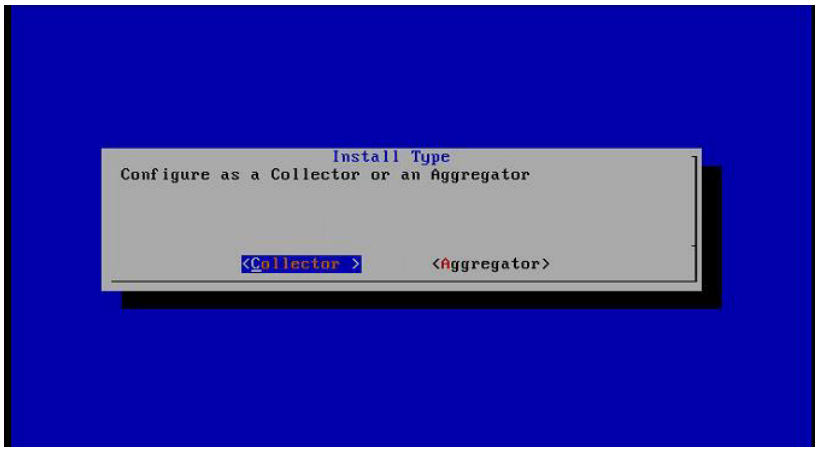


Figure 22. Guardium tipo colector

- Verificación de la instalación exitosa.

3.4.2 Instaladores.

SinergyTeam es un asociado de negocios para IBM, cuenta con acceso al portal Partner World, página donde se descargan los instaladores para crear ambientes de pruebas y desarrollo.

La solución requiere productos claves para habilitar las características instaladas a través de la interfaz de la aplicación. Los siguientes tipos son:

- Base key
- Appended Key

La Base key es también conocida como como una clave de reset y define el tipo de equipo que se utilizará, nuestra implementación es para un equipo colector.

La Append key requiere de una “base key” para ser instalada Múltiples appender key pueden ser aplicadas, estas están disponibles para las siguientes características:

- DAM Standard
- DAM Avanzada
- VAM Standard
- VA Avanzada

El DAM, se encarga del seguimiento, elaboración de informes y alertas en tiempo real de todas las actividades de acceso y extrusión que se observan.

La evaluación de la vulnerabilidad básica (VA) se centra en la vulnerabilidad de funcionamiento de los procesos de evaluación en contra de las bases de datos para informar sobre el nivel de seguridad de las bases de datos. La evaluación de la vulnerabilidad avanzada añade más componentes de seguridad impulsada por productos, tales como configuración de sistemas de auditoría (CAS) y Derecho de Información. CAS explora los archivos de configuración, directorios y otros componentes críticos externos de bases de datos y alertas sobre los cambios que podrían afectar la seguridad y la integridad de las bases de datos. Informes de informes Derecho y sigue los cambios en el derecho cuenta de usuario de base de datos sobre las diversas bases de datos.

3.4.3 Configuración de Inspection Engine.

El motor de inspección supervisa el tráfico entre el servidor y el equipo Guardium utilizando el protocolo de base de datos específica.

El motor de inspección extrae SQL de paquetes de red; compila analiza e identifican oraciones, peticiones, órdenes, objetos y campos; y registros detallados información sobre ese tráfico a una base de datos interna.

Puede configurar y arrancar o parar varios motores de inspección en el equipo Guardium.

Motores de inspección también se definen en el S-TAP. Si S-TAP informe a este aparato Guardium, asegúrese de que el aparato no supervisa el mismo tráfico que el S-TAP®. Si eso sucede, el motor de análisis se reciben paquetes duplicados, no será capaz de reconstruir los mensajes, y no hará caso de que el tráfico.

Cada motor de inspección supervisa el tráfico entre una o más de cliente y servidor de direcciones IP. En una definición motor de inspección se definen mediante una dirección IP y una máscara. Usted puede pensar en una dirección IP como un solo lugar y una máscara como un mecanismo de comodín que le permite definir un rango de direcciones IP.

Seleccione la Consola de administración> Motores de inspección.

Haga clic en Aplicar para guardar la configuración del sistema actualizado cuando haya terminado de hacer cambios.

Opcionalmente añadir comentarios a la Configuración del motor de Inspección.

Haga clic en Reiniciar Motores de inspección.

Los cambios aplicados no tendrán efecto hasta que se reinicien los motores de inspección. Después de aplicar los cambios de configuración del motor de inspección, haga clic en el botón Reiniciar para detener y reiniciar el sistema (utilizando los nuevos valores de configuración).

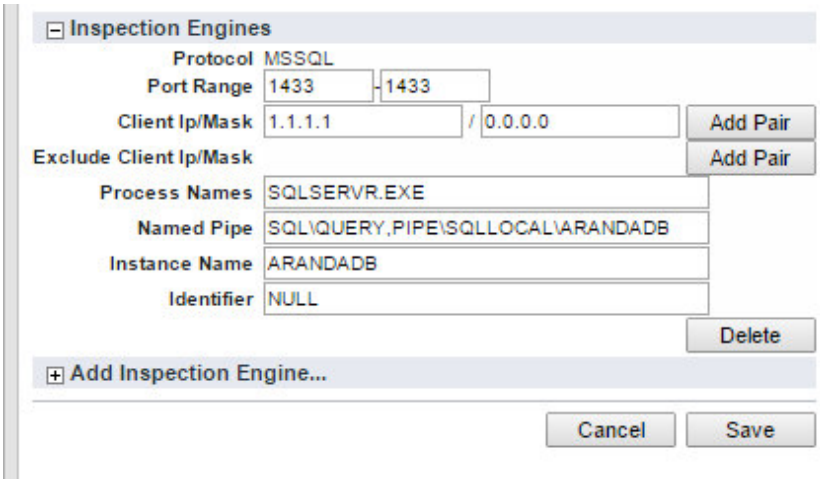


Figure 23. Configuración del Inspection engines

3.5. Configuración del software

3.5.1 Descubrimiento de la base de datos.

Guardium realiza un descubrimiento del entorno de base de datos. A través de la interfaz de usuario basada en web, que proporciona un informe de todas las bases de datos ubicadas en la red y las listas de la dirección, el tipo y el puerto en el que se encuentran estos sistemas. Esta importante información se puede utilizar como un mecanismo para identificar donde los agentes Installation Manager Guardium (GIM) S-TAP o requieren el despliegue.

3.5.1.1 Configuración Auto-Discovery.

Realizamos un escaneo de toda la red para contabilizar las bases de datos que se encuentran en toda lred incluso las que se encuentran en el servidor donde estás protegiendo la base de datos.

- Definimos un nombre al proceso de autodescubrimiento
- Definimos el segmento de red o solamente la IP donde deseamos ejecutar la revisión
- Definimos un rango de puertos donde creemos que se encuentran trabajando el motor de la base de datos

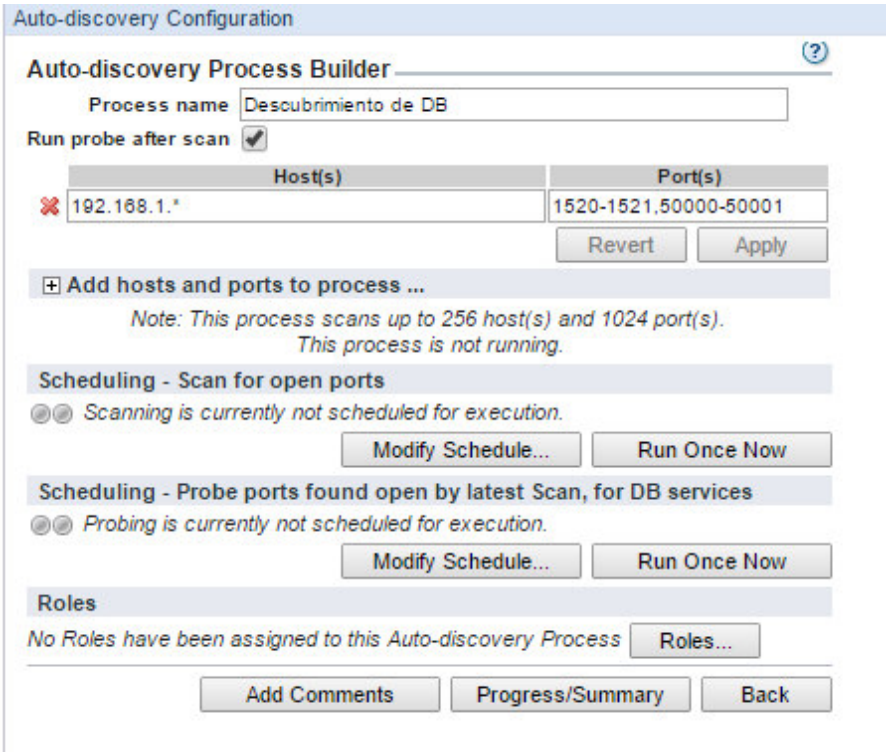


Figure 24. Pantalla de configuración de parámetros

3.5.1.2 Escaner de la base de datos.

Un trabajo de escaneado escanea cada host, y compila una lista de puertos abiertos de la lista de puertos especificados para ese host. Un trabajo de digitalización se debe ejecutar antes de ejecutar el segundo tipo de trabajo.

