Seguridad en Formiik

Autores
Christian Ramírez
Rogelio Barajas

Actualización 2018-11-14

CONTACTO
Av. Insurgentes Sur 1228, Oficina 401, Col. Tlacoquemecatl, México D.F., C.P. 03200, México T. 4161 4600 // info@formiik.com // www.formiik.com Carrera 10 No. 97 A – 13 Torre B Oficina 202, Bogotá D.C., C.P. 110121, Colombia, T. +57 (1) 7426478

Documento con toda la informacion relacionada a los elementos de seguridad que se utilizan en Formiik en todos sus elementos.

Seguridad Formiik

Introducción

Al ser Formiik un producto del tipo SaaS uno de los elementos más importantes en el diseño es la seguridad, ya que al no residir la información de nuestros clientes en su propia infraestructura es necesario tomar todas las consideraciones de los posibles escenarios de riesgo.
Formiik esta construido sobre la plataforma de cómputo en la nube de Microsoft llamada Windows Azure, que ha probado su confiabilidad y seguridad en cientos de proyectos alrededor del mundo.
A continuación se presenta a detalle el funcionamiento de cada uno de los puntos de seguridad existentes para todos los elementos que conforman el ecosistema Formiik.

Seguridad de la plataforma

Plataforma de cómputo en la nube

La plataforma de cómputo en la nube sobre la cual esta desarrollada Formiik se compone de 3 elementos:

Procesamiento: Son los elementos encargados de procesar la información con la cual opera Formiik, aquí tenemos 3 tipos:

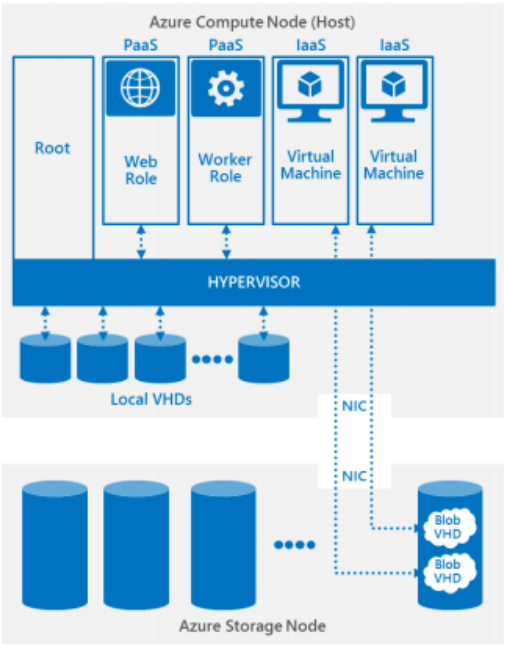
- Máquinas virtuales
- Websites
- Worker roles

Almacenamiento: esta parte esta formado por 2 grandes componentes:

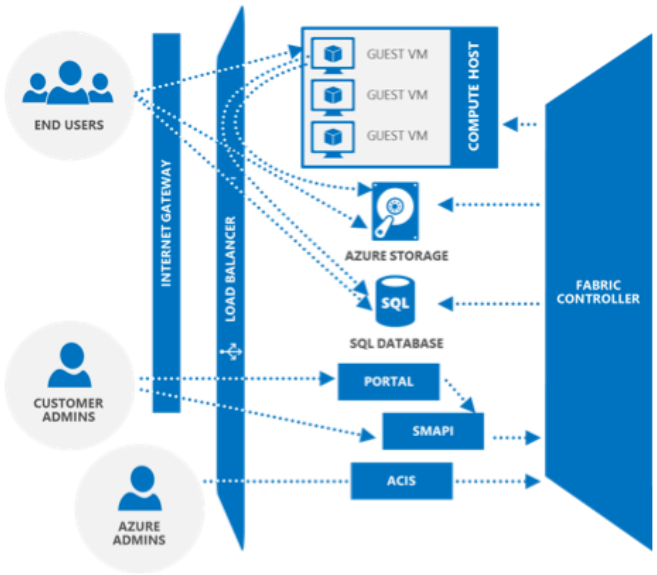
- Storage
  - Tablas del tipo llave-valor
  - Almacenamiento de blobs
  - Estructuras tipo cola
- Bases de datos transaccionales

Comunicación: la estructura de comunicación de Formiik esta formada por:

- redes virtuales
- endpoints al exterior (puertos abiertos)
- firewalls y balanceadores de carga



La arquitectura de la plataforma esta diseñada para otorgar una infraestructura consistente y un escalable conjunto de recursos.
El diseño de la nube que utiliza Formiik, es multi-tenant por lo que diversas máquinas virtuales residen sobre la misma infraestructura física.



