CENTROS DE DATOS, CERTIFICACIONES, SEGURIDAD/AUDITORIA, POLITICAS DE BACKUP, RECUPERACION DE DESASTRES Y ARQUITECTURA.

AUTHOR
iMedical Services SAS

Versión 1.3

Fecha Actualización : marzo/09/2023

info@imedicalservices.co

http://www.imedicalservices.co Todos los derechos reservados © 2023.

Tabla de Contenido

Introducción 2
Audiencia 2
Microsoft Azure 2
Regiones de Azure 2
Certificaciones 3
Centro de seguridad de Azure 3
Almacenamiento 4
Arquitectura iMedicalCloud en Azure 6
Aplicación Web, Servicios y Procesos en Background 6
Almacenamiento 8
Monitoreo y Soporte 9
Azure SQL Base de datos 10
Auditoría de bases de datos Azure SQL Database 10
Firewall de bases de datos Azure SQL Database 11
Cifrado de datos transparente para Azure SQL Database 13
Bases de Datos – Copias de seguridad 14
Recuperación de Desastres. 16

Introducción

Audiencia

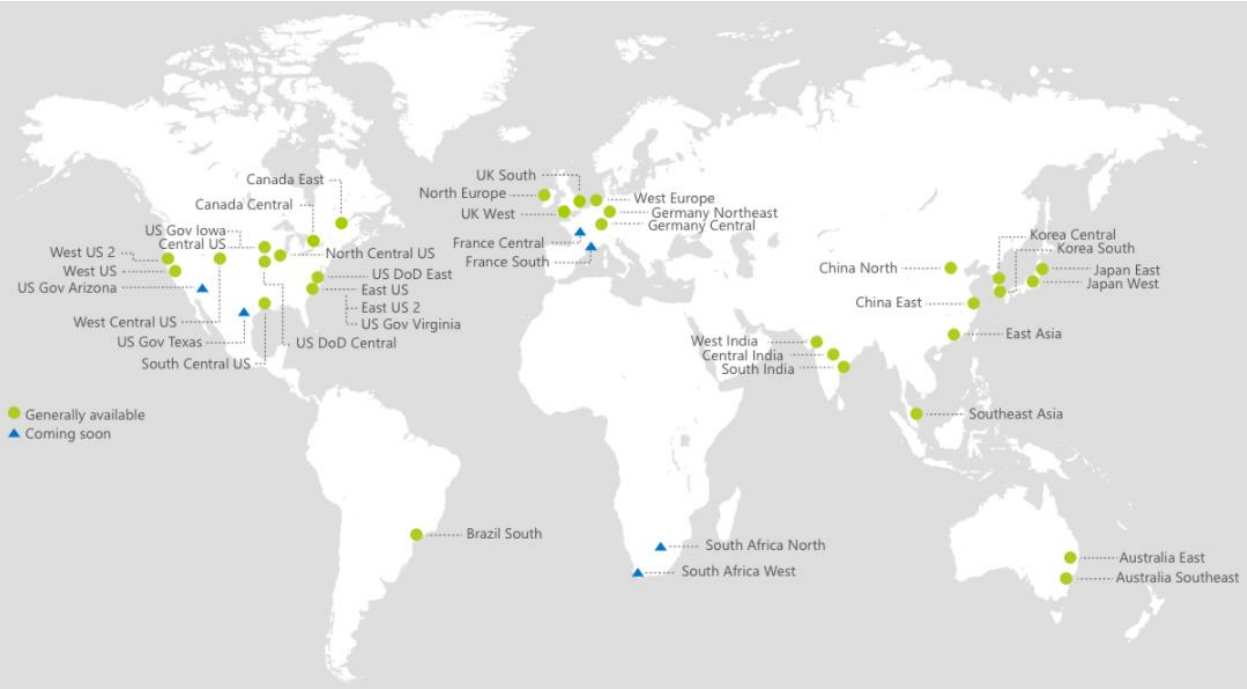
Este documento es un recurso para los profesionales de tecnología de la información (TI) y Auditoria de la información que describe como nuestra solución *iMedicalCloud* usa la nube de Microsoft y cumple con los más altos estándares de seguridad, backups, recuperación de desastres, calidad de la información y rendimiento de nuestro sistema.

Microsoft Azure

Microsoft Azure (anteriormente Windows Azure y Azure Services Platform) es un servicio en la nube ofrecida como servicio y alojado en los Data Centers de Microsoft. Anunciada en el Professional Developers Conference de Microsoft (PDC) del 2008 en su versión beta, pasó a ser un producto comercial el 1 de enero de 2010. Microsoft Azure es una creciente colección de servicios en la nube integrados que los desarrolladores y los profesionales de TI utilizan para crear, implementar y administrar aplicaciones a través de nuestra red global de centros de datos. Con Azure, se obtiene la libertad de crear e implementar donde quieran soluciones, utilizando las herramientas, las aplicaciones y los marcos de desarrollo que se prefieran.

Regiones de Azure

Azure tiene disponibilidad general en 34 regiones de todo el mundo, con previsiones anunciadas en 6 regiones adicionales. Otorga la más alta prioridad a la expansión geográfica, a fin de ofrecer mayor rendimiento y satisfacer las necesidades y preferencias a los clientes en cuanto a la ubicación de los datos.



Certificaciones

Para ayudarle a cumplir con los requisitos nacionales, regionales e industriales específicos que rigen la recopilación y el uso de los datos de las personas, Microsoft cumple con el mayor conjunto de certificaciones y estándares que cualquier proveedor de servicios en la nube.

La tabla de esta página contiene todas las certificaciones actuales y los filtros apropiados. Para encontrar información de auditoría, vaya a la certificación relacionada en el siguiente enlace. https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings



ISO/IEC



CSA/CCM



ITAR



CJIS



HIPAA



IRS 1075

Centro de seguridad de Azure

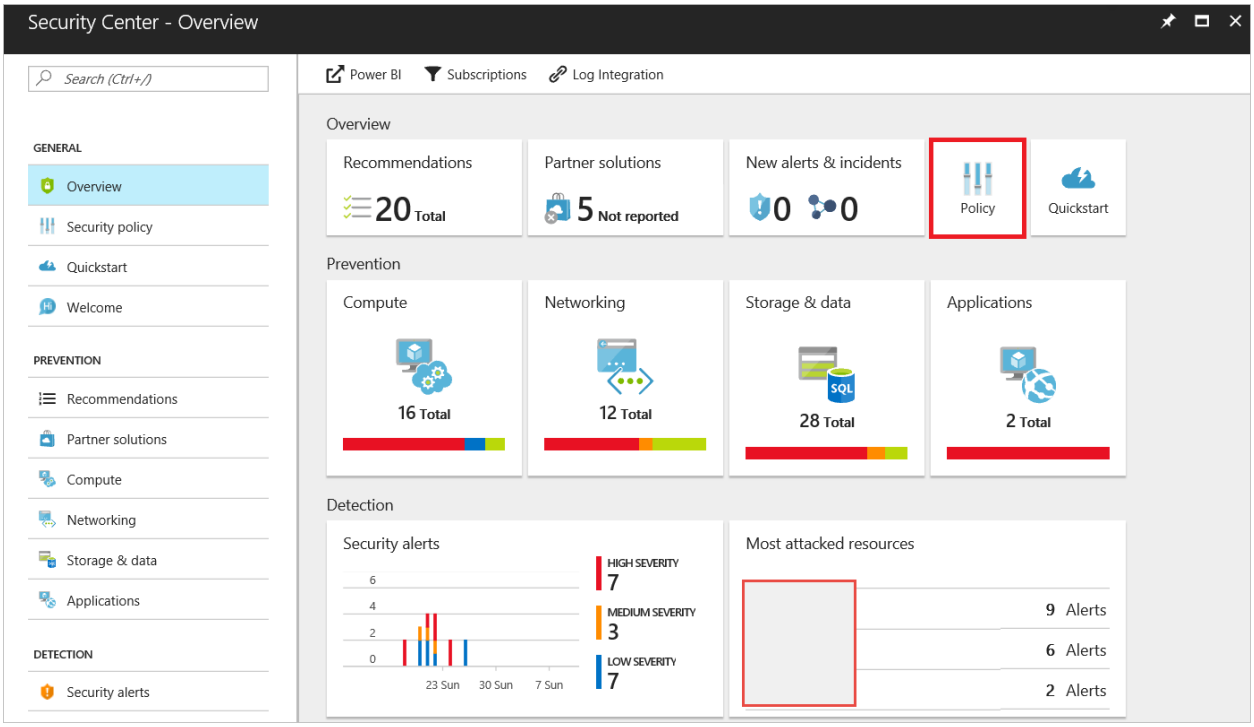
El Centro de seguridad ayuda a evitar, detectar y responder a amenazas con más visibilidad y control de la seguridad en los recursos de Azure. Proporciona administración de directivas y supervisión de la seguridad integrada en las suscripciones de Azure, ayuda a detectar las amenazas que podrían pasar desapercibidas y funciona con un amplio ecosistema de soluciones de seguridad.