Un trabajo de investigación utiliza la lista de puertos abiertos compilados durante la última exploración única completado. El trabajo de la sonda determina si hay servicios de bases de datos que se ejecutan en esos puertos. Puede ver los resultados de este trabajo en las bases de datos descubiertos

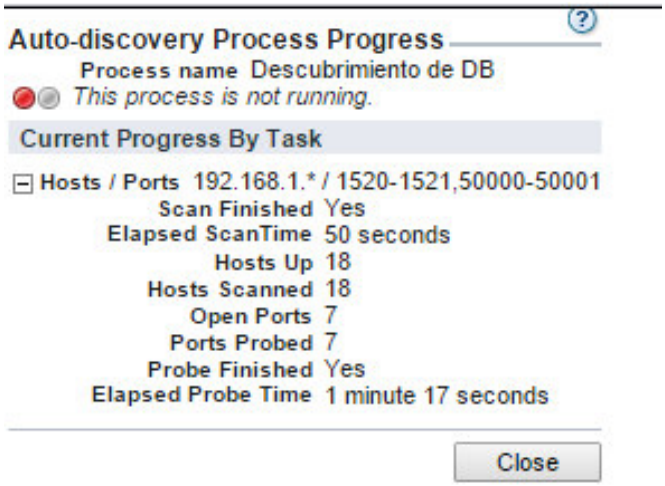


Figure 25. Pantalla del progreso de Autodescubrimiento

3.5.1.3 Reporte.

En la pestaña Daily Monitor, seleccionamor la funcionalidad de Database Discovered. Ahora tenemos un reporte de la base de datos que estamos escaneando.

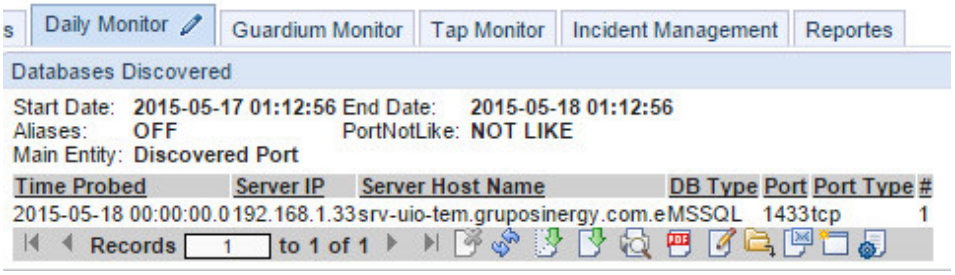


Figure 26. Reporte del proceso para el descubrimiento de la base de datos

3.5.2 Clasificación de la información.

El clasificador de la información es una característica de Guardium que ofrece la función para encontrar y clasificar los datos sensibles.

Módulo clasificador de Guardium descubre y clasifica automáticamente los datos sensibles dentro la base de datos. El clasificador utiliza un rastreador base de datos inteligente para buscar de manera eficiente los patrones personalizables, basado en expresiones regulares.

3.5.2.1 Políticas de Clasificación.

Una política de clasificación es un conjunto de reglas destinadas a descubrir y elementos sensibles de la etiqueta de datos (tablas de bases de datos o archivos). Se puede definir un conjunto de acciones que deben tomarse para cada regla. Una acción podría ser la de generar una alerta de correo electrónico, o para añadir un miembro a un grupo. Cada vez que una regla se cumple, que se registra el suceso, y por lo tanto se puede informar al menos que ignore se especifica como la acción a tomar, en cuyo caso no hay ningún registro de esa regla.

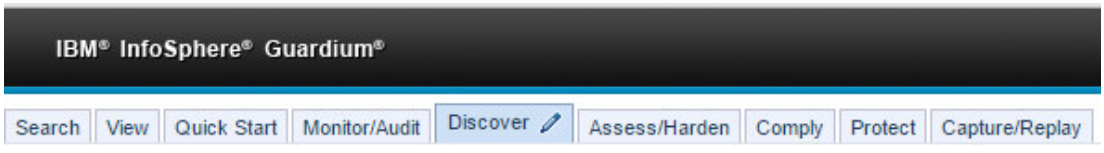


Figure 27. Pestaña Discover

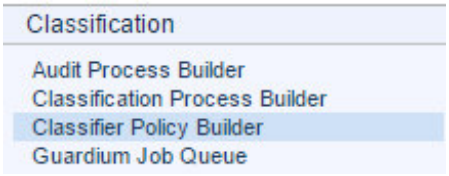


Figure 28. Classifier Policy Builder

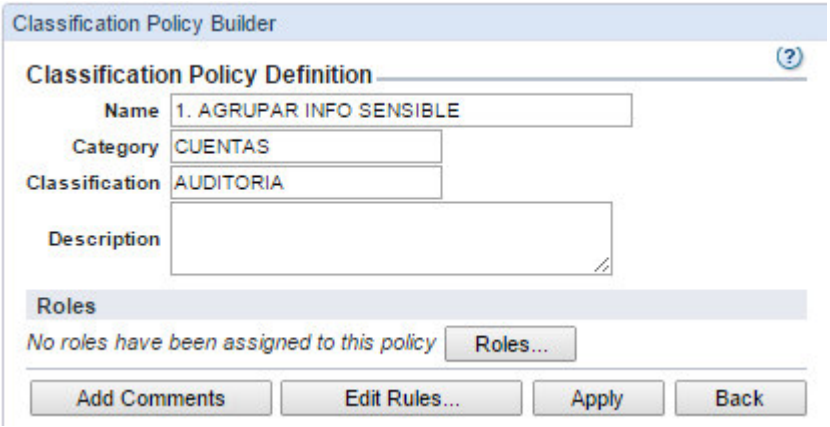


Figure 29. Definición política de Clasificación

3.5.2.2 Reglas de las políticas.

Define lo que se está buscando, como buscar y que acciones tomar si un objeto es encontrado.

- Catalog Search: Busca el catálogo de la base de datos por nombre de tabla o columna
- Search by permission: Busca for el tipo de acceso que ha sido garantizado a usuarios o reles.
- Search for data: Es la coincidencia de valores o patrones en la información
- Search for Unstructured Data: Coincidencia específica de valores o patrones en un archivo de data no estructurada.

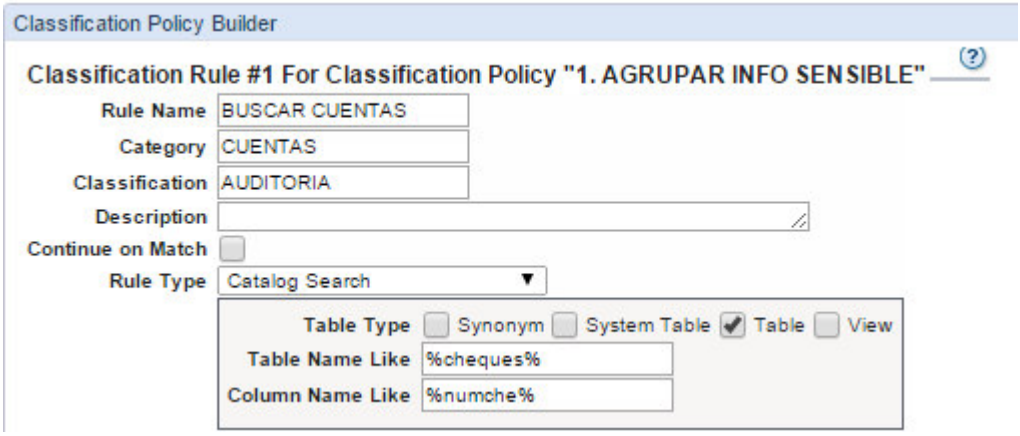


Figure 30. Classification Rule

3.5.2.3 Acciones de la clasificación.

Acciones que se tomaran cuando la data enocntrada

- Agregar a un grupo de objetos: Puede ser usado en data estructurada y archivos de datos no estructurados
- Agregar a un grupo de objetos: Un miembro será agregado a un grupo de objeto seleccionado
- Crear regla de acceso: Una regla de acceso será insertada a dentro de una política de seguridad definida
- Ignorar: No registra la coincidencia y no toma acciones adicionales
- Registro de resultados: Registra la coincidencia, y no toma acciones adicionales
- Envío de alerta: Una alerta se enviará a uno o más receptores

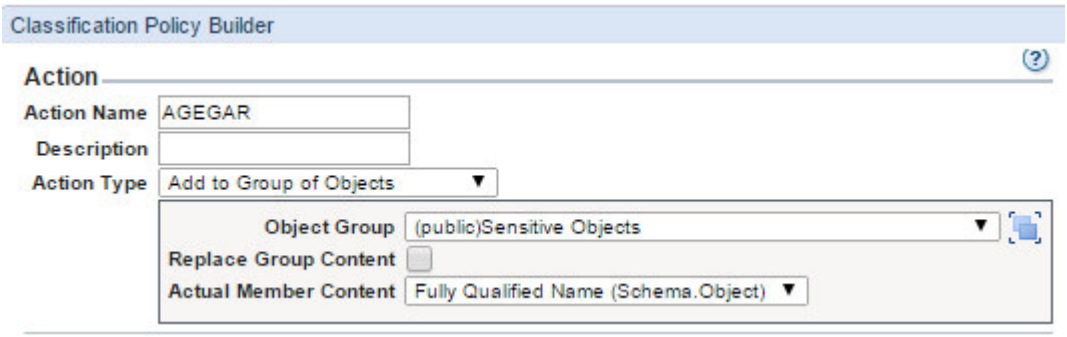


Figure 31. Acción de la regla

3.5.2.4 Clasificación del proceso.

Un proceso de clasificación define un trabajo que consiste en una política de clasificación y una o más fuentes de datos. El proceso puede ser presentado para ser ejecutado una vez, o puede ser programada para ejecutarse de forma periódica, como una tarea en un proceso de automatización del flujo de trabajo de cumplimiento.