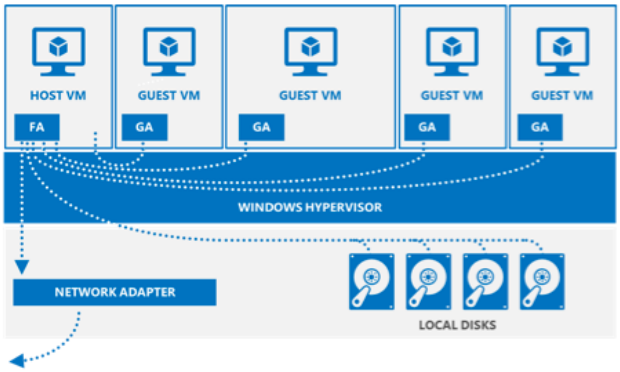
Servicios de almacenamiento

El almacenamiento que utiliza formiik se compone de 2 elementos:

1. Base de datos transaccional. Se trata de una version modificada de SQL server para funcionar sobre la nube y con la posibilidad de escalar en cuanto a recursos que utiliza.
2. Almacenamiento en disco
    a. blob. almacenamiento de archivos de todo tipo donde se asigna un UUID unico para identificar y acceder al recurso
    b. colas. almacenamiento de mensajes que se emplea como medio de comunicacion entre los diferentes elementos de la plataforma
    c. tablas del tipo llave-valor. estructura tabular del tipo NOSQL de baja latencia

Aislamiento: Windows Azure - Fabric

Todos los servicios de la nube están hospedados en maquinas virtuales dedicadas. Estas máquinas virtuales se ejecutan sobre un hipervisor controladas y administradas por un elemento llamado Fabric, las VM ejecutan una versión especial de windows server que ejecutan a su vez un agente de Fabric el cual acepta comandos del controlador de Fabric. Este controlador es el encargado de gestionar todos los recursos relacionados con la VM asi como las interconexiones entre los diferentes elementos, por lo que no se tiene acceso directo a los diferentes componentes virtualizados lo que da como resultado ambientes totalmente aislados.
De igual manera la VM host es la única puerta de acceso y salida hacia los recursos de red, por lo que la comunicación entre maquinas desde el mismo host no es posible de manera directa.



Seguridad de los servicios en la nube

La plataforma de computo en la nube está diseñada para proporcionar “defensa en profundidad”, lo que reduce el riesgo de que un error de un mecanismo de seguridad ponga en peligro la seguridad de todo el entorno. Las capas de defensa en profundidad incluyen:

Enrutadores de filtrado: los enrutadores de filtrado rechazan los intentos de comunicación entre direcciones y puertos no configurados como permitidos. De este modo, se previenen ataques comunes que usan “drones” o “zombies” en busca de servidores vulnerables. Aunque su bloqueo es relativamente sencillo, estos tipos de ataques siguen siendo el método preferido de los atacantes malintencionados que buscan puntos vulnerables. Los enrutadores de filtrado también permiten la configuración de servicios back-end de modo que solo estén accesibles desde sus correspondientes front-ends, como es el caso de formiik.

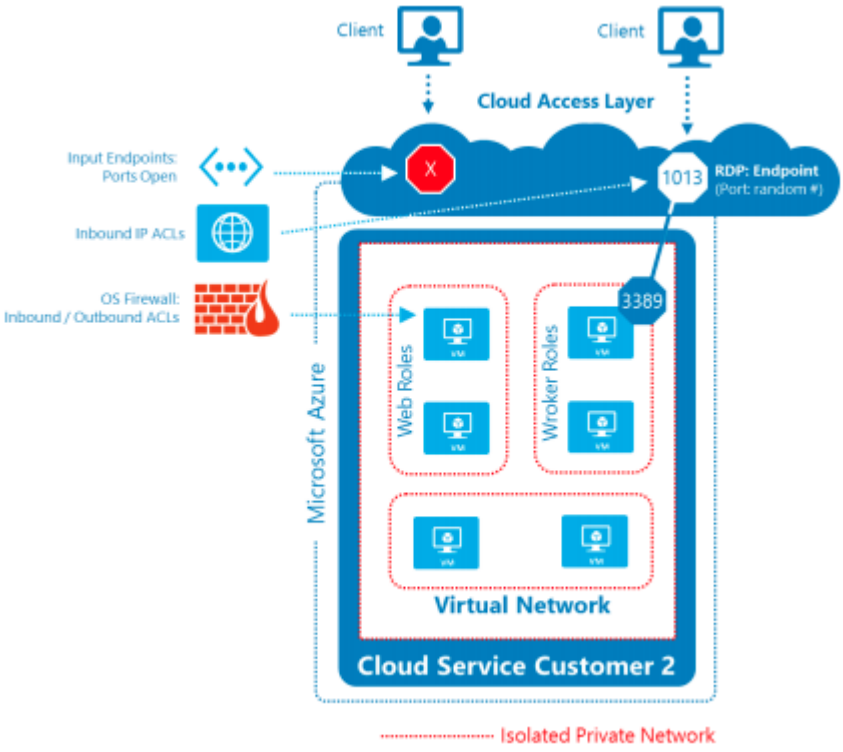
Firewalls: los firewalls restringen la comunicación de datos entre puertos, protocolos y direcciones IP de origen y destino autorizados y conocidos.

Protección criptográfica de mensajes: para proteger los mensajes de control que se envían entre los centros de datos y entre los clústeres de un centro de datos dado, se utiliza TLS con claves criptográficas de al menos 512 bits.

Administración de revisiones de seguridad de software: la administración de revisiones de seguridad es una parte de las operaciones que ayudan a proteger los sistemas de puntos vulnerables conocidos. La plataforma Windows Azure utiliza sistemas de implementación integrados para administrar la distribución e instalación de revisiones de seguridad de software de Microsoft.

Supervisión: la seguridad se supervisa con ayuda de sistemas de supervisión, correlación y análisis centralizados que administran la gran cantidad de información generada por los dispositivos del entorno, proporcionando supervisión y alertas pertinentes y puntuales.