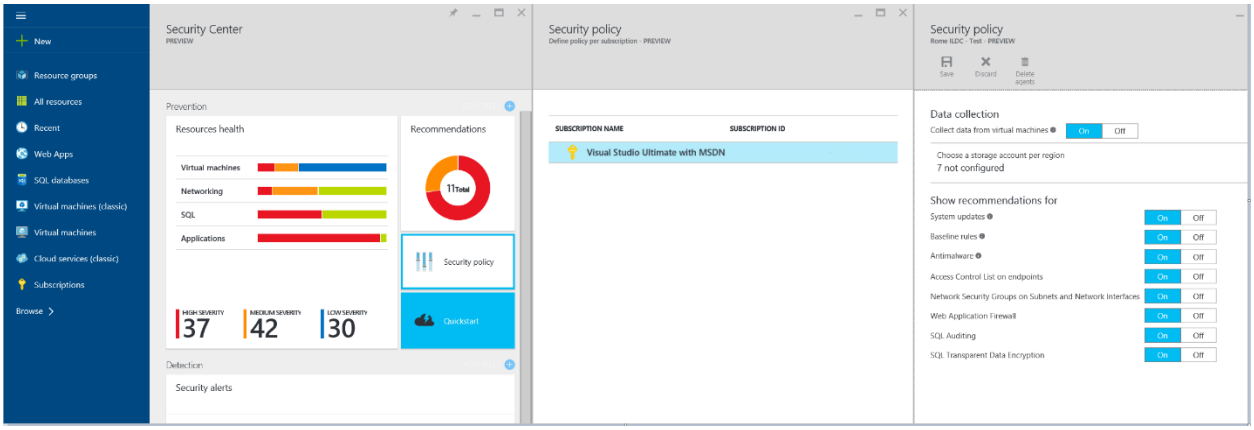
Principales capacidades

El Centro de seguridad ofrece las funcionalidades sencillas y eficaces de prevención, detección y respuesta ante amenazas integradas en Azure. Principales capacidades:

Fase	Capacidad
Prevención	Supervisa el estado de seguridad de los recursos de Azure
Prevención	Define las directivas de sus suscripciones y grupos de recursos de Azure en función de los requisitos de seguridad de su compañía, los tipos de aplicaciones que use y la confidencialidad de los datos
Prevención	Usa recomendaciones de seguridad controladas por directivas para guiar a los propietarios de los servicios a través del proceso de implementación de los controles necesarios
Prevención	Implementa rápidamente servicios y dispositivos de seguridad de Microsoft y asociados
Detección	Recopila y analiza automáticamente los datos de seguridad de los recursos de Azure, la red y las soluciones de asociados como firewalls y programas antimalware
Detección	Aprovecha la inteligencia de amenazas global de los productos y servicio de Microsoft, la Unidad de crímenes digitales de Microsoft, Microsoft Security Response Center (MSRC) y fuentes externas.
Detección	Aplica análisis avanzados, incluido el aprendizaje automático y el análisis de comportamientos
Respuesta	Proporciona seguridad prioritaria ante incidentes y alertas
Respuesta	Proporciona información sobre el origen del ataque y los recursos afectados
Respuesta	Sugiere formas de detener el ataque actual y de ayudar a impedir ataques futuros

La siguiente grafica muestra el panel de administración de seguridad que nuestra solución tiene con las diferentes alertas de nuestro centro de datos en Azure.





Almacenamiento

La informática en la nube posibilita nuevos escenarios para aplicaciones que requieren un almacenamiento escalable, duradero y de alta disponibilidad para sus datos, que es justo el motivo por el que Microsoft ha desarrollado Almacenamiento de Azure. Además de permitir a los desarrolladores compilar aplicaciones en la era de La informática en la nube posibilita nuevos escenarios para aplicaciones que requieren un almacenamiento escalable, duradero y de alta disponibilidad para sus datos, que es justo el motivo por el que Microsoft ha desarrollado Almacenamiento de Azure. Además de permitir a los desarrolladores compilar aplicaciones a gran escala para sustentar nuevos escenarios, Almacenamiento de Azure proporciona también la base de almacenamiento para Máquinas virtuales de Azure, una prueba más de su solidez.

Almacenamiento de Azure se puede escalar de forma masiva para almacenar y procesar cientos de **terabytes** de datos y admitir así los escenarios de datos de gran tamaño requeridos por las aplicaciones científicas, de salud, de análisis financiero, logístico, documental y multimedia. Igualmente, permite almacenar las pequeñas cantidades de datos que se necesitan en un sitio web de una pequeña empresa. Sean cuales sean sus necesidades, solo tiene que pagar por los datos que almacene. Actualmente, Almacenamiento de Azure alberga

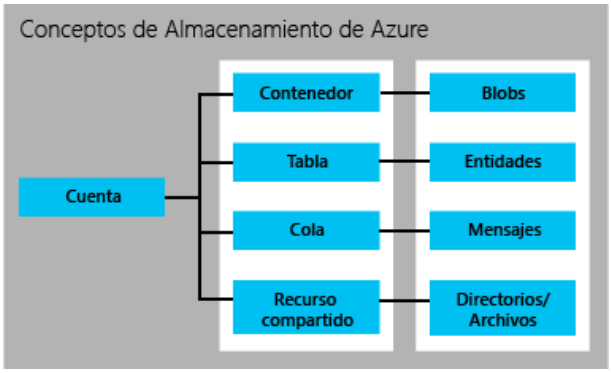
decenas de **billones** de objetos de cliente únicos y administra, por término medio, **millones** de solicitudes por **segundo**.

Almacenamiento de Azure utiliza un sistema de creación automática de particiones que equilibra la carga de los datos automáticamente en función del tráfico. Esto significa que, conforme crece la demanda en la aplicación, Almacenamiento de Azure asigna automáticamente los recursos adecuados para ajustarse a este requisito.