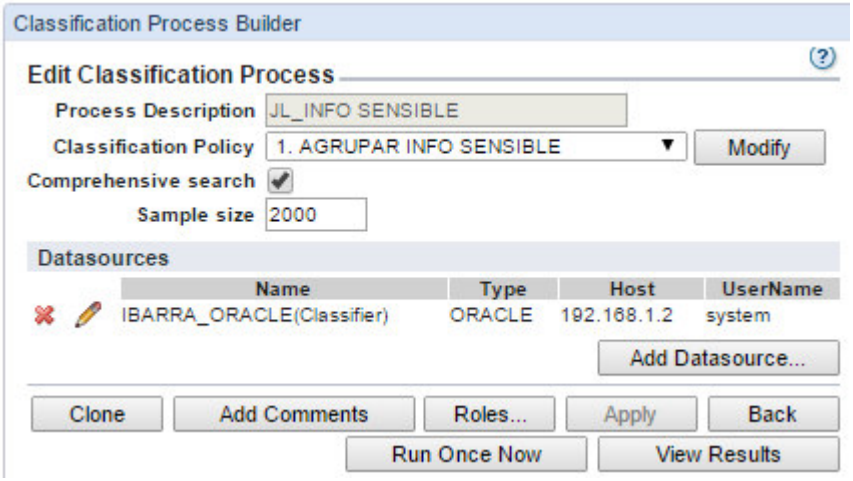


Figure 32. Classification Process Builder

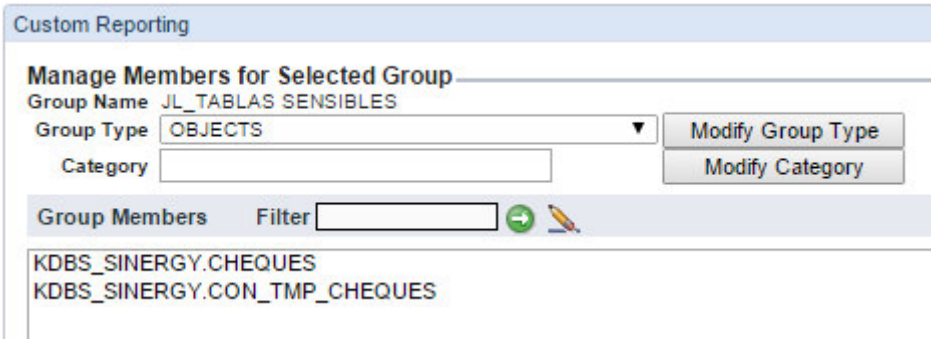


Figure 33. Grupo de objetos sensibles

3.5.3 Políticas de seguridad y logging.

Auditar la base de datos significa controlar y registrar todas las sentencias SQL, la configuración de cambios, y otras operaciones dirigidas contra el servidor de datos para su posterior consulta. Auditar el servidor de datos es a menudo un requisito de cumplimiento y también es una buena práctica para mantener seguro los datos en el servidor. Sin auditoría servidor de datos, sería casi imposible de confirmar quién es la realización de lo que las funciones de un servidor de datos. Guardium tiene un amplio conjunto de funciones para ayudarle con la auditoría de servidor de datos. Estas funciones pueden ayudar a las organizaciones a cumplir con los mandatos legales, y también puede ayudar a mantener los datos bien gobernados y seguros.

3.5.3.1 Políticas de seguridad.

Una política de seguridad contiene un conjunto ordenado de reglas que deben aplicarse al tráfico observado entre clientes y servidores de bases de datos. Cada regla puede aplicarse a una petición de un cliente, o para una respuesta de un servidor. Las

políticas pueden definir múltiples y múltiples políticas se pueden instalar en un dispositivo Guardium al mismo tiempo.

3.5.3.2 Reglas.

Una violación de la política se registra cada vez que una regla se activa (excepto cuando el Estado pida explícitamente ningún registro). Opcionalmente, el SQL que activa la regla (incluyendo los valores de datos) se puede grabar con la violación de la política. Violaciones de política se pueden asignar a los incidentes, ya sea de forma automática mediante un proceso, o manualmente por los usuarios autorizados (ver en la ficha Gestión de Incidentes en la GUI Guardium. Para más información, consulte Gestión de Incidentes

3.5.3.3 Acciones.

Cada regla de una política define una acción condicional. La condición probada puede ser una prueba simple - por ejemplo, se podría comprobar si hay acceso desde una dirección IP del cliente que no pertenece a un grupo de direcciones IP de cliente autorizado. O la condición probada puede ser una prueba compleja que considera mensaje múltiple y atributos de sesión (usuario de base de datos, programa de fuente, tipo de comando, hora del día, etc.), y puede ser sensible al número de veces que la condición se cumple dentro de un periodo de tiempo indicado.

La acción desencadenada por la regla puede ser una acción de notificación (correo electrónico a uno o más destinatarios, por ejemplo), una acción de bloqueo (la sesión de cliente podría ser desconectado), o el evento podría simplemente estar conectado como una violación de la política. Las acciones personalizadas se pueden desarrollar

para llevar a cabo las tareas necesarias para las condiciones que pueden ser exclusivos de un entorno o aplicación determinada. Para obtener una lista completa de acciones, véase la Regla acciones Descripción general a continuación.

3.5.3.4 Instalación de la política de seguridad.

Más de una política instalada se permite al mismo tiempo. Todas las políticas instaladas están disponibles para la acción. Existen limitaciones: las políticas definidas como políticas de auditoría selectivos no se pueden mezclar con las políticas que no se definen como políticas de auditoría selectivos, y las políticas definidas como registro de plano no se puede mezclar con políticas que no se definen como log plana. Si se trata de mezclar las políticas, un mensaje de error se traducirá al instalar estas políticas mixtas.

3.5.3.5 Configuración de Inspection Engine.

El motor de inspección extrae SQL de paquetes de red; compila analizar árboles que identifican oraciones, peticiones, órdenes, objetos y campos; y registros detallados información sobre ese tráfico a una base de datos interna.

Motores de inspección también se definen en el S-TAP. Si S-TAP informe a este aparato Guardium, asegúrese de que el aparato no supervisa el mismo tráfico que el S-TAP. Si eso sucede, el motor de análisis recibe paquetes duplicados, no será capaz de reconstruir los mensajes, y no hará caso del tráfico

3.5.4 Correlación de Alertas.

Una alerta de correlación se desencadena por una consulta que mira hacia atrás durante un período de tiempo especificado para determinar si el umbral de alerta se ha cumplido. El Guardium Anomaly Detection Engine ejecuta consultas de correlación de forma programada. De forma predeterminada, las alertas de correlación no registran violaciónes de política, pero pueden ser configurados para hacer eso.

Figure 34. Pestaña Tools

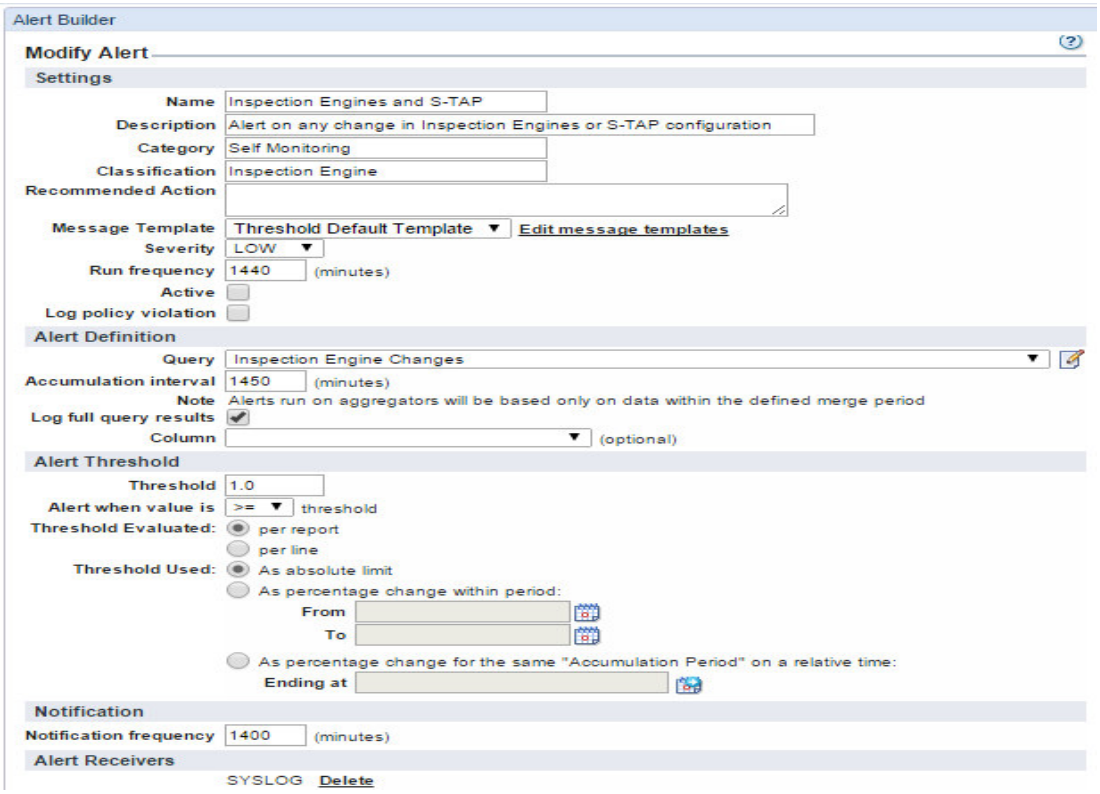


Figure 35. Alert on any change in inspection Engines or S-TAP configuration

3.5.4.1 Tipos de notificación.

El componente Guardium de alerta, contiene los siguientes mecanismos de notificación:

SMTP - El servidor SMTP (correo saliente). La alerta pasa mensajes de correo electrónico estándar para el servidor SMTP para el que se ha configurado.