Segmentación de la red: Se utilizan varias tecnologías para crear barreras para el tráfico no autorizado en las conexiones hacia y en los centros de datos, incluidos firewalls, cuadros de traducción de direcciones de red (equilibradores de carga) y enrutadores de filtrado. La red back-end se compone de redes de área local con particiones para servidores web y de aplicaciones, almacenamiento de datos y administración centralizada. Estos servidores se agrupan en segmentos de direcciones privadas protegidos por enrutadores de filtrado.



Identidad y administración del acceso al portal de formiik

Se cuenta con identificación en todo momento de quien accede a la plataforma, mediante un usuario y contraseña únicos por cliente.

Se realiza una verificación de los permisos concedidos al usuario y validación para que sólo puedan ejecutar aquellas personas con los permisos relevantes. Si se solicita una operación y el usuario no tiene los permisos requeridos, se niega la solicitud.

Administración de excepciones

Todas las excepciones, tanto del sistema en la nube como de los móviles son registradas, con el fin de tener una bitácora confiable para realizar diagnósticos en caso de situaciones anormales.

Autenticación portal de administración de servicios en la nube

La administración de los servicios en la nube se realiza de manera centralizada en un portal de control y gestión de los recursos, el acceso a dicho portal es mediante el otorgamiento de credenciales de administración de la suscripción, que consiste de usuario y password asociados a una identidad certificada así como privilegios por cada una de las suscripciones.

Autenticacion para el uso de la API de administracion de servicios

La administración de los servicios se hace mediante web services los mismos usan un protocolo que corre sobre ssl y es autenticado con OAuth2.0.

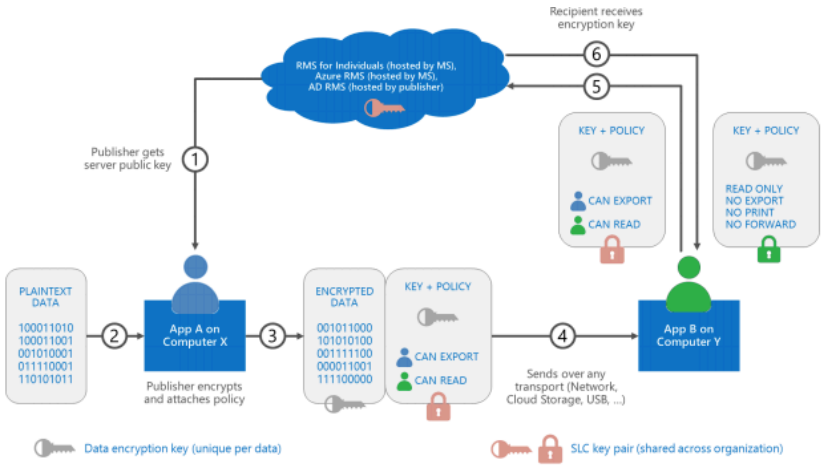
Autenticación para el almacenamiento

Se proveen de 2 llaves secretas que son usadas para controlar el acceso a la cuenta de almacenamiento(la segunda es provista para acceder cuando se están haciendo operaciones de rollover con la llave primaria). la llave es utilizada para computar un mensaje de código de autenticación basado en hash (HMAC por sus siglas en ingles) de una petición de información y un registro de tiempo para probar que se conoce la llave secreta.

Administración de llaves para los servicios en la nube

Para disminuir el riesgo de exposición de los certificados y claves privadas a los desarrolladores, se instalan a través de un mecanismo independiente del código que las usa. Los certificados y claves privadas se cargan a través de SMAPI o del Portal de administración como PKCS12 (PFX) Los archivos son protegidos en tránsito mediante SSL. Estos archivos se almacenan cifrados dentro de los controladores de la nube.

Los datos de configuración asociada con cualquier función dentro de la misma suscripción especifica los certificados que deben estar disponibles para el role. Cuando un role se instancia en una máquina virtual, el controlador de Fabric recupera el certificado correspondiente, descifra el blob PKCS12, y lo vuelve a cifrar con la clave de transporte públic, y lo envía al agente en el node. El agente en el nodo envía al agente en la máquina virtual donde se crearon los roles, y luego el agente lo instala en el almacén de certificados del sistema operativo con una bandera que indica que la clave privada se puede utilizar, pero no exporta. Después de la instalación, todas las copias temporales de los certificados y claves son destruidos; si se requiere la reinstalación, los certificados deben ser empaquetados de nuevo por el controlador de Fabric.



Autenticacion mutua mediante SSL e IP para el trafico interno

La mayoría de las comunicaciones entre los componentes internos de los servicios en la nube de formiik están protegidas con SSL. Hay una serie de diferentes mecanismos por los que estos certificados SSL son validados. En algunos casos, una huella digital del certificado SSL está configurado en la VM del autenticador; los certificados que participan pueden ser de tipo auto-firmado. En otros casos, el nombre en el certificado se comprueba y la cadena de los certificados es creada por una CA de confianza En otros casos, un servicio de token (DSTS) se utiliza y la autenticación se basa en tokens firmados. Este intermediario es interno de la plataforma en la nube y por lo tanto no depende de ninguna autoridad ajena.

Además de la autenticación criptográfica estas conexiones internas, los componentes residentes en la nube deben comprobar las direcciones IP de los servicios que inician conexiones con ellos. El hipervisor de la plataforma de computo en la nube y la infraestructura de enrutamiento no permiten un servicio para suplantar la dirección IP de un servicio diferente.
Estos dos mecanismos trabajan conjuntamente para proporcionar una defensa en profundidad contra los ataques basados en la red.