Puede obtener acceso a este servicio desde cualquier lugar del mundo y cualquier tipo de aplicación, ya se ejecute en la nube, en el escritorio, en un servidor local o en un dispositivo móvil o tableta. Almacenamiento de Azure se puede usar en escenarios móviles donde la aplicación almacena un subconjunto de datos en el dispositivo y los sincroniza con todo un conjunto de datos almacenados en la nube.

Almacenamiento de Azure admite clientes que utilizan una gran variedad de sistemas operativos (incluidos Windows y Linux) y diversos lenguajes de programación (incluidos .NET, Node.js, Python, Ruby, PHP y C++, así como lenguajes de programación móvil) para un desarrollo más práctico. Además, expone recursos de datos a través de sencillas API REST, disponibles para cualquier cliente capaz de enviar y recibir datos mediante HTTP/HTTPS.

Una cuenta de almacenamiento de Azure es una cuenta segura que proporciona acceso a los servicios del Almacenamiento de Azure. La cuenta de almacenamiento ofrece el espacio de nombres exclusivo para los recursos de almacenamiento. La siguiente imagen muestra las relaciones entre los recursos de Almacenamiento de Azure en una cuenta de almacenamiento:

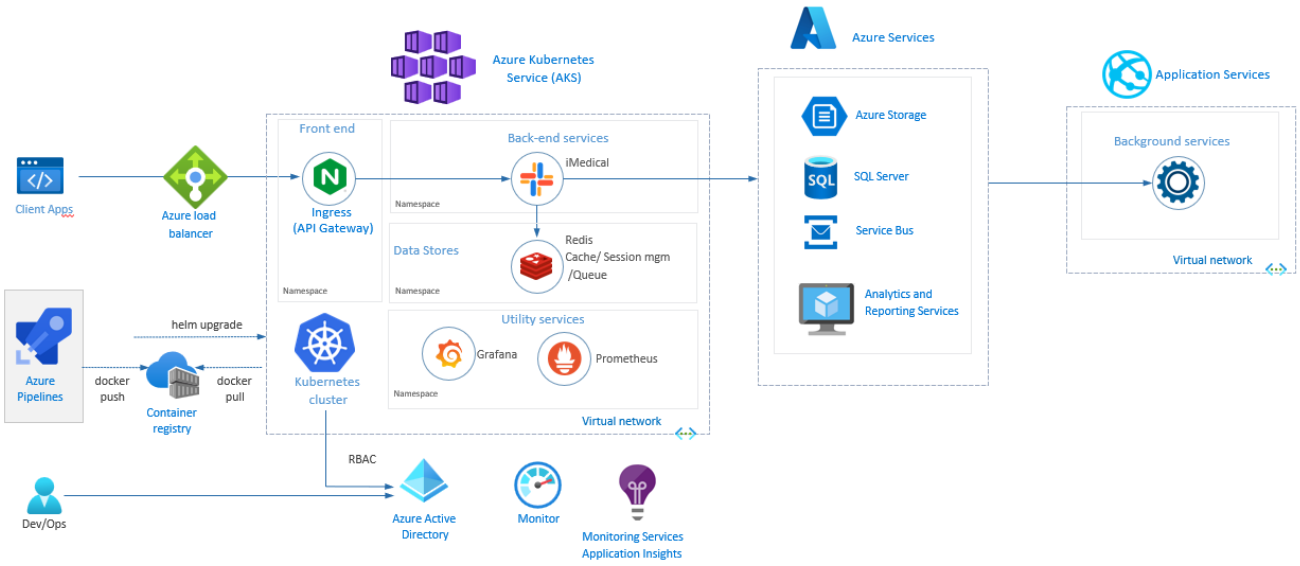


Arquitectura iMedicalCloud en Azure

iMedicalcloud es una solución 100% web diseñada para ser usa en modalidad de software como servicio y trabajar en el cloud computing de Microsoft Azure. Al estar diseñada para ser contenida en azure hereda todas las características de sus tecnologías anteriormente mencionadas, los siguientes diagramas muestran la arquitectura actual de iMedicalCloud en la nube.

Aplicación Web, Servicios y Procesos en Background

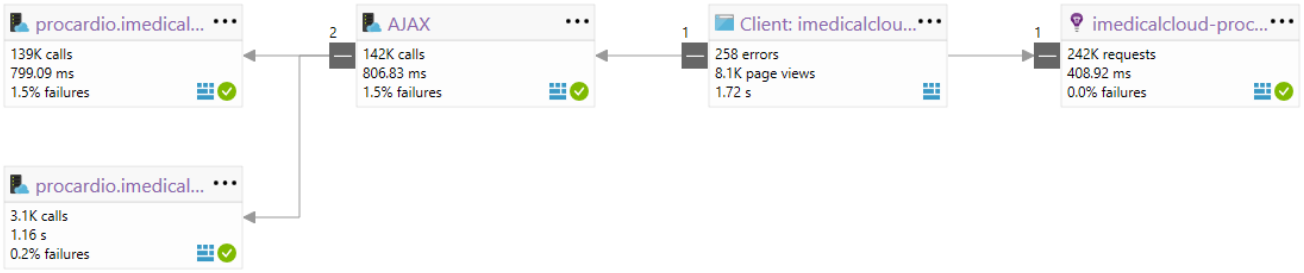
Las aplicaciones web están en modelo de servidor de aplicaciones hiper escalable en Kubernates que gestiona de forma automática el escalamiento dinámico de la aplicación dependiendo de variables como consumo de CPU y Memoria, garantizando esto que el sitio web brinde el mejor rendimiento posible sin importar la cantidad de usuarios que usen el sistema. La aplicación también cifra todas las comunicaciones entre los clientes y los diferentes sistemas usando conexiones cifradas vía HTTPS, la siguiente es la arquitectura sistema.



El sistema puede escalar dinámicamente hasta mil (1000) nodos en Linux/Windows actualmente el sistema tiene los siguientes:

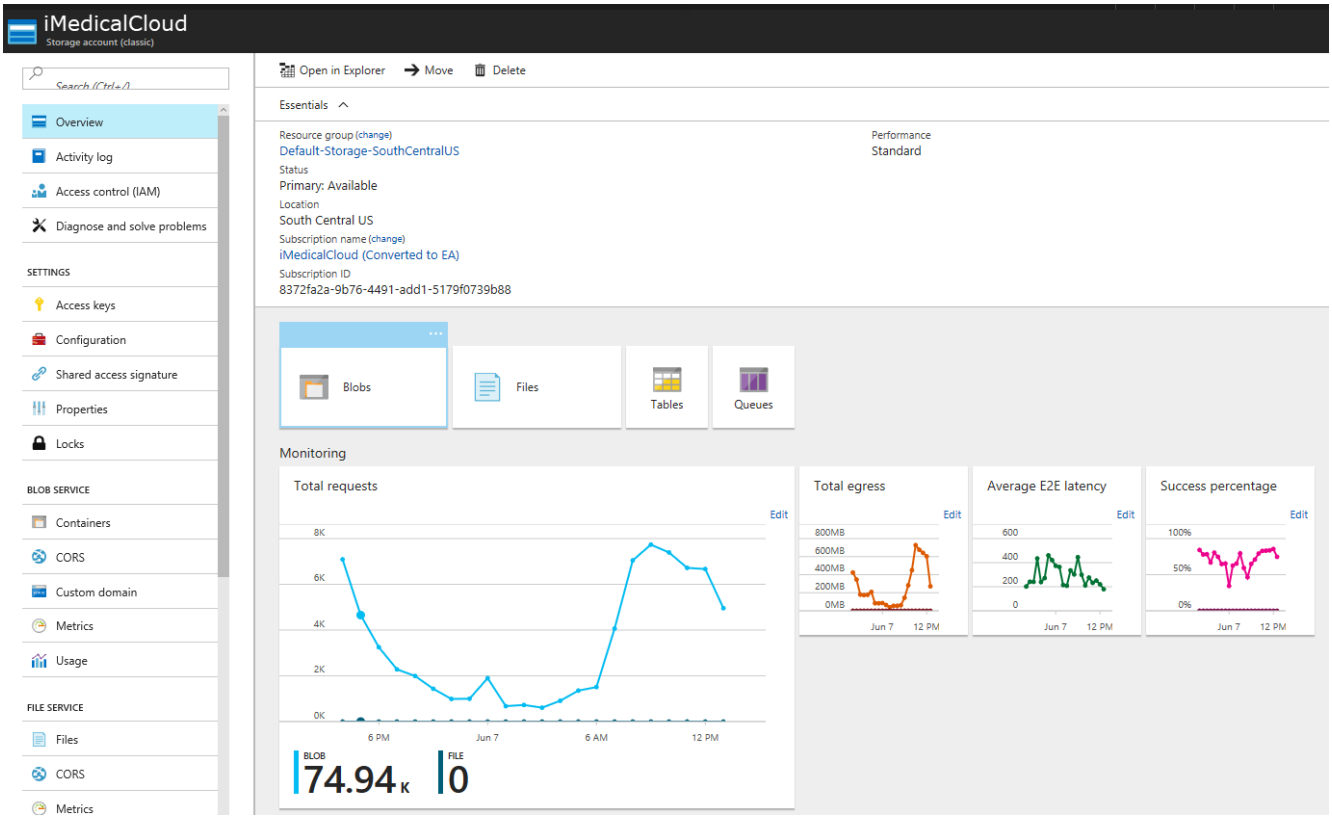
Node pool	Provisioning state	Power state	Node count	Mode	Kubernetes version	Node size	Operating system
syspool01	Succeeded	Running	2/2 ready	System	1.23.8	Standard_E4as_v5	Linux
win001	Succeeded	Running	3/3 ready	User	1.23.8	Standard_E8as_v5	Windows

El sistema de forma automática realiza un diagrama de red cada uno de los diferentes ambientes de producción he identifica las diferentes interfaces internas y externas que el sistema cuenta. Actualmente iMedical cuenta con 5 nodos dos Linux (8 vCores y 64 GB de memoria) y 3 Windows (24 vCores y 64 GB de memoria)


procardio.imedical...
139K calls
799.09 ms
1.5% failures
2
AJAX
142K calls
806.83 ms
1.5% failures
1
Client: imedicalclou...
258 errors
8.1K page views
1.72 s
1
imedicalcloud-proc...
242K requests
408.92 ms
0.0% failures
procardio.imedical...
3.1K calls
1.16 s
0.2% failures

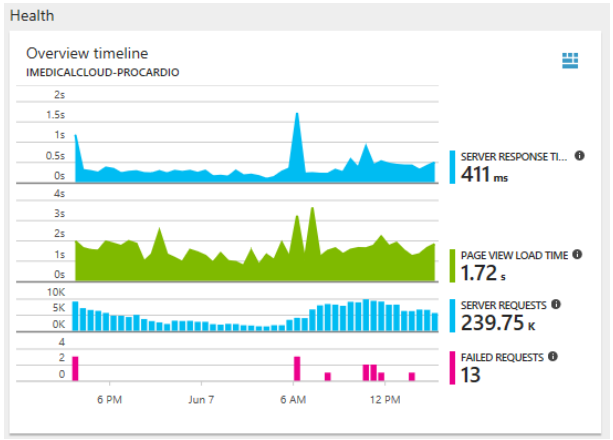
Almacenamiento

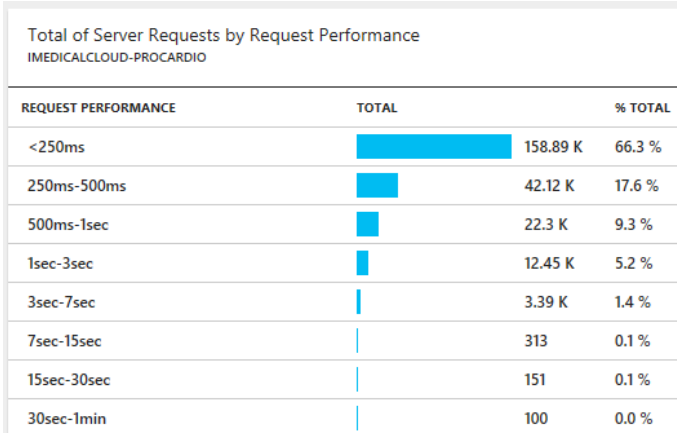
En Azure Storage o almacén de datos iMedicalCloud almacena y respalda toda la información de los diferentes archivos cargados a las historias clínicas, garantizando según la ley colombiana copias de esta información hasta por 15 años o con acuerdos con algunos clientes por tiempo ilimitado mientras el contrato este vigente.

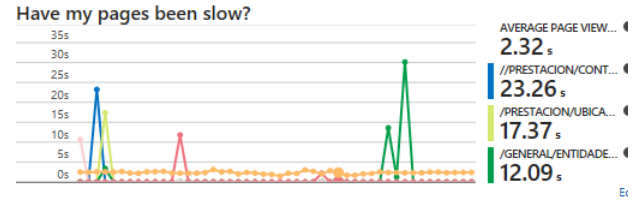


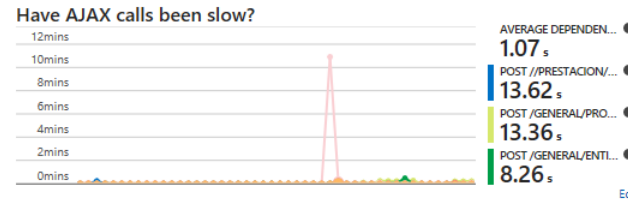
Monitoreo y Soporte

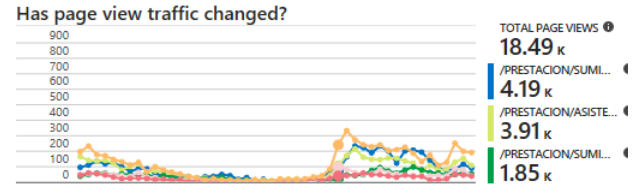
Nuestra solución cuenta con herramientas que generan métricas de rendimiento, tiempos de respuesta, fallos y alertas que nos permiten detectar de forma temprana diferentes problemas en la aplicación antes de que el cliente los reporte o se percate de ellos. Adicional podemos generar informes de tipos de navegadores que usa el cliente, versiones de sistemas operativos y tiempos de respuesta de su red, adicional proveemos un servicio en línea en donde se puede revisar la disponibilidad del sistema en tiempo real [iMedical Estado de Servicios (imedicalcloud.net)]