SNMP - El SNMP (información de la red y el control) del servidor. Cuando se selecciona SNMP para una notificación de alerta, la alerta pasa todos los mensajes de alerta de ese tipo a la comunidad de captura única para la cual la alerta se ha configurado.

Syslog - La alerta está escrito en syslog en el aparato Guardium (que puede ser configurado por el Administrador Guardium para escribir mensajes syslog a un sistema remoto).

Para SNMP o SYSLOG, la longitud máxima del mensaje es de 3000 caracteres. Cualquier mensaje más largo que se truncarán.

3.5.4.2 Acciones de alertas en tiempo real.

Una alerta en tiempo real se desencadena por una regla de política de seguridad. El componente Guardium motor Inspección dirige la política de seguridad, ya que recoge y analiza el tráfico de base de datos en tiempo real.

3.5.5 S-Gate.

La solución de control de acceso de nivel de datos evita que los usuarios de bases de datos no autorizados realicen acciones específicas, definidas por los usuarios Guardium, en un servidor de base de datos. Un caso de uso común para esta funcionalidad es la prevención de los administradores de bases subcontratados tengan acceso a los datos del cliente, mientras que les permite realizar su actividad autorizada en el día a día.

3.5.5.1 Modo S-GATE.

El primer paso en este proceso es determinar el modo (abierto o cerrado) en la que el S-GATE funcionará. En modo abierto de todas las sesiones no se adjuntarán de forma predeterminada en el modo de cerrado todas las sesiones se adjuntarán de forma predeterminada.

Modo abierto

El S-GATE se habilita mediante una opción en el archivo de configuración del S-TAP (guard_tap.ini). Para activar el SGATE, un administrador del servidor establece el siguiente parámetro FIREWALL_INSTALLED = 1 y se reinicia el S-TAP. Un administrador también puede habilitar el S-GATE desde GIM. Por defecto la entrada FIREWALL_DEFAULT_STATE se establece en 0, lo que significa que el S-GATE se ejecutará en modo "abierto". En el modo abierto, no hay usuarios adjuntos a menos que exista una regla de política explícita para hacerlo. Esto presenta la menor cantidad de riesgo debido a los servidores de aplicaciones sólo se pueden adjuntar a través de las reglas de políticas, que se gestionan fácilmente.

Modo Cerrado

En el modo abierto el primer comando que el colector recibe dispara la acción de la política 'adjuntar'. Dado que el usuario no está adjunto hasta este punto, la sesión no se puede terminar hasta que Guardium recibe un segundo comando. En muchos casos, esto no representa un problema debido a que el cliente de la base de datos emite una serie de comandos en segundo plano al iniciar la sesión que activarán la regla adjuntar, de forma que cuando el usuario realiza su primera petición SQL, la sesión ya ha sido adjuntada.

Sin embargo, en otros ambientes el primer SQL que un usuario ejecuta (por ejemplo, el usuario está ejecutando un comando) es el primer comando que es enviado al colector Guardium. Puesto que el primer comando que se requiere para disparar la regla “adjuntar”, éste comando no podrá ser bloqueado y, por lo tanto, si un usuario al ejecutar el primer comando es un comando no autorizado, no será bloqueado. Pudiera ser que el primer comando SQL sea elegible por el colector de Guardium o no para ser bloqueado, pero esto dependerá de un número de factores, tales como el tipo de servidor de be de datos, la misma base de datos y el modo en que un cliente accede al servidor.

Incluso en los casos en que un comando inicial pudiera no ser bloqueado, muchos clientes continuarán funcionando en el modo abierto porque Guardium contiene otra funcionalidad, como la de almacenar toda la información en el colector y generar alertas en tiempo real, que ayuda a mitigar el potencial de acceso a datos confidenciales.

Sin embargo, debido a las regulaciones, requisitos de auditoría y otros factores, otros clientes no tienen la flexibilidad y eligen el modo cerrado. En el modo cerrado en lugar de adjuntar las sesiones, se toma el camino contrario; todas las sesiones se

adjuntan por defecto y las sesiones o usuarios autorizados no se adjuntarán a través de las reglas de las políticas. Dado que todas las sesiones se unen de forma predeterminada, el primer comando que un usuario ejecute será bloqueado, si no está autorizado.

3.5.5.2 Configuración.

El proceso de prevención de accesos a la base de datos funciona de la siguiente manera:

1.- Un usuario 'adjunto (attached)' emite una petición SQL.

2.- S-GATE, que es un componente de agente de S-TAP de Guardium, intercepta la solicitud y la envía al colector Guardium.

3.- El colector Guardium procesa la petición contra las reglas de política configurada e instalada.

4.- Si la solicitud contiene la acción no autorizada (select * from customer_table, por ejemplo) el aparato Guardium envía un veredicto 'terminar la sesión' al S-GATE.

5.- El S-GATE termina la sesión del usuario y no envía el comando a la base de datos.

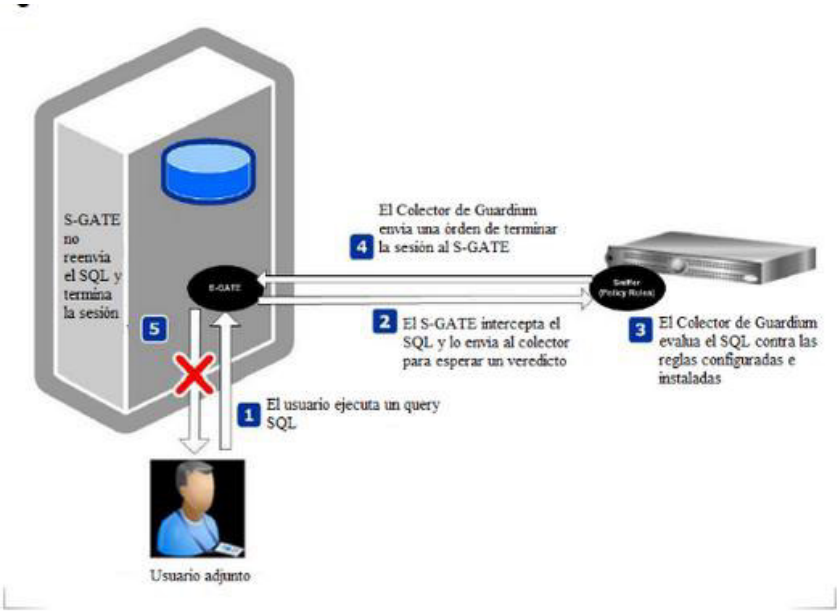


Figure 36. Conexión en modo abierto o cerrado del S-GATE. (IBM Developers Works, 2013).

3.5.5.3 Acciones en reglas de seguridad.

Usando acciones S-GATE en reglas de seguridad. Cuando está en modo abierto asumen que todas las sesiones son seguras. No presenta problemas de latencia.

- S-TAP TERMINATE se utiliza si se produce una excepción o si los datos sensibles se extraen.

- S-GATE ATTACH se utiliza cuando la sesión muestra comportamientos extraños. Ejemplo:

Si la sesión se conecta pasado las horas de trabajo, entonces se aplica el S-GATE y la sesión pasa a modo cerrado. Se observará retrasos y está preparado para S-GATE TERMINATE

- S-GATE TERMINATE se utiliza para terminar la sesión si se producen violaciones graves

Después de S-GATE ATTACH se aplicó. Por ejemplo, si la información del cliente es sensible Consultado el entonces S-GATE Terminar se aplica a la sesión

El modo cerrado por defecto asume que todas las sesiones son sospechosas.

- S-GATE DETACH se utiliza cuando se considera una sesión para estar seguro. Por ejemplo, si el usuario de la sesión de base de datos es parte de los grupos de usuarios de confianza entonces S-GATE es DETACH aplicada a la sesión. Escenarios de modo abierto se aplicarán a partir de este punto.