Credenciales en los dispositivos de hardware

Adicional a las llaves de las aplicaciones, el controlador Fabric mantiene otro juego de llaves que utiliza para autenticar el hardware que controla y tiene acceso. Uno de los principales usos es cuando se accede a recursos de red, por lo que antes de transferir información valida que el hardware sea valido.

Aislamiento del hypervisor

Un elemento que aumenta el nivel de aislamiento del hypervisor así como de los diferentes ambientes huéspedes, es un arreglo especial de firewalls y filtrado de paquetes para evitar que exista comunicación no solicitada o autorizada entre los elementos de la nube.

Ejecucion de software sin privilegios

Todo el software que se ejecuta en la plataforma cloud de formiik se ejecuta con los permisos minimos indispensables, con el fin de evitar alteraciones y posibles vulnerabilidades; de igual manera se evitan que un atacante puede explotar algun tipo de tecnica de escalamiento de privilegios.

Aislamiento de red para los servicios en la nube

El hypervisor y el sistema operativo anfitrión proporcionan filtrado de paquetes de red que ayudan a asegurar que VM en las que no se confía pueden generar tráfico falso, no pueden recibir tráfico no dirigido a ellos, no pueden dirigir el tráfico a los endpoints de infraestructura protegida y no pueden enviar o recibir tráfico de broadcast inadecuada.
El acceso a la red para máquinas virtuales se ve limitada por el filtrado de paquetes en el borde de la red, en los balanceadores de carga, y a nivel de sistema operativo anfitrión. Los clientes pueden, además, configurar sus firewalls para limitar aún más la conectividad. En particular, la depuración, control remoto, Terminal Services remotos, o el acceso remoto a recursos compartidos de archivos de la VM no está permitido por defecto. La plataforma de computo en la nube permite especificar en cada puerto de escucha si se aceptan conexiones desde Internet o sólo de instancias de rol dentro del mismo servicio en la nube o VNET.
Las conexiones entre las instancias de rol de los diferentes servicios en la nube son considerados como las conexiones a Internet, excepto cuando se utilizan VNET, en cuyo caso se consideran todos los servicios en la nube dentro de una sola VNET al estar conectados localmente.

Para cada máquina virtual, el Fabric Controller compone (y mantiene al día) una lista de direcciones IP de las máquinas virtuales en el mismo servicio en la nube. Esta lista de direcciones IP es utilizada por el agente de Fabri para programar los filtros de paquetes para permitir solamente la comunicación a dichas direcciones IP.

Borrado de datos

Una vez que los datos han sido borrados del almacenamiento quedan totalmente inaccesibles ya que todas las operaciones del almacenamiento están diseñadas para ser efectivas en el momento. Una operación de borrado remueve todas las referencias al elemento por lo que ya no puede ser accesado. Los bits son físicamente sobreescritos.

Disponibilidad

Una de las ventajas del computo en la nube es la alta disponibilidad de los servicios, para garantizar lo anterior el diseño de la plataforma considera alta redundancia para todos los elementos de storage por lo que todos los elementos se encuentran en tres nodos en tres racks separados, para afrontar posibles desastres o fallas.

Operaciones en las instalaciones físicas

La información de todo formiik se encuentra dispersa en pequeñas partes en varias ubicaciones físicas y respaldada de forma redundante, es decir, no se encuentra todo en la misma maquina.
Por otro lado los discos donde la información se almacena están cifrados y la llave es la misma que utiliza el usuario para acceder a los servicios de almacenamiento.
Todos los datacenter cumplen con el estándar ISO27001

Seguridad física

Ninguno de los equipos físicos cuenta con dispositivos de I/O conectados o habilitados, adicionalmente todos los elementos físicos cuentan con una alarma de ubicación, es decir, si una maquina, un disco, un cable son desconectados se activa una alarma.

Controles de acceso

Los datacenters donde reside formiik, están diseñados para operar de manera remota, por lo que el acceso de personal solo es por motivos de mantenimiento.
Todas las personas que tienen acceso físico a las instalaciones donde se encuentra el hardware han aprobado controles de confianza, de igual manera el acceso a las instalaciones se realiza de manera granular mediante accesos controlados por secciones, es decir, una sola persona no tiene acceso a la totalidad de las instalaciones, para acceder a las áreas permitidas se requieres de credenciales (usuarios, password) un código de seguridad que se envía a un dispositivo móvil tipo tarjeta cada vez que se quiere acceder y controles biométricos.
Se lleva un registro y control de acceso que incluye horarios de acceso y desalojo así como tiempo de permanencia, que funciona las 24 horas los 365 días del año.

Energía redundante y tolerante a fallas

Cada uno de los centros de datos donde reside formiik, tiene como mínimo 2 fuentes de energía eléctrica incluyendo una fuente de generación fuera de la red eléctrica. Se tienen controles ambientales al interior de los datacenter que permiten la operación ininterrumpida.
En caso de emergencias debidas a fenómenos naturales la información se encuentra distribuida de forma redundante en otro datacenter a miles de kilómetros por lo que no existe riesgo de perdida de información.

Redundancia

Cada capa de la infraestructura de Windows Azure está diseñada para que continúen las operaciones en caso de que se produzca un error, incluidos los dispositivos de red redundantes de cada capa y los proveedores de acceso a Internet duales de cada centro de datos. La conmutación por error es automática en la mayoría de los casos y no requiere la intervención del usuario. El Centro de operaciones de red supervisa la red las 24 horas del día, los 7 días de la semana, a fin de detectar cualquier anomalía o posibles problemas en la red.