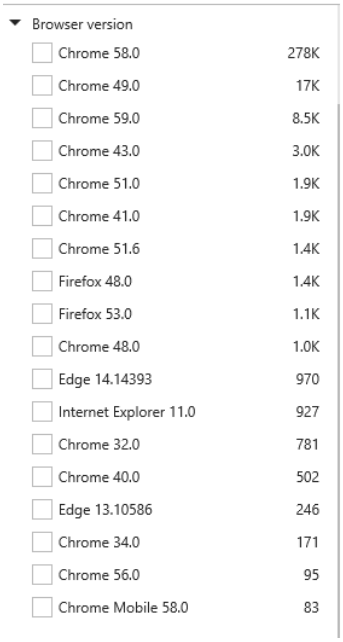


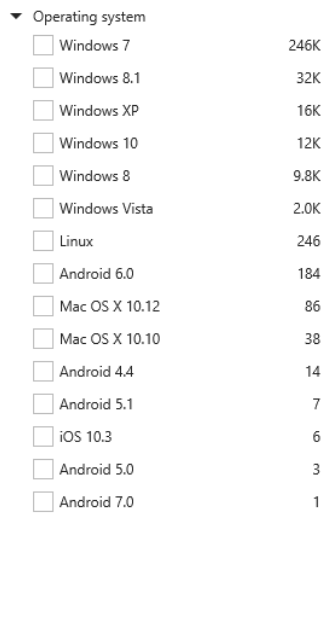






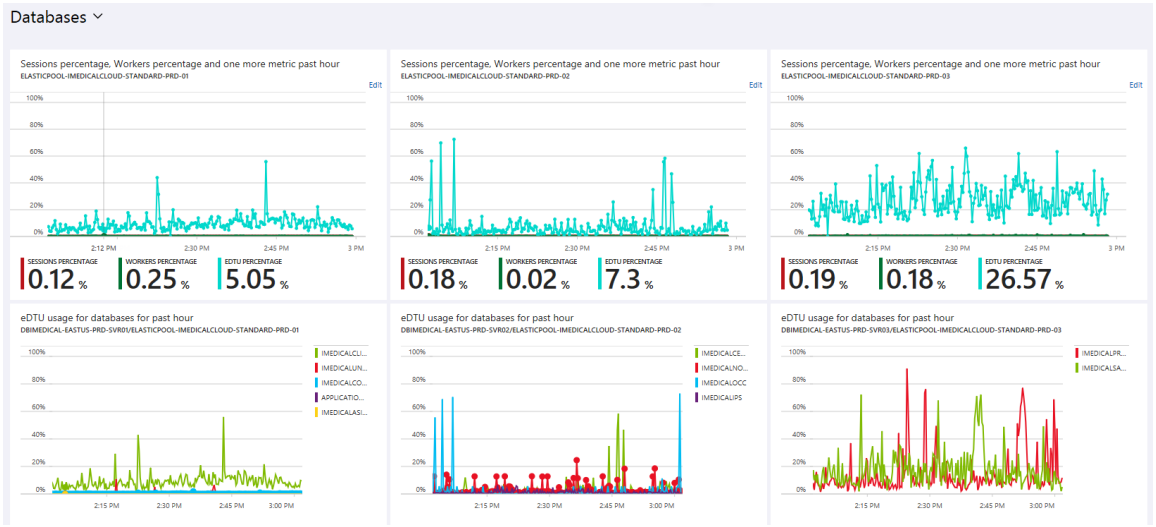






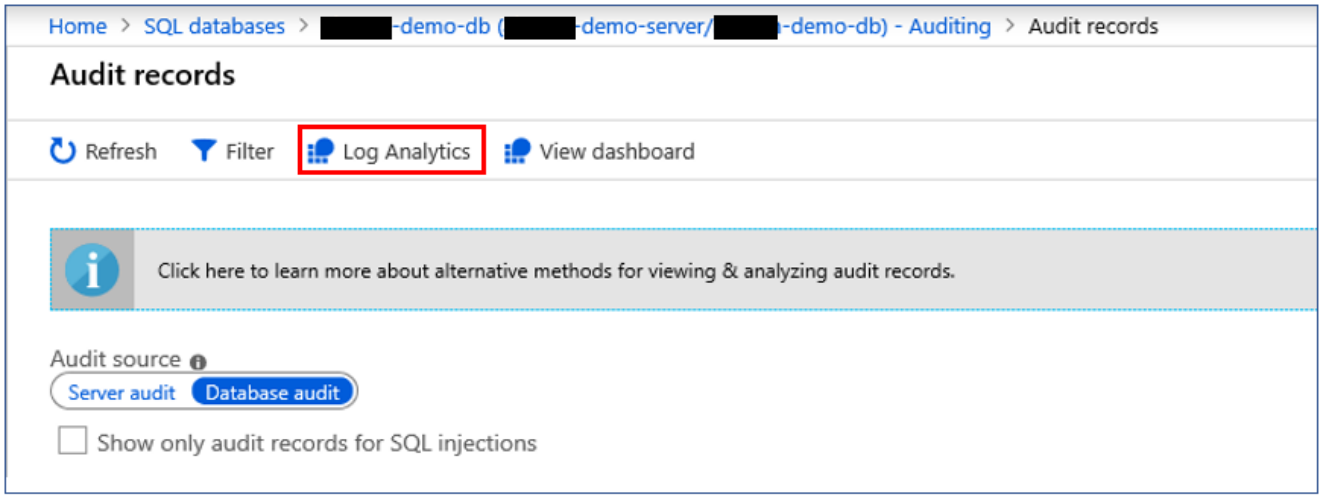
Azure SQL Base de datos

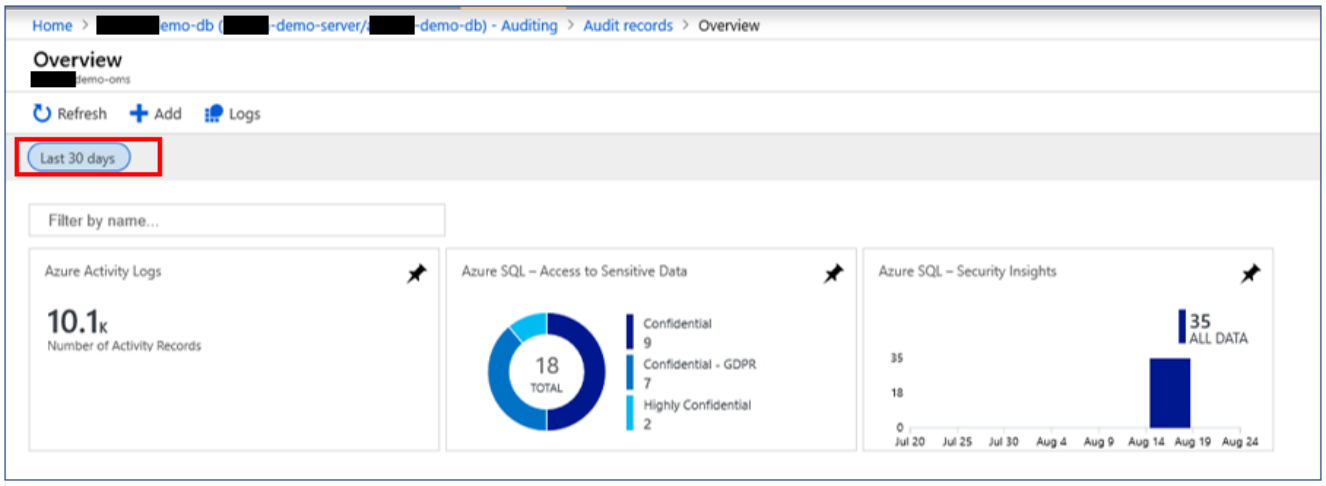
Nuestra solución usa Azure SQL para toda la administración de base de datos los servidores cuentan con respaldo automático y recuperación de desastres automática. Azure nos garantiza un SLA en SQL Azure del 99.99%. equivale esto a máximo 1 hora acumulada por fuera al año en caso de fallas. Pueden garantizar esta disponibilidad ya que las bases de datos estas almacenadas en servidores en clúster altamente redundantes que puede crecer dinámicamente hasta 128 vCores y 625 GB de memoria, en el clúster las bases de datos se encuentran encriptadas y los backups también se almacenan encriptados en zona GEO-Redundante.