- S-GATE TERMINATE se puede aplicar sin S-GATE ATTACH desde sesiones que están listas en modo cerrado. El escenario S-GATE TERMIANTE anterior es aplicable

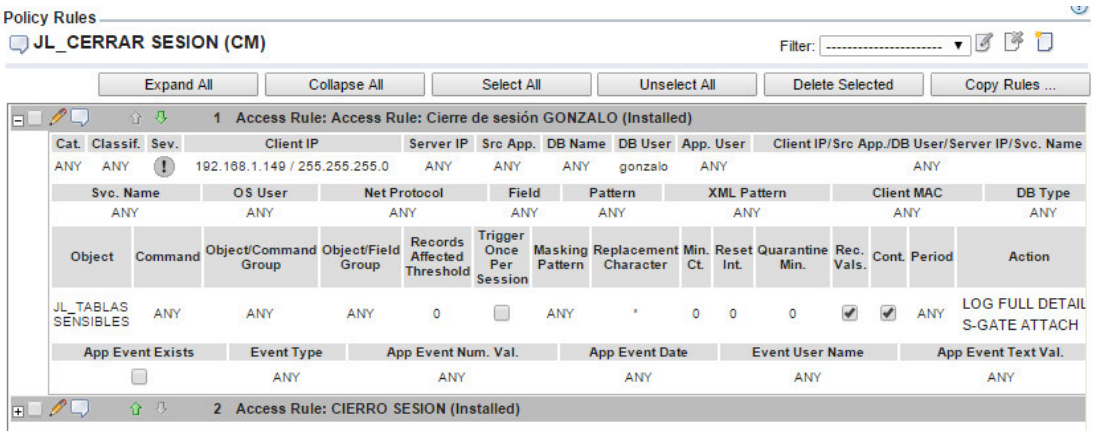


Figure 37. Access Rule: Cierre de sesión Gonzalo

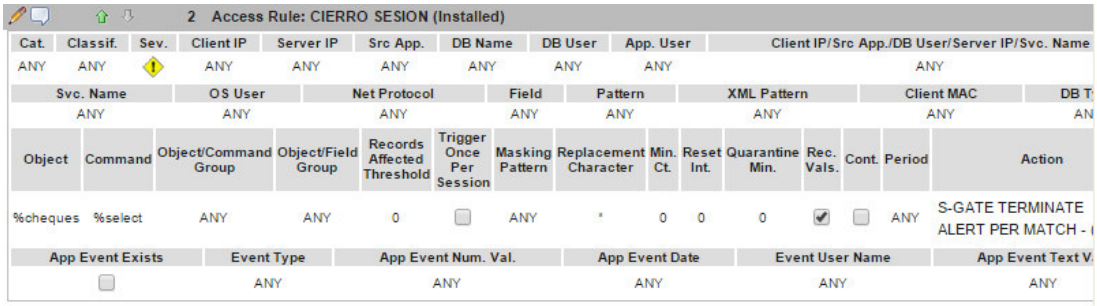


Figure 38. Access Rule: Cierro Sesión

3.6. CÓMO BLOQUEA LAS VULNERABILIDADES, CUÁLES SON LAS CARACTERÍSTICAS DEL SOFTWARE PARA BOQUEARLAS.

La evaluación de seguridad de bases de datos de Guardium examina toda la infraestructura de la base de datos para descubrir vulnerabilidades y ofrece una evaluación actual de la seguridad de su base de datos, utilizando datos históricos y en tiempo real.

Brinda una vasta biblioteca de pruebas pre-configuradas basadas en las mejores prácticas de la industria así como en las vulnerabilidades específicas de la plataforma, que son actualizadas regularmente mediante el servicio de suscripción de Guardium.

También se pueden definir pruebas personalizadas para cubrir necesidades específicas. El módulo de evaluación también señala vulnerabilidades relacionadas al cumplimiento, como el acceso no autorizado a tablas reservadas de Oracle EBS y SAP para cumplimiento con SOX y PCI DSS. Las evaluaciones se dividen en dos amplias categorías:

- Pruebas de vulnerabilidad y configuración verifican si hay vulnerabilidades, como parches faltantes, privilegios mal configurados y cuentas predeterminadas.

● Las pruebas de comportamiento identifican vulnerabilidades basadas en la forma en que se realiza el acceso y el manejo de las bases de datos - como una cantidad excesiva de ingresos negados, clientes que ejecutan comandos administrativos, o ingresos después de horas - supervisando todo el tráfico de la base de datos en tiempo real.

Además de producir informes detallados con capacidad de cambio rápido, el módulo de evaluación genera una tarjeta de informe de salud de la seguridad con medidas evaluadas (Basadas en las mejores prácticas) y recomienda planes concretos de acción para reforzar la seguridad de la base de datos.

3.7. ARQUITECTURA DE LA SOLUCIÓN

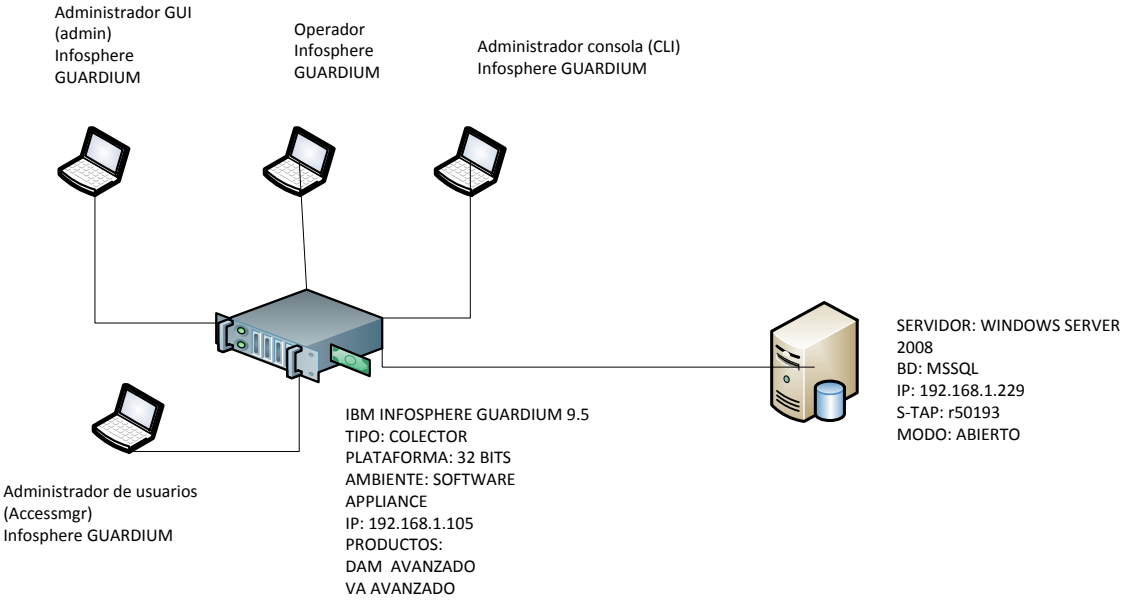


Figure 39. Arquitectura del solución IBM Infosphere Guardium

3.8. PRUEBAS DE VULNERABILIDAD

Por medio del usuario administrador “admin” ingresamos a la consola del equipo Guardium, en la pestaña Tools. Seleccionamos la funcionalidad de evaluación de vulnerabilidades

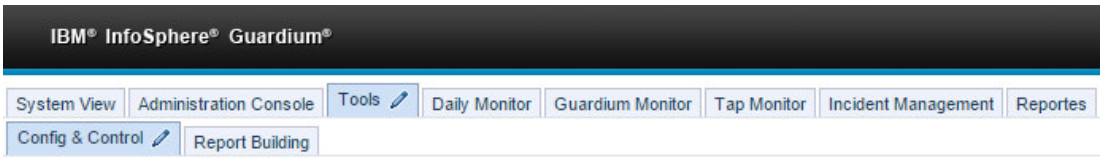


Figure 40. Consola gráfica, Tools

Pulsamos el botón Add Datasource para agregar una base de datos para realizar la evaluación de las vulnerabilidades.

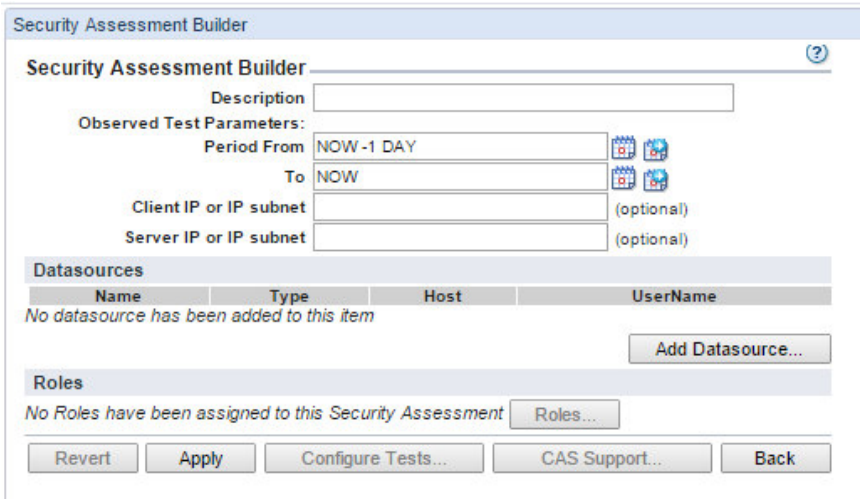


Figure 41. Constructor evaluador de seguridades

Pulsamos el botón New para inciar las nuevas configuraciones de la fuente de datos