Regulaciones y estándares

Toda la infraestructura física, virtual y datacenters cumple rigurosamente con las regulaciones y estándares en la materia que son referencia a nivel mundial, a continuación se listan todas aquellas que han sido evaluadas y certificadas de forma independiente por terceras partes.

- ISO 27001/27002
- SOC 1/SSAE 16/ISAE 3402 and SOC 2
- Cloud Security Alliance CCM
- FedRAMP
- FISMA
- FBI CJIS (Azure Government)
- PCI DSS Level 1
- United Kingdom G-Cloud
- Australian Government IRAP
- Singapore MTCS Standard
- HIPAA
- EU Model Clauses
- Food and Drug Administration 21 CFR Part 11
- FERPA
- FIPS 140-2
- CCCPPF
- MLPS

Seguridad componentes de la aplicacion movil

Todos los componentes están declarados con un permiso interno que cuenta con un nivel de protección signature por lo tanto solamente componentes firmados con el mismo certificado pueden “invocarlos” mediante un broadcast.

Transmisiones seguras desde el dispositivo móvil

Toda la comunicación entre los equipos móviles y la plataforma en la nube de formiik, se cuenta con cifrado mediante comunicación segura basada en SSL y TLS.
Se usan certificados X.509 y por lo tanto criptografía asimétrica para autentificar a la contraparte con quien se están comunicando, y para intercambiar una llave simétrica. Esta sesión es luego usada para encriptar el flujo de datos entre las partes. Esto permite la confidencialidad del dato/mensaje, y códigos de autenticación de mensajes para integridad y como un producto lateral, autenticación del mensaje.

Teléfonos extraviados

En caso de perdida de un equipo movil con formiik podemos:

- Cancelar y recuperar todas las ordenes asignadas en el teléfono extraviado
- Reenviar todas las ordenes asignadas a un nuevo dispositivo
- Bloquear el acceso desde el dispositivo hacia formiik
- Recuperar y reenviar todos los mensajes

Lo anterior permite restaurar el instrumento y la información de trabajo de manera sencilla, rápida y sin perdida de información asignada.

Network sniffing

Los routers internos de los centros de computo no conectan directos a Internet y se ejecutan en un modo muy restringido para bloquear cualquier conexion no autenticada. No hay acceso inalámbrico a cualquier red de producción, sistemas o infraestructura.

Continuidad del negocio

A pesar de que Formiik se encuentra dentro de una de las plataformas de computo en la nube mas confiables a nivel mundial, no esta exento de desastres naturales, conflictos belicos, sociales o politicos. Por lo anterior es indispensable contar con un plan de continuidad del negocio.

Recuperación de fallas locales

Existen dos posibles tipos de fallas locales, la primera es que la capacidad de computo sea sobrepasada y por lo tanto nuestros servicios fallen y la segunda es la posibilidad de que algun componente fisico presente alguna falla de cualquier tipo.
Para el primer caso, la configuración de la nube donde reside Formiik considera una opcion de monitoreo constante y escalamiento por lo tanto cuando se detenctan sobrecargas a la capacidad de computo, la misma se incrementa de manera automatica de acuerdo a un modelo de autoescalamiento que provisiona toda la capacidad de computo necesaria.
En casos donde falla algun componente fisico como discos, tarjetas de red, etc el controlador Fabric identifica el problema y cambia toda la VM a un nuevo nodo, de forma automática e instantánea.

Recuperación de la perdida de una region de la nube

La plataforma de computo en la nube de Formiik esta dividida en 8 regiones fisicas 4 en Estados 2 en Europa y 2 en Asia; en caso de existir la perdida total o parcial de una de estas regiones existen diferentes estrategias de recuperacion, acorde a los requerimientos de cada aplicacion que componen la plataforma completa de Formiik.

- Redespliegue en desastre. Las aplicaciones se redespliegan en una nueva ubicacion desde cero, dado que el proceso es completamente automatizado se garantiza el mismo tiempo de respuesta y de despliegue que en la ubicacion original.
- Respaldo emergente. Se crea un segundo servicio en una region diferente para atender el trafico minimo de aplicaciones no esenciales.

Recuperación usando almacenamiento geo-redundante

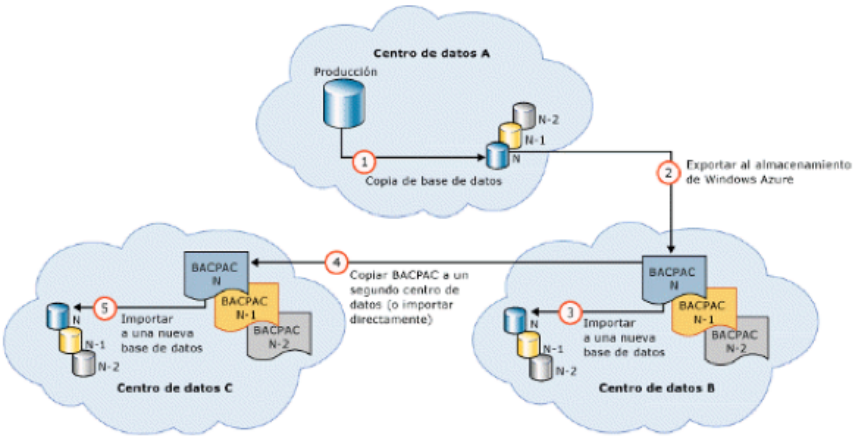
En la nube de formiik todos los almacenamientos tipo blobs, colas, tablas tipo llave-valor y discos de maquinas virtuales son georeplicados en su tottalidad por defecto. En un evento de falla en una region geografica no habra ningun cambio en como se accede a la cuenta, sin embargo la cuenta de almacenamiento se encontrara en una region distinta de forma automatica.