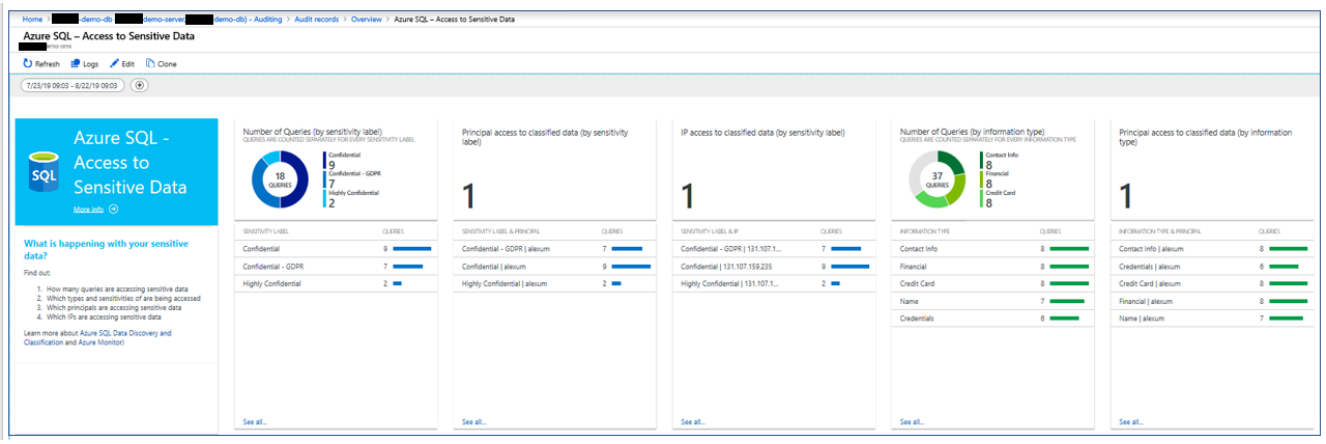


Auditoría de bases de datos Azure SQL Database

La auditoría de Azure SQL Database seguimiento de eventos de base de datos y los escribe en un registro de auditoría de la cuenta de Azure Storage, área de trabajo de Log Analytics o Event Hubs. La auditoría también da cumplimiento de normatividad, registra la actividad de las bases de datos y permite conocer las discrepancias y anomalías que pueden indicar problemas en el negocio o infracciones de seguridad sospechosas. Las siguientes son características de auditoria que iMedicalCloud usa de sus bases de datos alojadas en Azure SQL Database.







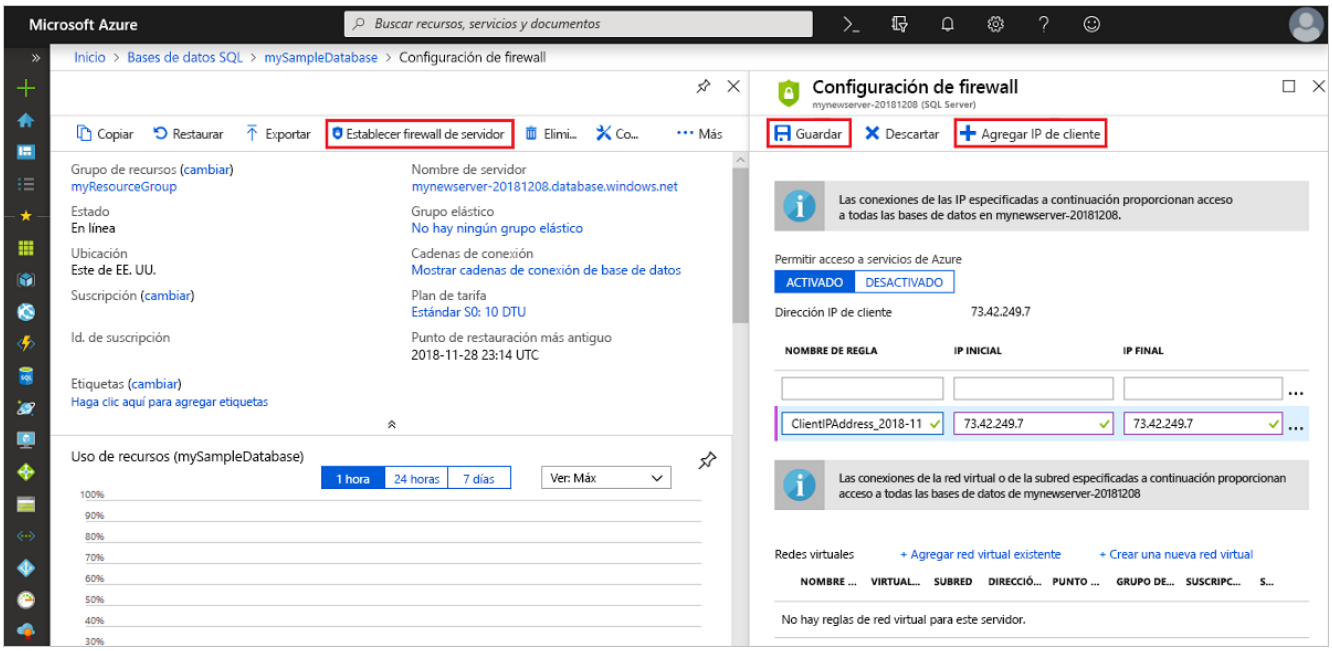
Firewall de bases de datos Azure SQL Database

El firewall de Azure SQL Database nos permite restringir el acceso no autorizado a las bases de datos y permite configurar desde que IP Address se pueden realizar una conexión, por defecto esta activo y solo permite conexión desde los endopoint de la VPN de Azure de la capa de servicios y de aplicación.

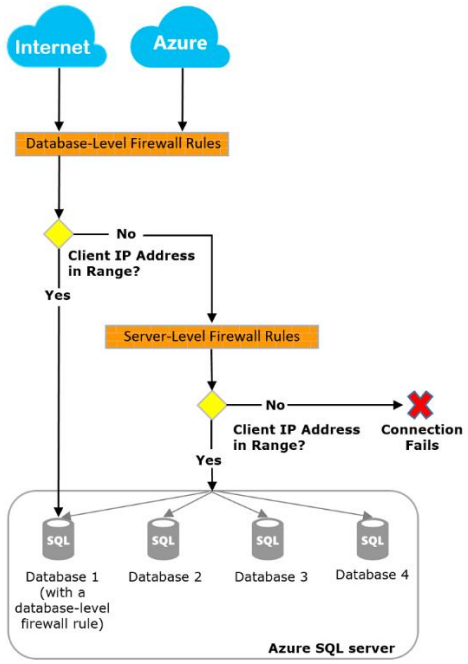
Enmascaramiento de datos dinámicos

Usamos en Azure SQL el enmascaramiento dinámico de datos. El enmascaramiento dinámico de datos limita la exposición de información confidencial ocultándolos a los usuarios sin privilegios.

El enmascaramiento de datos dinámicos ayuda a impedir el acceso no autorizado a datos confidenciales permitiendo a los usuarios designar la cantidad de los datos confidenciales que se revelarán con un impacto mínimo en el nivel de aplicación. Se trata de una característica de seguridad basada en directivas que oculta la información confidencial del conjunto de resultados de una consulta de campos designados de una base de datos, sin modificar los datos de esta última.



Arquitectura de Ejecución del Azure SQL Database Firewall.



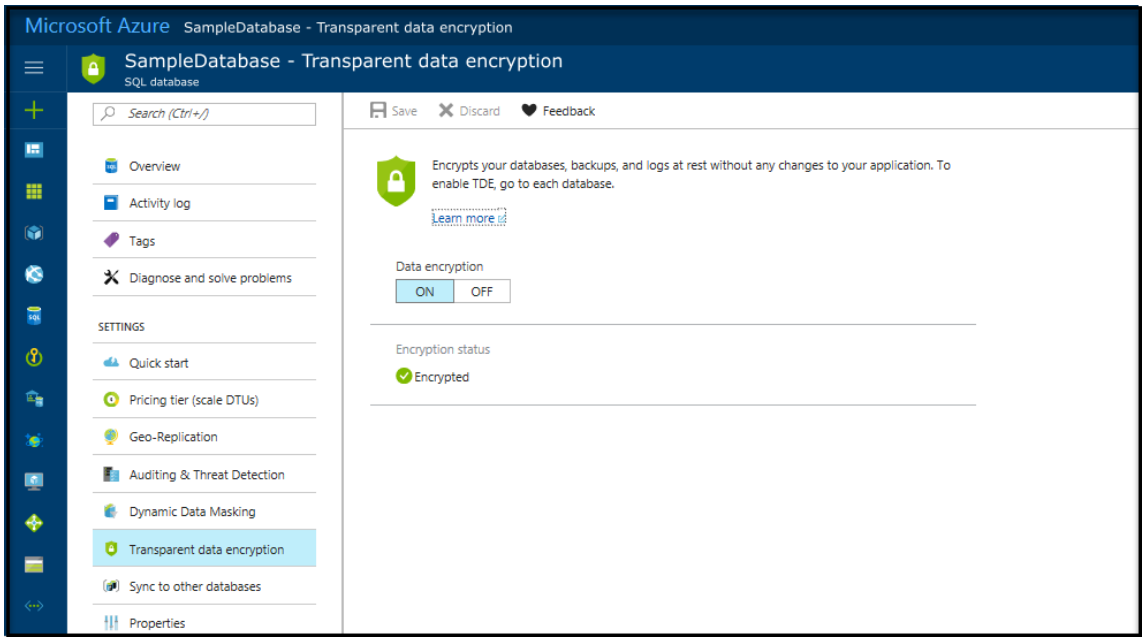
Cifrado de datos transparente para Azure SQL Database

El Cifrado de datos transparente (TDE) ayuda a proteger Azure SQL Database, frente a la amenaza de actividades malintencionadas sin conexión, ya que cifra los datos en reposo. También realiza cifrado y descifrado de la base de datos en tiempo real, copias de seguridad asociadas y archivos de registro de transacciones en reposo sin necesidad de efectuar cambios en la aplicación. De forma predeterminada, TDE está habilitado para todas las bases de datos de Azure SQL recién implementadas. TDE no se puede usar para cifrar la base de datos maestra lógica en SQL Database. La base de datos maestra contiene objetos que son necesarios para realizar las operaciones de TDE en las bases de datos de usuario.

TDE debe habilitarse manualmente para las bases de datos anteriores de Azure SQL Database, Las bases de datos de Instancia administrada creadas mediante restauración heredan el estado de cifrado de la base de datos de origen.

El cifrado de datos transparente se encarga de cifrar el almacenamiento de toda una base de datos mediante una clave simétrica denominada clave de cifrado de base de datos. Esta clave de cifrado de base de datos está protegida por el protector de cifrado de datos transparente. El protector es un certificado administrado por el servicio (cifrado de datos transparentes administrado por el servicio) o una clave asimétrica almacenada en Azure Key Vault (Bring Your Own Key). Establezca el protector de cifrado de datos transparente a nivel de servidor para Azure SQL Database y Data Warehouse, y a nivel de instancia para la Instancia administrada de Azure SQL Database. El término servidor hace referencia tanto a servidor como a instancia a lo largo de este documento, a menos que se indique lo contrario.

Durante el inicio de la base de datos, la clave de cifrado de base de datos cifrada se descifra y, a continuación, se usa para descifrar y volver a cifrar los archivos de base de datos en el proceso del motor de base de datos de SQL Server. El cifrado de datos transparente realiza el cifrado de E/S en tiempo real y el descifrado de los datos en el nivel de página. Todas las páginas se descifran cuando se leen en la memoria y, a continuación, se cifran antes de escribirse en el disco. Para consultar una descripción general del cifrado de datos transparente, consulte Cifrado de datos transparente (TDE).

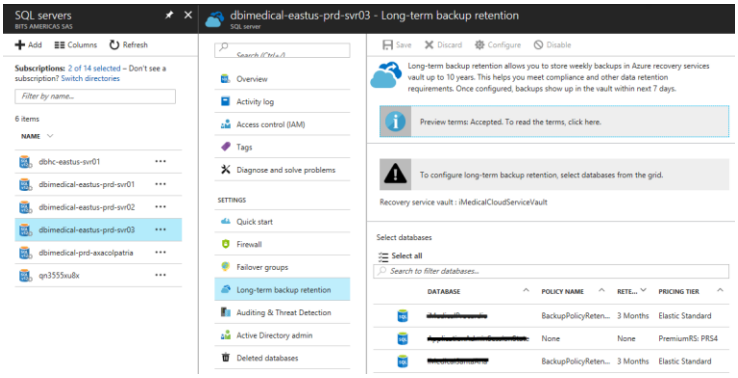


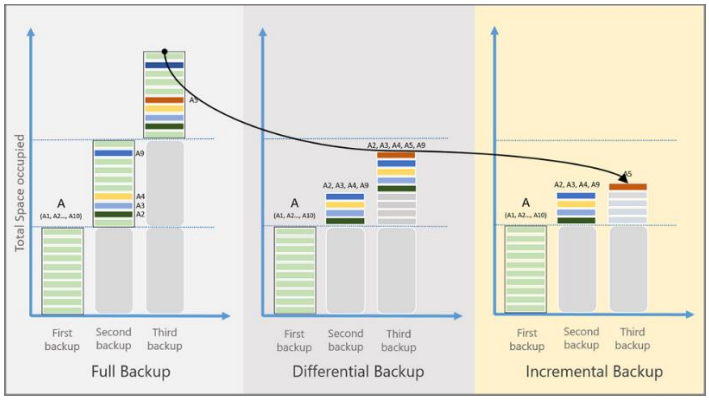
Bases de Datos – Copias de seguridad

Azure SQL Database emplea tecnología de SQL Server para crear copias de seguridad completas, diferenciales y del registro de transacciones. Por lo general, las copias de seguridad del registro de transacciones se producen cada 2-10 minutos, y la frecuencia depende del nivel de rendimiento y de la cantidad de actividad de la base de datos. Las copias del registro de transacciones, junto con las completas y diferenciales, permiten restaurar una base de datos a un momento específico en el mismo servidor que hospede la base de datos. Cuando se restaura una base de datos, el servicio calcula qué copia de seguridad completa, diferencial o del registro de transacciones es necesario restaurar.

Puede utilizar estas copias de seguridad para realizar lo siguiente:

- Restaurar una base de datos a un momento dado dentro del período de retención. Esta operación creará una base de datos nueva en el mismo servidor de la base de datos original.
- Restaurar una base de datos eliminada al momento en que se eliminó o a cualquier otro punto comprendido en el periodo de retención. La base de datos eliminada solo se puede restaurar en el mismo servidor donde se creará la original.
- Restaurar una base de datos en otra región geográfica. Esta opción permite recuperarse de un desastre en una región geográfica cuando no puede acceder a su servidor y base de datos. Crea una nueva base de datos en cualquier servidor existente del mundo.
- Restaurar una base de datos desde una copia de seguridad específica guardada en el almacén de Azure Recovery Services. Esta opción permite restaurar una versión antigua de la base de datos para respetar una solicitud de cumplimiento o ejecutar una versión antigua de la aplicación. Consulte el tema sobre la retención a largo plazo.





Servicio de Backup en Zona y Geo Redundante

Las soluciones de copia de seguridad tradicionales han evolucionado para tratar la nube como un punto de conexión, o destino de almacenamiento estático, similar a un disco o una cinta. Aunque este enfoque es simple, es limitado y no aprovecha una plataforma de nube subyacente, lo que se traduce en una solución ineficaz y costosa. Algunas soluciones son costosas porque se acaba pagando por el tipo incorrecto de almacenamiento o almacenamiento que no necesita. Otras soluciones a menudo son ineficaces porque no ofrecen el tipo o la cantidad de almacenamiento que necesita, o las tareas administrativas exigen demasiado tiempo. En cambio, Azure Backup proporciona las siguientes ventajas principales:

Administración de almacenamiento automática: los entornos híbridos requieren con frecuencia almacenamiento heterogéneo, unos locales y otros en la nube. Con Azure Backup, no hay ningún costo por el uso de dispositivos de almacenamiento local. Azure Backup asigna y administra automáticamente almacenamiento de copia de seguridad y emplea un modelo de pago por uso. Esto significa que solo paga por el almacenamiento que consume. Para más información, consulte el artículo sobre precios de Azure.

Escalado ilimitado: Azure Backup usa la eficacia subyacente y la escala ilimitada de la nube de Azure para proporcionar alta disponibilidad, sin sobrecarga de mantenimiento o supervisión. Puede configurar alertas para proporcionar información sobre los eventos, pero no tiene que preocuparse por la alta disponibilidad de los datos en la nube.

Varias opciones de almacenamiento: un aspecto de alta disponibilidad es la replicación del almacenamiento. Azure Backup ofrece dos tipos de replicación: almacenamiento con redundancia local, en Zona y almacenamiento con redundancia geográfica. Elija la opción de almacenamiento de copia de seguridad más acorde con sus necesidades:

- El almacenamiento con redundancia local (LRS) replica los datos tres veces (crea tres copias de los datos) en un centro de datos emparejado de la misma región. LRS es una opción de bajo costo para proteger los datos contra errores de hardware local.
- El almacenamiento con redundancia geográfica (GRS) replica los datos en una región secundaria (a cientos de kilómetros de la ubicación principal del origen de datos). GRS cuesta más que LRS, pero proporciona un mayor nivel de durabilidad de los datos, incluso si hay una interrupción regional.

Transferencia de datos ilimitada: Azure Backup no limita la cantidad de datos de entrada y salida que se transfieren. Tampoco cobra por los datos que se transfieren. Sin embargo, si usa el servicio Azure Import/Export para importar grandes cantidades de datos, existe un costo asociado con los datos de entrada. Para más información sobre este costo, consulte Flujo de trabajo de copia de seguridad sin conexión en Azure Backup. Datos de salida hacen referencia a los datos transferidos desde un almacén de Recovery Services durante una operación de restauración.

Cifrado de datos: el cifrado de datos permite la transmisión y el almacenamiento seguros de los datos en la nube pública. La frase de contraseña de cifrado se almacena localmente y nunca se transmite ni se almacena en Azure. Si es necesario restaurar algunos de los datos, solo cuenta con la frase de contraseña o clave de cifrado.

Copia de seguridad coherente con la aplicación: tanto si va a realizar una copia de seguridad de un servidor de archivos, una máquina virtual o una base de datos SQL, debe saber que un punto de recuperación tiene todos los datos necesarios para restaurar la copia de seguridad. Azure Backup proporciona copias de seguridad coherentes con la aplicación, lo que garantiza que no se necesitan correcciones adicionales para restaurar los datos. La restauración de datos coherentes con la aplicación reduce el tiempo de restauración, lo que le permite volver rápidamente a un estado de ejecución.

Retención a largo plazo: en lugar de pasar las copias de seguridad de disco a cinta y luego trasladar la cinta a una ubicación externa, puede usar Azure para la retención a corto y largo plazo. Azure no limita la cantidad de tiempo que los datos permanecen en un almacén de Backup o Recovery Services. Los datos se pueden conservar en un almacén tanto tiempo como se desee. Azure Backup tiene un límite de 9999 puntos de recuperación por instancia protegida. Consulte la sección Copia de seguridad y retención de este artículo para obtener una explicación de la forma en que este límite puede afectar a sus necesidades de copia de seguridad.

Recuperación de Desastres.

¿Qué diferencias hay entre Copia de seguridad de Azure y Azure Site Recovery?

Azure Backup y Azure Site Recovery tienen en común que ambos servicios realizan una copia de seguridad de los datos y pueden restaurar dichos datos. Sin embargo, estos servicios atienden a finalidades distintas para proporcionar recuperación ante desastres y continuidad empresarial en su organización. Usamos Azure Backup para proteger y restaurar datos en un nivel más pormenorizado. Por ejemplo, si una aplicación de un servidor resulta dañada, podría usar Azure Backup para restaurarla. Si desea replicar la configuración y los datos de una máquina virtual en otro centro de datos, utilice Azure Site Recovery.

Azure Backup protege los datos locales y en la nube. Azure Site Recovery coordina la replicación de la máquina virtual y el servidor físico, la conmutación por error y la conmutación por recuperación. Ambos servicios son importantes porque la solución de recuperación ante desastres debe mantener los datos seguros y recuperables (Copia de seguridad) y mantener las cargas de trabajo disponibles (Recuperación del sitio) cuando se producen interrupciones.

Detalles Copia de seguridad Recuperación ante desastres (DR)

Concepto	Detalles	Copia de seguridad	Recuperación ante desastres (DR)
Objetivo de punto de recuperación (RPO)	La cantidad aceptable de pérdida de datos si debe realizarse una recuperación.	Las soluciones de copia de seguridad tienen una gran variabilidad en su RPO aceptable. Las copias de seguridad de máquina virtual normalmente tienen un RPO de un día, mientras que las copias de seguridad de base de datos tienen RPO bajos, de hasta 15 minutos.	Las soluciones de recuperación ante desastres tienen RPO bajos. La copia de DR puede estar detrás de algunos segundos o minutos.
Objetivo de tiempo de recuperación (RTO)	La cantidad de tiempo que se tarda en completar una recuperación o restauración.	Debido a un RPO mayor, la cantidad de datos que una solución de copia de seguridad debe procesar es normalmente mucho mayor, lo que da lugar a RTO más largos. Por ejemplo, la restauración de datos de cintas puede tardar días, dependiendo del tiempo necesario para transportar la cinta desde una ubicación externa.	Las soluciones de recuperación ante desastres tienen RTO más pequeños, ya que están más en sincronización con el origen. Además, se necesita procesar menos cambios.
Retención	¿Cuánto tiempo necesitan almacenarse los datos?	En escenarios que requieren recuperación de operaciones (daños en los datos, eliminación involuntaria de archivos o errores del SO), los datos de copia de seguridad normalmente se conservan durante 30 días o menos.	La recuperación ante desastres solo necesita datos de recuperación operativos, lo que normalmente tarda unas pocas horas o hasta un día. Debido a la captura de datos específicos que se usa en soluciones de recuperación ante desastres, la retención a largo plazo no se recomienda si se usan datos de recuperación ante desastres.