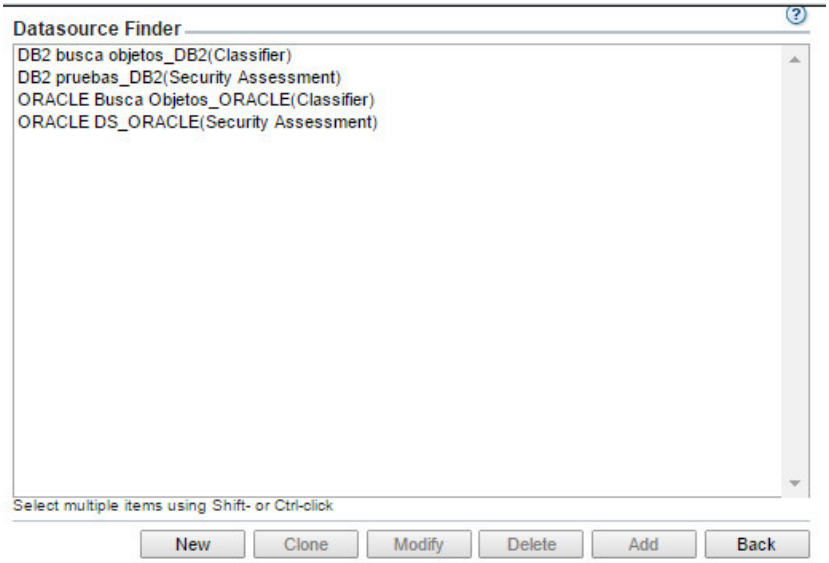


Figure 42. Crear nueva Fuente de datos

Definimos un nombre a la fuente de datos, escogemos el tipo de base de datos que se requiere evaluar, asignamos credenciales de acceso, puerto de comunicación y la instancia e la base de datos. Pulsamos el botón Apply y realizamos pruebas de conexión.

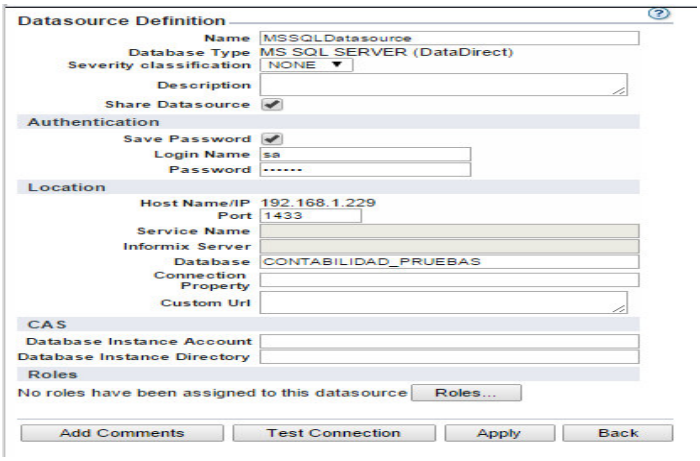


Figure 43. Parametrizando Fuente de datos

Seleccionamos nuestra fuente de datos para agregarla en la lista de evaluación. Pulsamos Add

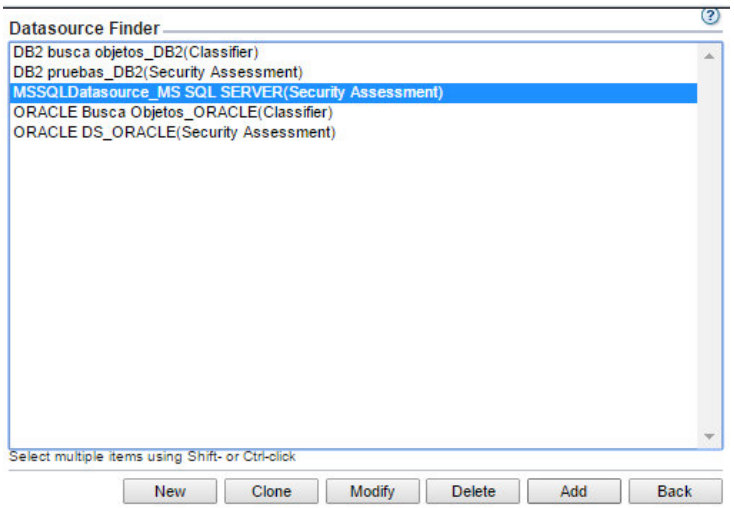


Figure 44. Selección de base de datos

Definimos un nombre a nuestro proceso de evaluación "Vulnerability Assessment"

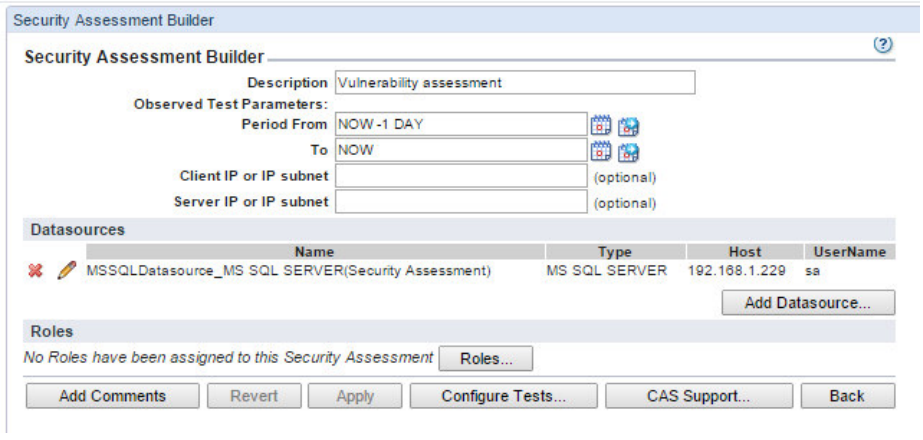


Figure 45. Constructor de evaluación de seguridad

Escogemos el tipo de motor de base de datos, seleccionamos las pruebas que se ejcutaran sobre la base de datos. Add selections

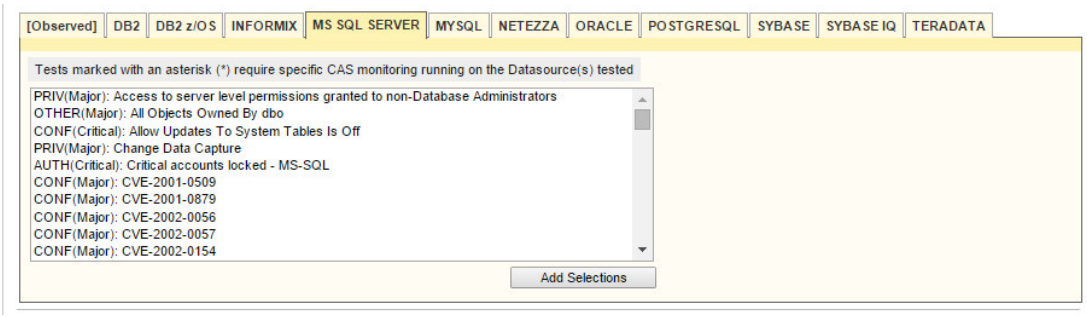


Figure 46. Pruebas para MS SQL SERVER

Se presentan las pruebas que se ejecutaran sobre el motor de base de datos MSSQL SERVER. Ejecutamos le proceso

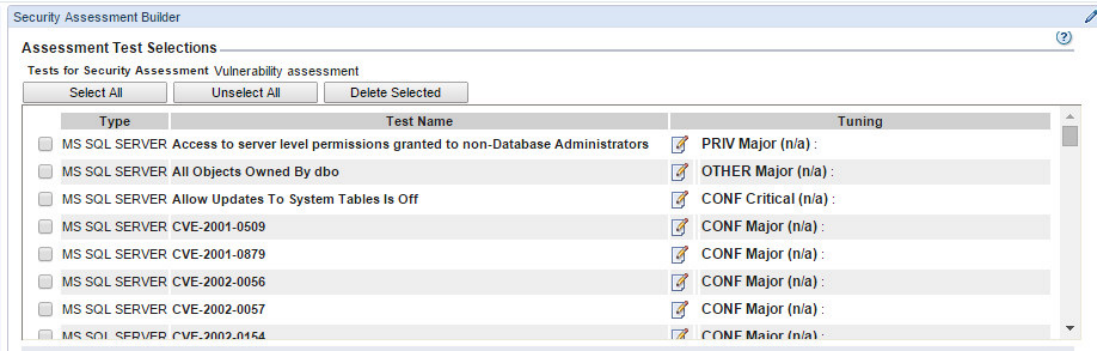


Figure 47. Selección de pruebas para evaluación de base de datos

El estatus del proceso de ejecución puede visualizarse en la pestaña Guardium Monitor

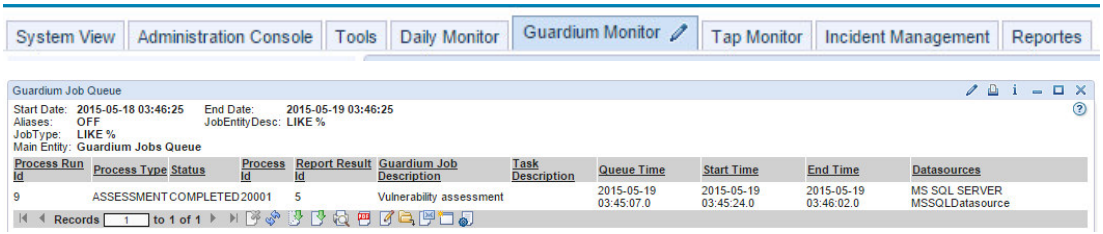


Figure 48. Guardium job Queve

3.9. EFICIENCIA

La solución InfoSphere Guardium Vulnerability Assessment explora infraestructura de la base de datos para detectar vulnerabilidades y sugerir acciones para remediarlas.