Redundancia en base de datos

Cada instancia de SQL tiene tres réplicas que residen en tres equipos físicos diferentes de un centro de datos: una réplica principal y dos secundarias. Todas las lecturas y escrituras pasan a través de la réplica principal y los cambios se replican en las réplicas secundarias de forma asincrónica.
SQL emplea un esquema de confirmación basado en quórum donde la escritura se debe completar en la réplica principal y en una réplica secundaria para que la transacción se considere confirmada. Si se produce un error de hardware en la réplica principal, el tejido de SQL lo detecta y conmuta por error a la réplica secundaria. Por tanto, también hay al menos dos copias físicas coherentes transaccionalmente de los datos en un centro de datos. Las tres réplicas para cada instancia de SQL protegen los datos frente a errores de servidores individuales, dispositivos o conectividad de red. Además de las réplicas redundantes, la red de SQL Azure de Windows Azure mantiene un mínimo de 14 días de copias de seguridad tomadas en incrementos de cinco minutos para todas las bases de datos del centro de datos. Estas copias de seguridad se almacenan en el centro de datos como medida preventiva frente a errores de hardware y del sistema simultáneos o catastróficos.

Respaldo de bases de datos

Como parte de las políticas de respaldo y seguridad de formiik se crean 2 copias de respaldo de la base de datos, la primera mediante una herramienta de respaldos y la segunda mediante las operaciones de mantenimiento de la base de datos. Dichas copias son almacenadas en diferentes centros de computo de con diferentes ubicación geográficas.



Seguridad en Base de Datos

Protección de datos

Cifrado

Para proteger los datos, SQL Database cifra los datos en movimiento a través del protocolo de Seguridad de la capa de transporte, los datos en reposo a través del Cifrado de datos transparente y los datos en uso a través de Always Encrypted.

Importante

Todas las conexiones a Azure SQL database requieren cifrado (SSL/TLS) siempre que haya datos "en tránsito" hacia y desde la base de datos. En la cadena de conexión de la aplicación, debe especificar los parámetros necesarios para cifrar la conexión y *no* confiar en el certificado de servidor (esto se hace automáticamente si copia la cadena de conexión fuera de Azure Portal).

Clasificación y detección de datos

La opción Clasificación y detección de datos proporciona funcionalidades avanzadas integradas en Azure SQL Database para detectar, clasificar, etiquetar y proteger la información confidencial de las bases de datos. Las funciones de detección y clasificación de la información confidencial más importante (empresarial, financiera, médica, personal, etc.) desempeñan un rol fundamental en el modo en que se protege la información de su organización. Puede servir como infraestructura para:

- Varios escenarios de seguridad, como la supervisión (auditoría) y las alertas relacionadas con accesos anómalos a información confidencial.
- Controlar el acceso y mejorar la seguridad de las bases de datos que contienen información altamente confidencial.
- Ayudar a cumplir los requisitos de cumplimiento de normas y los estándares relacionados con la privacidad de datos.

Control de acceso

SQL Database protege los datos mediante la limitación del acceso a la base de datos a través de reglas de firewall, de mecanismos de autenticación que requieren que los usuarios prueben su identidad y de la autorización a través de pertenencias y permisos basados en roles, así como la seguridad de nivel de fila y el enmascaramiento dinámico de datos.

Importante

La administración de bases de datos y servidores lógicos en Azure se controlan mediante las asignaciones de roles de su cuenta de usuario del portal.

Firewall y reglas de firewall

Para ayudarle a proteger los datos, los firewalls impiden todo acceso al servidor de bases de datos hasta que especifique los equipos que tienen permiso mediante reglas de firewall. Asimismo, otorgan acceso a las bases de datos según la dirección IP de origen de cada solicitud.

Autenticación

La autenticación de SQL Database indica cómo probar su identidad al conectarse a la base de datos. SQL Database admite dos tipos de autenticación:

- **Autenticación de SQL**, que usa un nombre de usuario y una contraseña. Al crear el servidor lógico de la base de datos, especificó un inicio de sesión de "administrador de servidor" con un nombre de usuario y una contraseña. Con estas credenciales, puede autenticarse en cualquier base de datos en ese servidor como propietario de la base de datos, o "dbo".

Autorización

Autorización indica las acciones que pueden realizar los usuarios en Azure SQL Database, algo que controlan los permisos de nivel de objeto y las pertenencias a roles de bases de datos de la cuenta de usuario. Como procedimiento recomendado, debe conceder a los usuarios los privilegios mínimos necesarios. La cuenta de administrador de servidor con la que se está conectando forma parte de db_owner, que tiene autoridad para realizar cualquier acción en la base de datos. Guarde esta cuenta para implementar las actualizaciones de los esquemas y otras operaciones de administración. Utilice la cuenta "ApplicationUser" con permisos más limitados para conectarse desde la aplicación a la base de datos con los privilegios mínimos que necesita la aplicación.
Seguridad de nivel de fila

La seguridad de nivel de fila permite a los clientes controlar el acceso a las filas de una tabla de base de datos en función de las características del usuario que ejecuta una consulta (por ejemplo, la pertenencia a un grupo o el contexto de ejecución). Para más información, consulte Seguridad de nivel de fila.

Supervisión proactiva

SQL Database protege los datos proporcionando funcionalidades de auditoría y detección de amenazas.
Auditoría

SQL Database Auditing realiza un seguimiento de las actividades de la base de datos y ayuda a mantener el cumplimiento normativo, para lo que graba eventos de base de datos en un registro de auditoría de su cuenta de Azure Storage. La auditoría permite conocer las actividades en curso de la base de datos, así como analizar e investigar la actividad histórica para identificar posibles amenazas o supuestas infracciones de seguridad y abusos.

Detección de amenazas complementa la auditoría, ya que proporciona una capa adicional de inteligencia de seguridad integrada en el servicio de Azure SQL Database que detecta intentos inusuales y potencialmente dañinos para obtener acceso a las bases de datos o vulnerarlas. Recibirá alertas de actividades sospechosas, vulnerabilidades potenciales y ataques por inyección de código SQL, así como patrones anómalos de acceso a bases de datos. Las alertas de Detección de amenazas pueden verse en Azure Security Center y proporcionar detalles de actividad sospechosa y la acción recomendada sobre cómo investigar y mitigar la amenaza.

Cumplimiento normativo

Además de las anteriores características y funcionalidades que pueden ayudar a la aplicación a cumplir distintos requisitos de seguridad, Azure SQL Database también participa en las auditorías regulares y ha obtenido la certificación de una serie de normas de cumplimiento.

Administración de la seguridad

SQL Database le ayuda a administrar la seguridad de los datos con análisis de bases de datos y un panel de seguridad centralizado mediante la evaluación de vulnerabilidades de SQL.

Evaluación de vulnerabilidad: la valuación de vulnerabilidades de SQL es una forma sencilla de configurar la herramienta integrada en Azure SQL Database que puede detectar, realizar un seguimiento y corregir posibles vulnerabilidades de la base de datos. La evaluación ejecuta un análisis de vulnerabilidades en la base de datos y genera un informe que proporciona visibilidad sobre el estado de seguridad, incluidos los pasos útiles para resolver problemas de seguridad y mejorar la seguridad de la base de datos. Es posible personalizar un informe de evaluación para su entorno estableciendo una línea de base aceptable para las configuraciones de permisos, configuraciones de características y configuración de base de datos. Esto puede ayudarle a:

- Satisfacer los requisitos de cumplimiento que requieren los informes de análisis de base de datos.
- Cumplir los estándares de privacidad de datos.
- Supervisar un entorno de base de datos dinámico en el que es complicado realizar un seguimiento de los cambios.

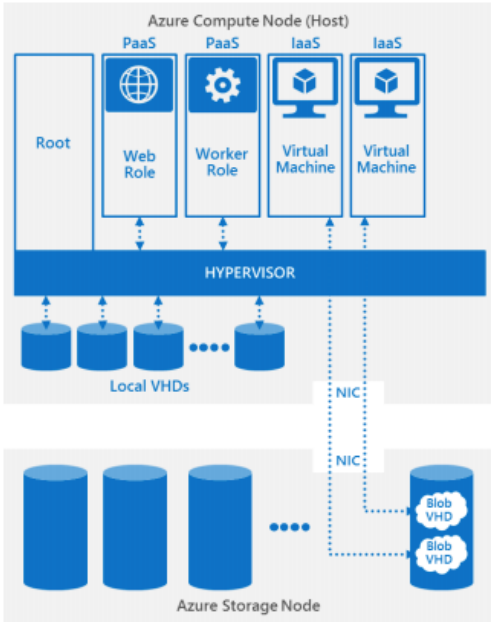
Seguridad de los datos

Entre las capacidades de protección de datos con las que cuenta formiik están el desarrollo de servicios, componentes y configuraciones que aplican encripcion interna de información y trafico.

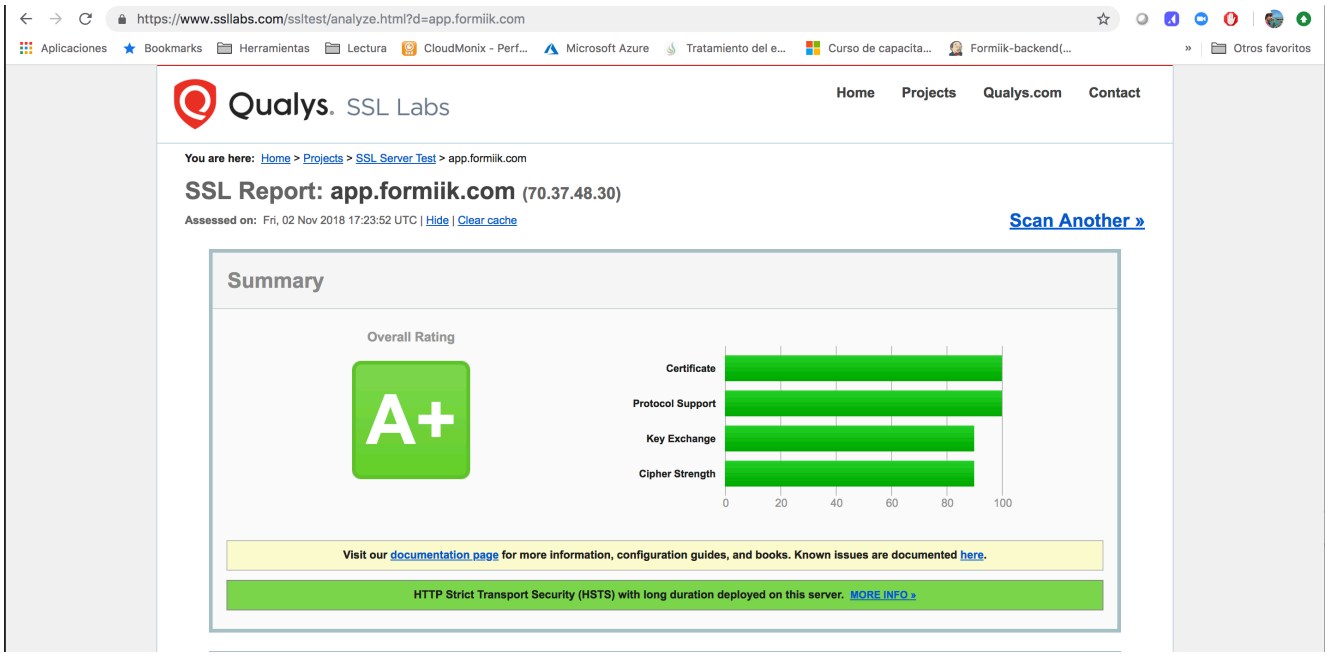
Many of these mechanisms are enabled by default in the platform while others need to be configured by
a customer administrator (such as IPsec VPN). Some can be optionally invoked at VM boot-time through
service configuration files, or called by application components directly.

La plataforma de computo en la nube implementa encripcion utilizando llaves simétricas y asimétricas para proteger la información confidencial:

- Software-based AES-256 para encripcion y descifrado simétrico.
- Llaves asimétricas de 2048-bit o mejores
- SHA-256 o mejor para hashing seguro



Como resultado de los recientes pentest el portal app.formiik.com cumple con los estándares de la industria nivel de seguridad en las conexiones soportando conexiones solo con versión de certificado TLS 1.2.



Referencias

Azure Security Overview Training Module
http://www.microsoftvirtualacademy.com/tracks/windows-azure-security-overview

Azure Security Review
http://blogs.msdn.com/b/buckwoody/archive/2011/08/02/windows-azure-securityreview.aspx

Crypto Primer: Understanding encryption, public/private key, signatures and certificates
http://blogs.msdn.com/b/plankytronixx/archive/2010/10/23/crypto-primerunderstanding-encryption-public-private-key-signatures-and-certificates.aspx

Field Note: Using Certificate-Based Encryption in Windows Azure Applications
http://blogs.msdn.com/b/windowsazure/archive/2011/09/07/field-note-using-certificatebased-encryption-in-windows-azure-applications.aspx

Azure Security Guidance http://www.windowsazure.com/en-us/documentation/articles/best-practices-security

Windows Azure Security Best Practices – Part 7: Tips, Tools, Coding Best Practices
http://blogs.msdn.com/b/usisvde/archive/2012/03/15/windows-azure-security-bestpractices-part-7-tips-tools-coding-best-practices.aspx

Should All Data Be Encrypted By Default?
http://blogs.msdn.com/b/buckwoody/archive/2011/08/09/should-all-data-be-encryptedby-default.aspx

Crypto Primer: How does SSL work?
http://blogs.msdn.com/b/plankytronixx/archive/2010/10/28/crypto-primer-how-does-sslwork.aspx

Windows Azure Data Security (Cleansing and Leakage)
http://blogs.msdn.com/b/walterm/archive/2012/02/01/windows-azure-data-cleansingand-leakage.aspx

Crypto Services and Data Security in Microsoft Azure http://msdn.microsoft.com/en-us/magazine/ee291586.aspx

Deploying Highly Available and Secure Cloud Solutions
http://Aka.ms/avail

10 Things to know about Azure Security http://technet.microsoft.com/en-us/cloud/gg663906.aspx
Windows Azure Security Essentials
http://technet.microsoft.com/en-us/gg621084.aspx

Azure SQL Database and SQL Server - Performance and Scalability Compared and Contrasted
http://msdn.microsoft.com/en-us/library/windowsazure/jj879332.aspx

Azure Table Storage and Windows Azure SQL Database - Compared and Contrasted
http://msdn.microsoft.com/en-us/library/windowsazure/jj553018.aspx

Data Series: Exploring Windows Azure Drives, Disks, and Images
http://azure.microsoft.com/blog/2012/06/27/data-series-exploring-windows-azuredrives-disks-and-images/

Authenticating Access to Your Azure Storage Account http://msdn.microsoft.com/en-us/library/hh225339.aspx

How to: Implement Role Based Access Control (RBAC) in a Claims-Aware ASP.NET Application Using WIF and ACS
http://msdn.microsoft.com/en-us/library/gg185914.aspx

Understanding the Temporary Drive on Azure Virtual Machines
http://blogs.msdn.com/b/wats/archive/2013/12/07/understanding-the-temporary-driveon-windows-azure-virtual-machines.aspx

RMS Boot Camp http://curah.microsoft.com/56313/boot-camp-for-windows-azure-rights-managementrms

Qualys SSL Labs: https://www.ssllabs.com/ssltest/analyze.html?d=app.formiik.com