La solución permite a las organizaciones eliminar el enorme riesgo generado por las configuraciones de bases de datos no seguras, la falta de parches, un débil sistema de contraseñas y otras vulnerabilidades, y ofrece:

- Cientos de pruebas de vulnerabilidad preconfiguradas, que incluyen prácticas recomendadas de CIS y STIG
- Pruebas estáticas específicas de plataforma que detectan configuraciones no seguras de la base de datos concreta que se está evaluando
- Pruebas dinámicas, lo que permite la detección de vulnerabilidades de comportamiento, como la compartición de cuentas, el exceso de inicios de sesión de administración y la actividad inusual fuera de horas
- Un resumen de la evaluación de seguridad, además de detalles, ordenados según prioridades, que recomiendan medidas correctivas
- El más amplio soporte heterogéneo, que incluye plataformas de bases de datos de ocho proveedores de los principales sistemas operativos

- Pruebas exhaustivas de vulnerabilidad que no se basan en aprovechamientos intrusivos ni en pruebas que puedan afectar a la disponibilidad del sistema, así como información de consulta sobre vulnerabilidades externas, como identificadores de CVE

El resultado de nuestra evaluación de vulnerabilidades es el siguiente reporte, el cual presenta un breve resumen donde hay 5 categorías con estatus de Crítical, Major, Minor, Caution o Info.

La eficiencia de la evaluación de vulnerabilidades es la medida según el resultado en porcentaje. Cuando corregimos según las recomendaciones presentadas por la solución el porcentaje y volvemos a realizar la prueba de vulnerabilidades el valor se incrementa lo cual proyecta el fortalecimiento de la base de datos.

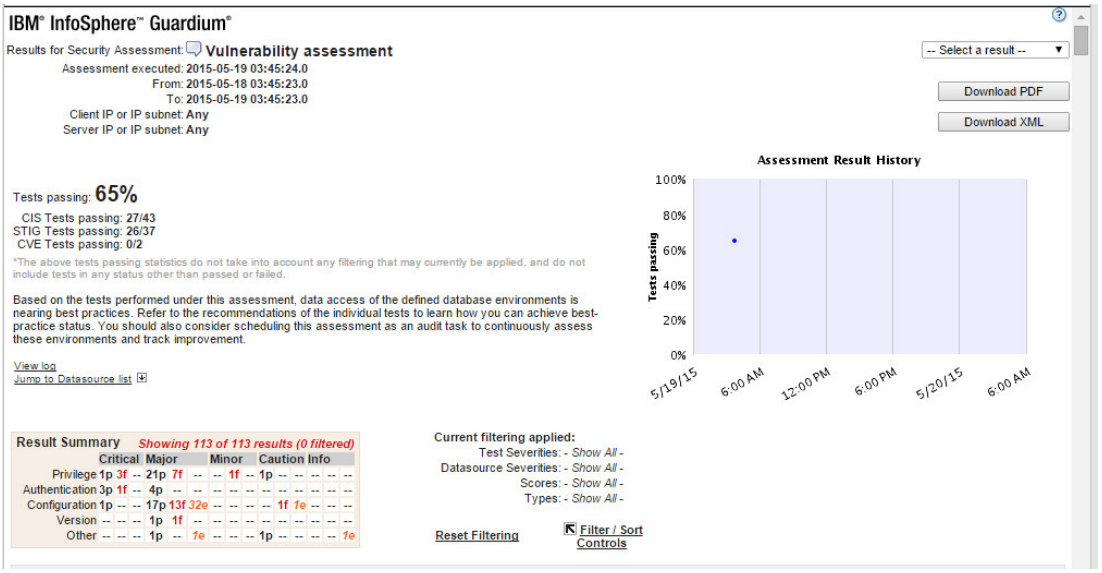
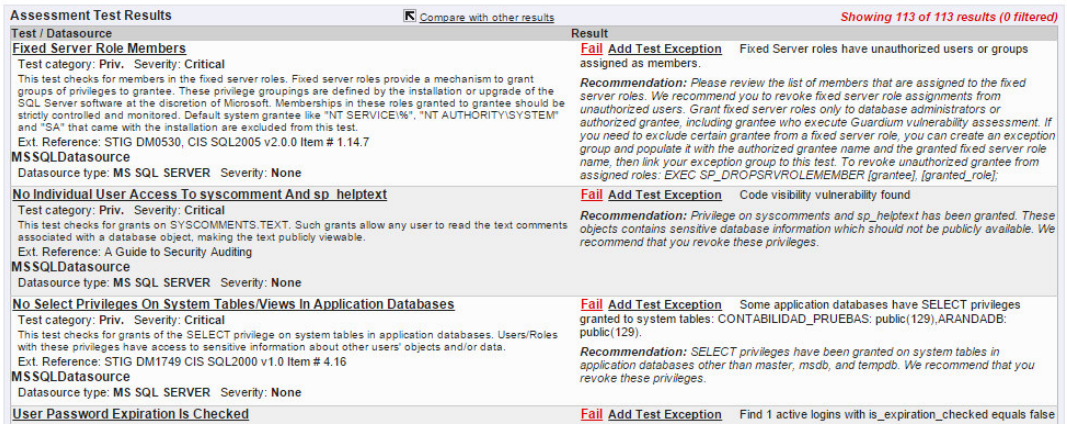


Figure 49. Evaluación de vulnerabilidades

Continuando con el reporte de la solución en cuanto al producto de evaluación de vulnerabilidades, ofrece las recomendaciones que se deben tomar para fortalecer la protección en la base de datos.



Assessment Test Results — Compare with other results — *Showing 113 of 113 results (0 filtered)*

Test / Datasource	Result
Fixed Server Role Members Test category: **Priv.** Severity: **Critical** This test checks for members in the fixed server roles. Fixed server roles provide a mechanism to grant groups of privileges to grantee. These privilege groupings are defined by the installation or upgrade of the SQL Server software at the discretion of Microsoft. Memberships in these roles granted to grantee should be strictly controlled and monitored. Default system grantee like "NT SERVICE\%", "NT AUTHORITY\SYSTEM" and "SA" that came with the installation are excluded from this test. Ext. Reference: STIG DM0530, CIS SQL2005 v2.0.0 Item # 1.14.7 **MSSQLDatasource** Datasource type: **MS SQL SERVER** Severity: **None**	Fail Add Test Exception Fixed Server roles have unauthorized users or groups assigned as members. ***Recommendation:*** *Please review the list of members that are assigned to the fixed server roles. We recommend you to revoke fixed server role assignments from unauthorized users. Grant fixed server roles only to database administrators or authorized grantee, including grantee who execute Guardium vulnerability assessment. If you need to exclude certain grantee from a fixed server role, you can create an exception group and populate it with the authorized grantee name and the granted fixed server role name, then link your exception group to this test. To revoke unauthorized grantee from assigned roles: EXEC SP_DROPSRVROLEMEMBER [grantee], [granted_role];*
No Individual User Access To syscomment And sp_helptext Test category: **Priv.** Severity: **Critical** This test checks for grants on SYSCOMMENTS.TEXT. Such grants allow any user to read the text comments associated with a database object, making the text publicly viewable. Ext. Reference: A Guide to Security Auditing **MSSQLDatasource** Datasource type: **MS SQL SERVER** Severity: **None**	Fail Add Test Exception Code visibility vulnerability found ***Recommendation:*** *Privilege on syscomments and sp_helptext has been granted. These objects contains sensitive database information which should not be publicly available. We recommend that you revoke these privileges.*
No Select Privileges On System Tables/Views In Application Databases Test category: **Priv.** Severity: **Critical** This test checks for grants of the SELECT privilege on system tables in application databases. Users/Roles with these privileges have access to sensitive information about other users' objects and/or data. Ext. Reference: STIG DM1749 CIS SQL2000 v1.0 Item # 4.16 **MSSQLDatasource** Datasource type: **MS SQL SERVER** Severity: **None**	Fail Add Test Exception Some application databases have SELECT privileges granted to system tables: CONTABILIDAD_PRUEBAS: public(129),ARANDADB: public(129). ***Recommendation:*** *SELECT privileges have been granted on system tables in application databases other than master, msdb, and tempdb. We recommend that you revoke these privileges.*
User Password Expiration Is Checked	Fail Add Test Exception Find 1 active logins with is_expiration_checked equals false

Figure 50. Recomendaciones para solucionar problemas de seguridad

CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Infosphere Guardium contiene dos productos importantes. DAM que supervisa y controla al usuario privilegiado sobre la información sensible. El siguiente producto es VA el cual ayuda a evaluar las vulnerabilidades de la base de datos, tomar decisiones y ejecutar manualmente cambios para fortalecer la base de datos.
- La funcionalidad auto descubrimiento facilita el conocimiento y el inventario de las bases de datos que se encuentran trabajando sobre el servidor de datos y mejorar el consumo de recursos.
- La funcionalidad de clasificador resulto para la empresa muy apropiado porque le ayudo a saber las bases de datos que han quedado abandonadas y los puertos abiertos.
- la solución IBM Infosphere Guardium 9.5 soporta a la base de datos MSSQL server
- Se implementa la arquitectura básica para el monitoreo y control de la base de datos. La cual consiste de un colector instalado sobre el mismo segmento de red del servidor de base de datos, los agentes fueron desplegados desde el colector hacia el servidor de datos, configurando motores de inspección para la recolección de información y ejecución de políticas.
- La valoración de vulnerabilidades Guardium requiere el acceso a las bases de datos que evalúa. Para ello, Guardium ofrece un conjunto de scripts de SQL (una secuencia de comandos para cada tipo de base de datos) que crea los usuarios y roles en la base de datos para ser utilizados por Guardium.
- Se implementa la solución Guardium según los requerimientos del cliente obtenido en el levantamiento de la información.

4.2. Recomendaciones

- Actualmente la empresa SinergyTeam presenta la arquitectura de la solución Infosphere Guardium configurada con la opción básica del S-TAP. Existen algunas opciones de configuración que pueden afectar de manera general la arquitectura de la solución. Recomendamos se implemente la opción de "Failover S-TAP" adicionando un colector a la arquitectura, en esta configuración el S-TAP envía todo el tráfico a un colector a menos que encuentre problemas de conectividad para que el colector dispare un failover a un segundo colector como se ha configurado.
- Cuando se implementa la solución IBM Infosphere Guardium es importante conocer los componentes funcionales del producto, uno de estos componentes es el Descubrimiento y Clasificación, funcionalidad que descubre y etiqueta la información sensible. Aplicar políticas de clasificación con procesos de clasificación para uno o más fuentes de datos y generar alertas que notifiquen por medio de un correo electrónico al operador cuando se intente acceder a la información.
- Con la reciente reubicación física del centro de datos, se recomienda utilizar la funcionalidad de descubrimiento de bases de datos, con esta funcionalidad consiguen identificar todos los motores de bases de datos que se encuentran escuchando en la red.
- Siendo Guardium un software de seguridad para las bases de datos, en su organización de seguridad presenta tres tipos de usuario básicos: Administrador de consola de comandos, Administrador de consola gráfica y el Administrador de accesos. Se recomienda asignar los usuarios de seguridad a personas diferentes y así poder controlar la seguridad de la data registrada en su repositorio.
- IBM continuamente libera parches para el colector, se recomienda la actualización de los mismos los cuales ayuda a prevenir fallos del equipo.
- Las reglas monitorean el comportamiento de los usuarios por medio de la acción "Log Full Details", se recomienda utilizar la acción "Audit-Only", audita solo los usuarios específicos e ignora las otras conexiones. En este modo el S-TAP filtra

muchas de las sesiones y solo un pequeño subconjunto del tráfico en general es enviado al equipo Guardium. El filtrado es realizado sobre el nivel de sesión por el S-TAP.

- Siempre está la tendencia de asumir que la opción de encriptación es la mejor. Los agentes S-TAP pueden ser configurados para comunicar sobre la red a los colectores en una manera de encriptación (TLS), sin embargo recomendamos mantener la configuración por defecto del S-TAP en "no encryption" para evitar algún impacto de rendimiento del servidor de la base de datos. Tome en cuenta, cuando se configura el S-TAP con (TLS) requerirá tiempo de encriptación extra y el colector también requerirá tiempo para desencriptar este tráfico.
- El equipo Guardium tiene un repositorio para mantener la información monitoreada registrada, este repositorio es limitado en tamaño, por esta razón puede usar back up o archive para descargar la data. El descuido de estas copias de seguridad puede causar problemas para las políticas de retención.
- El colector recibe y procesa el trafico monitoreado en tiempo real desde los agentes que están desplegados sobre el servidor de la base de datos, recomendamos que el colector debe estar cerca de la red y tener conectividad de alta velocidad LAN para reducir latencia en la red.
- La empresa SinergyTeam no cuenta con un ambiente de pruebas, es recomendado un permanente ambiente de pruebas Guardium para recrear problemas y probar nuevos componentes o configuraciones antes de desplegar a producción. El ambiente de pruebas debe ser similar al ambiente de producción.
- Es importante asegurar que la solución Guardium se encuentre disponible y funcionando apropiadamente y alertar a los usuarios de problemas, se recomienda implementar alertas de umbral auto monitoreo del tipo: Alertar una vez por hora sobre todos los S-TAP que no estén escuchando desde un período específico; alertar cuando no hay tráfico que no está colectado desde un servidor desde el cual el sistema Guardium estuvo colectando tráfico en algún punto durante las últimas 48 horas; alertar cuando el espacio libre disponible para la base de datos disponible cae por debajo del umbral de configuración.

- Cuando se utiliza una clave de licencia de producto expira, o de licencia con un número limitado de fuentes de datos, el mensaje siguiente puede aparecer: ". No se puede agregar origen de datos se ha alcanzado el número máximo de fuentes de datos permitido por la licencia." La Licencia válida hasta la fecha y el número de fuentes de datos se puede ver en el panel de configuración del sistema de la consola de administrador. Una vulnerabilidad o el proceso de clasificación con N fuentes de datos se cuentan como N escanea cada vez que se ejecutan.

Bibliografía

IBM. (2015). *Support Portal.* Obtenido de www.ibm.com

IBM. (s.f.). *Access Management Overview*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/access_management/topics/access_management_overview.html?lang=es

IBM. (s.f.). *Assess and Harden help book*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/assess_harden/topics/AssessAndHardenHelpBook.html?lang=es

IBM. (s.f.). *Assess and Harden help book*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/monitor_audit/topics/audit_and_report_overview.html?lang=es

IBM. (s.f.). *Classification.* Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/discover/topics/classification.html?lang=es

IBM Developers Works. (30 de Septiembre de 2013). *Conceptos y Mejores Prácticas para el control de accesos del agente STAP de IBM Infosphere Guardium*. Obtenido de http://www.ibm.com/developerworks/ssa/security/library/Conceptos_y_Mejores_Pr%C3%A1cticas_para_el_control_de_accesos_del_agente_STAP_de_IBM_Infosphere_Guardium/index.html

IBM. (s.f.). *Discover help book.* Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/discover/topics/discover_cover.html?lang=es

IBM. (s.f.). *Infosphere Guardium Data Activity Monitor*. Obtenido de http://www-03.ibm.com/software/products/es/infosphere-guardium-data-activity-monitor

IBM. (s.f.). *Manage Roles*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/access_management/topics/managing_roles.html?lang=es

IBM. (s.f.). *Manage Users*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/access_management/topics/manage_users.html?lang=es

IBM. (s.f.). *Monitor and Audit Help Book*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/monitor_audit/topics/monitor_cover.html?lang=es

IBM. (s.f.). *Vulnerability Assessment*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/assess_harden/topics/assess.html?lang=es

Junta Bancaria del Ecuador . (26 de Abril de 2012). . Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

Maulini, M. (14 de Diciembre de 2010). *Desarrollo de Seguridad y Aplicaciones web y moviles*. Obtenido de http://tecnologiasweb.blogspot.com/2010/12/los-diez10-tipos-de-vulnerabilidades-de.html

Mcafee. (2014). *McAfee Vulnerability Manager for Databases*. Obtenido de http://www.mcafee.com/us/products/vulnerability-manager-databases.aspx

Mcafee. (2015). *McAfee Database Activity*. Obtenido de http://www.mcafee.com/us/resources/data-sheets/ds-database-activity-monitoring.pdf

Mcafee. (s.f.). *McAfee Virtual Patching for Databases*. Obtenido de http://www.ndm.net/mcafee/Database-Security/mcafee-virtual-patching-for-databases

Vergara, C. (14 de Julio de 2012). *Ataque y Seguridad a la base de datos*. Obtenido de http://ataquebd.blogspot.com/

Vormetric. (2015). *Transparent Encryption*. Obtenido de http://www.vormetric.com/products/transparent-encryption

Wikipedia. (4 de Noviembre de 2013). Obtenido de https://es.wikipedia.org/wiki/Triple_DES

Wikipedia. (10 de Marzo de 2014). Obtenido de https://es.wikipedia.org/wiki/Blowfish

Wikipedia. (14 de Diciembre de 2014). Obtenido de https://es.wikipedia.org/wiki/ECDSA

Wikipedia. (28 de Diciembre de 2014). Obtenido de https://es.wikipedia.org/wiki/International_Data_Encryption_Algorithm

Wikipedia. (11 de Mayo de 2015). Obtenido de https://es.wikipedia.org/wiki/Advanced_Encryption_Standard

Wikipedia. (19 de Abril de 2015). Obtenido de https://es.wikipedia.org/wiki/RC4

Wikipedia. (10 de Julio de 2015). Obtenido de https://es.wikipedia.org/wiki/Data_Encryption_Standard

Wikipedia. (8 de Junio de 2015). Obtenido de https://es.wikipedia.org/wiki/DSA

Wikipedia. (30 de Marzo de 2015). Obtenido de https://es.wikipedia.org/wiki/ROT13

Wikipedia. (5 de Junio de 2015). Obtenido de https://es.wikipedia.org/wiki/RSA

FECHA DE ENTREGA

El proyecto fue entregado al departamento de Eléctrica y Electrónica y reposa en la Universidad de las Fuerzas Armadas – ESPE, desde:

Sangolquí, 20 de Mayo del 2015

ELABORADO POR:

_____

Jimmy Fabian Ludeña Carrión

CI: 0703532242

AUTORIDADES:

_____

Dr. Nikolay Espinosa.

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS