centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 884C

Guía de configuración segura para SQL Database

ENERO 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.01.13 12:14:44 +01'00'

NIPO: 083-19-259-8

Fecha de Edición: enero de 2020

Plain Concepts ha participado en la realización y modificación del presente documento y sus anexos. Sidertia Solutions S.L. ha participado en la revisión de esta guía.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA AZURE SQL DATABASE 5
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA 5
2. DESPLIEGUE DE AZURE SQL DATABASE 5
2.1 PRERREQUISITOS PARA EL DESPLIEGUE MEDIANTE POWERSHELL 5
2.2 DESPLIEGUE DE AZURE SQL DATABASE MEDIANTE POWERSHELL 5
2.2.1.1 DESPLIEGUE POWERSHELL 5
2.2.1.2 DESPLIEGUE POR EL PORTAL AZURE. 6
3. CONFIGURACIÓN DE AZURE SQL DATABASE 9
3.1 MARCO OPERACIONAL 9
3.1.1 CONTROL DE ACCESO 9
3.1.1.1 IDENTIFICACIÓN 9
3.1.1.2 REQUISITOS DE ACCESO 9
3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS 12
3.1.1.4 MECANISMO DE AUTENTICACIÓN 14
3.2 EXPLOTACIÓN 16
3.2.1 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS 16
3.2.2 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS 17
3.2.3 MONITORIZACIÓN DEL SISTEMA 19
3.3 MEDIDAS DE PROTECCIÓN 22
3.3.1 PROTECCIÓN DE LAS COMUNICACIONES 22
3.3.1.1 PERÍMETRO SEGURO 22
3.3.2 PROTECCIÓN DE LA INFORMACIÓN 23
3.3.2.1 CALIFICACIÓN DE LA INFORMACIÓN 23
3.3.2.2 COPIAS DE SEGURIDAD (BACKUP) 24
3.4 SCRIPTS DE CONFIGURACIÓN 26
4. GLOSARIO Y ABREVIATURAS 27
5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD 29

1. Guía de configuración segura para Azure SQL Database

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo del presente guía es seguir las recomendaciones de seguridad en la utilización del servicio Azure SQL Database cumpliendo con los requisitos necesarios del Esquema Nacional de Seguridad en su categoría ALTA.

Azure SQL Database es una base de datos relacional de propósito general como servicio (DBaaS) basada en la última versión estable de Microsoft SQL Server Database Engine, de alto rendimiento, fiable y segura que puede utilizar para crear aplicaciones y sitios web basados en datos en el lenguaje de programación de su elección, sin necesidad de gestionar la infraestructura.

2. DESPLIEGUE DE AZURE SQL DATABASE

2.1 Prerrequisitos para el despliegue mediante PowerShell

A continuación, se detallan los prerrequisitos para el despliegue de la instalación de SQL Database.

Requisitos de sistema:

Como requisito de sistema operativo es recomendable que consulte el siguiente link de Microsoft.

https://docs.microsoft.com/es-es/powershell/scripting/install/windows-powershell-system-requirements?view=powershell-6

Instalación PowerShell

1. Se debe conectar al módulo de PowerShell.
2. Instalar el módulo desde Powershell.

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

2.2 Despliegue de Azure SQL Database mediante PowerShell

El despliegue de Azure SQL se puede realizar desde el portal de Azure o bien desde el script que se comenta a continuación.

Nota: *Es importante que en el script se escriba el nombre que tendrá el servidor y la ubicación donde se va a desplegar.*

2.2.1.1 Despliegue Powershell

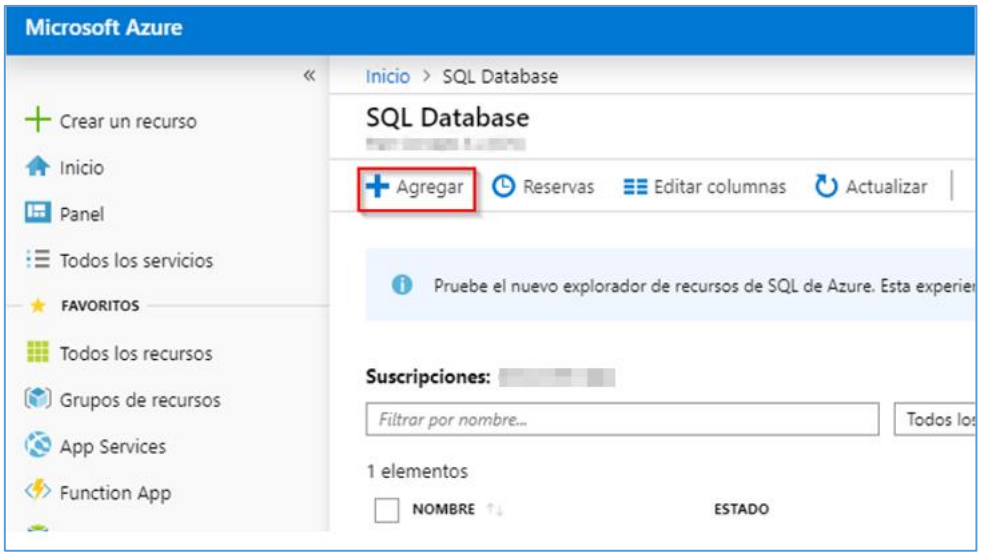
1. Copiar el contenido del script y ejecutar en PowerShell.

```
#   ## Se declaran las variables que son necesarias para la ejecución del script.
#   $serverName= "Nombre del Servidor"
#   $Location= "Nombre de localización Ej. "Nort Europe""
#   $resourceGroupName= "Nombre del Grupo de Recursos donde se creará el servidor"
#   $databaseName = "Nombre de la base de datos"
#   $adminSqlLogin = "Nombre Administrador de la base de datos"
#   $Password= "Escriba la contraseña"
#
#   ## Se encripta la contraseña de la variable Password para securizarla.
#   $PasswordSegura = ConvertTo-SecureString -String $Password -AsPlainText -Force
#
#   ## Para la creación del servidor que albergara la base de datos se necesita crear el
    objeto credencial donde contendrá el nombre del usuario administrador y la contraseña
    segura.
#   $credentialObject = New-Object -TypeName System.Management.Automation.PSCredential `
#         -ArgumentList $adminSqlLogin,`
#          $PasswordSegura
#
#   ##Creamos el servidor en Azure con los parámetros definidos previamente
#     $server = New-AzSqlServer -ResourceGroupName $resourceGroupName `
#         -ServerName $serverName `
#         -Location $location `
#         -SqlAdministratorCredentials $credentialObject
#   ## Creamos la base de de datos en el servidor creado previamente
#         $database = New-AzSqlDatabase  -ResourceGroupName $resourceGroupName `
#         -ServerName $serverName `
#         -DatabaseName $databaseName `
#         -RequestedServiceObjectiveName "S0"
```

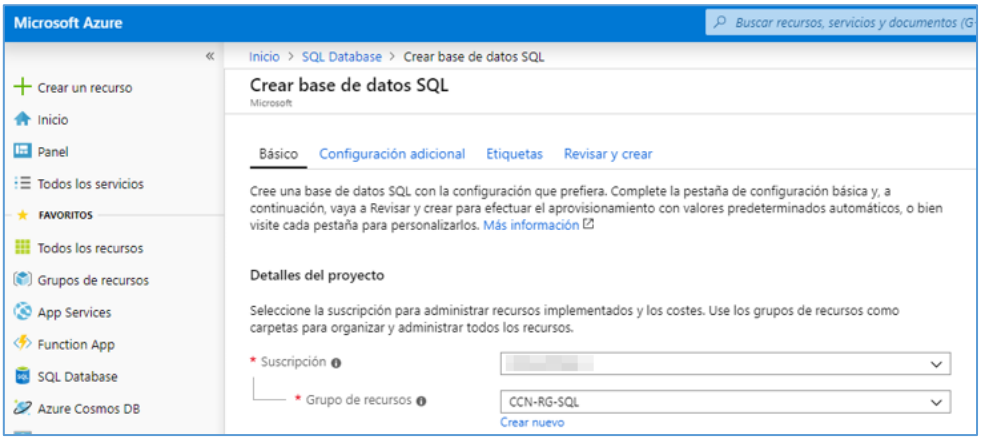
2.2.1.2 Despliegue por el portal Azure.

1. Buscar SQL Database.

2. Pulsar en [agregar].



3. Se debe seguir el asistente de configuración.

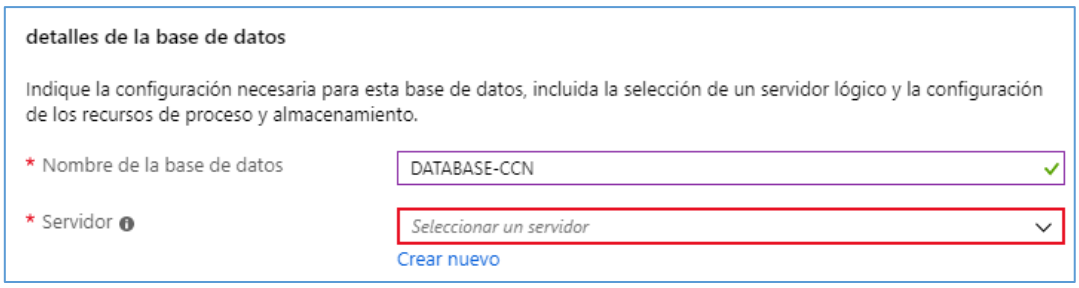


4. Se debe crear un nuevo grupo de recursos.

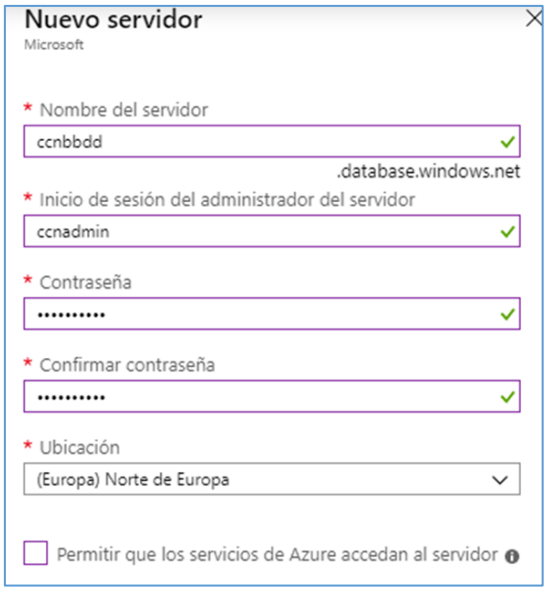
Nota: *Para una gestión más avanzada hay que recurrir al apartado [2.3 Gestión de recursos Azure/Grupo de recursos] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

Nombre de la base de datos: Definir un nombre para la base de datos.

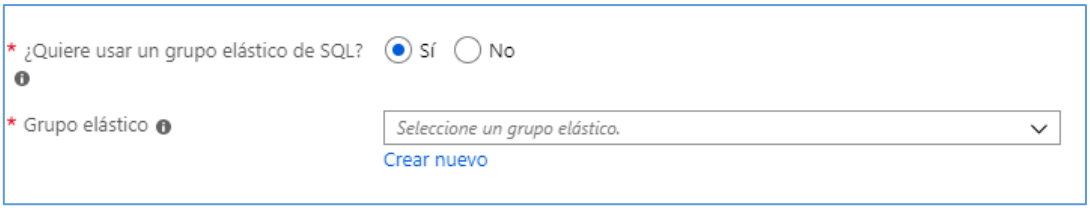
5. **Servidor:** Pulsar en [crear nuevo].



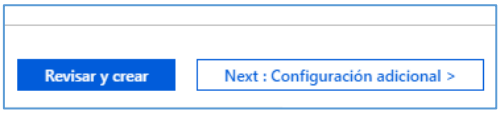
6. Se debe rellenar los campos que se solicita para el nuevo servidor.



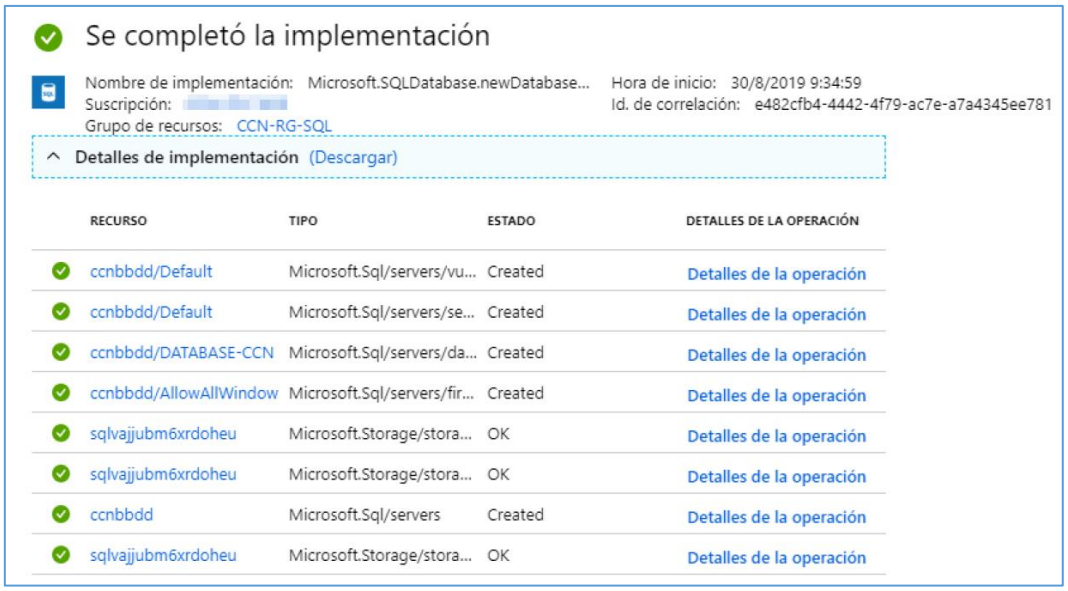
- **Nombre del servidor:** Nombre que tendrá la máquina virtual.
- **Inicio de sesión del administrador del servidor:** Usuario Admin local
- **Contraseña:** Se recomienda una contraseña compleja.
- **Ubicación:** Seleccionar Norte de Europa
- **Permitir que los servicios de Azure accedan al servidor:** La opción de Permitir que los servicios de Azure accedan al servidor debe estar desmarcada.
- **Quiere usar un grupo elástico de SQL:** Es recomendable seleccionar el grupo elástico que le permite administrar el rendimiento de múltiples bases de datos y almacenamiento compartido configurando límites.
- **Grupo elástico:** Pulsar en [crear nuevo]



7. Pulsar en [revisar y crear].



Nota: *La implementación del recurso puede tardar varios minutos hasta su finalización. Una vez haya finalizado verá la siguiente información.*



3. CONFIGURACIÓN DE AZURE SQL DATABASE

3.1 Marco operacional

3.1.1 Control de Acceso

3.1.1.1 Identificación

Azure AD proporciona la administración de identidades basada en la nube y permite usar una identidad única en todo su *Tenant* y las aplicaciones de acceso en Azure.

Se recomienda que para la gestión de los administradores se utilice Azure Active directory en la gestión de cuentas de administradores y delegación en base de datos.

Nota: *Para una gestión más avanzada hay que recurrir al apartado [3.1.1 Azure Active Directory / Alta, baja y modificación de cuentas y grupos] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.1.1.2 Requisitos de acceso

En esta guía se trata la seguridad en el acceso a los servidores de SQL Database.

Para ello, se debe aplicar una capa de seguridad mediante RBAC creando un nuevo rol personalizado, permitiendo dar un privilegio de administración a los servidores de SQL.

Nota: *Recordar que tan sólo los usuarios que tengan permisos de creación de roles pueden crearlos.*

Los permisos son:

```
Microsoft.Authorization/roleDefinitions/write
Microsoft.Authorization/roleDefinitions/delete
```

Creación de ROL personalizado.

1. Desde Powershell ejecutar:

```
#    New-AzRoleDefinition -InputFile "c:\temp\SQLAdmRole.json"
```

Nota: *El fichero SQLAdmRole.Json se puede encontrar adjunto en el apartado de Scripts de Configuración de la presente guía.*

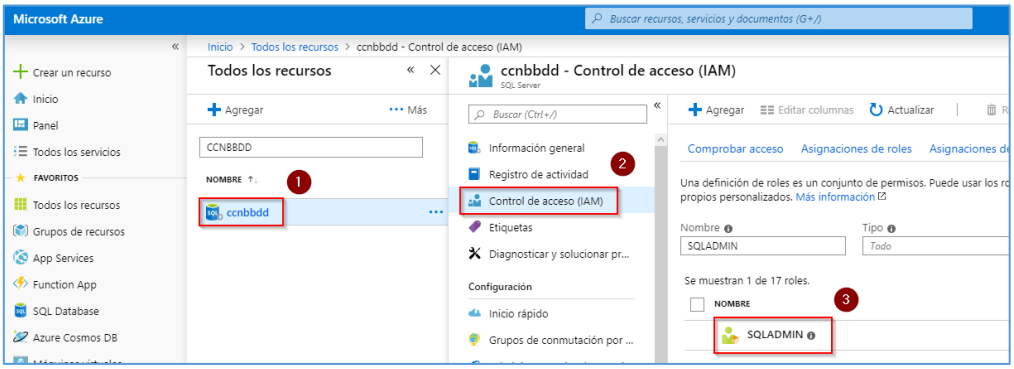
Al ejecutar este comando devuelve esta información.

```
Administrador: Windows PowerShell
PS C:\WINDOWS\system32> New-AzRoleDefinition -InputFile "c:\temp\SQLAdmRole.json"


Name             : SQLADMIN
Id               : c1a58e11-0521-455f-b505-516aab72d904
IsCustom         : True
Description      : Utilizado para gestionar SQL PaaS de Azure.
Actions          : {Microsoft.Authorization/*/read, Microsoft.Insights/alertRules/*,
                   Microsoft.ResourceHealth/availabilityStatuses/read, Microsoft.Resources/deployments/*...}
NotActions       : {Microsoft.Sql/managedInstances/databases/currentSensitivityLabels/*,
                   Microsoft.Sql/managedInstances/databases/recommendedSensitivityLabels/*,
                   Microsoft.Sql/managedInstances/databases/schemas/tables/columns/sensitivityLabels/*,
                   Microsoft.Sql/managedInstances/databases/securityAlertPolicies/*...}
DataActions      : {}
NotDataActions   : {}
AssignableScopes : {/subscriptions/965c7398-06c7-4edf-87ee-35744843942b}
```

Nota: *Recordar que puede comprobar este nuevo ROL desde el portal tal y como se indica a continuación.*

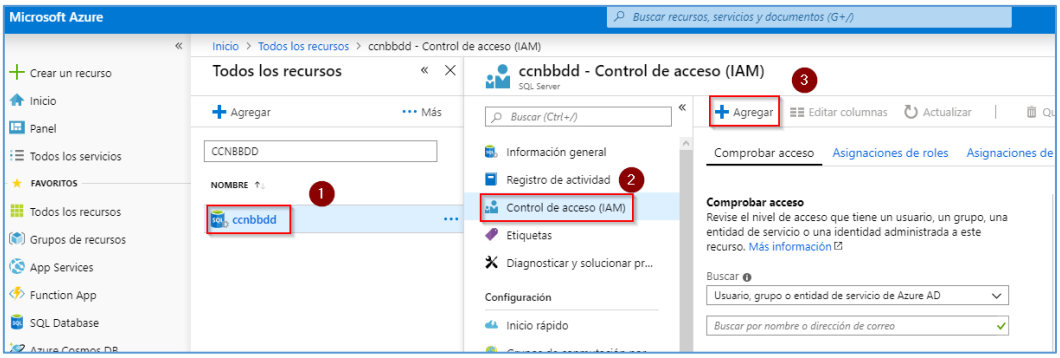
1. Pulsar en todos los recursos.
2. Buscar el nuevo servidor de SQL.
3. Pulsar en [Control de acceso/Roles].



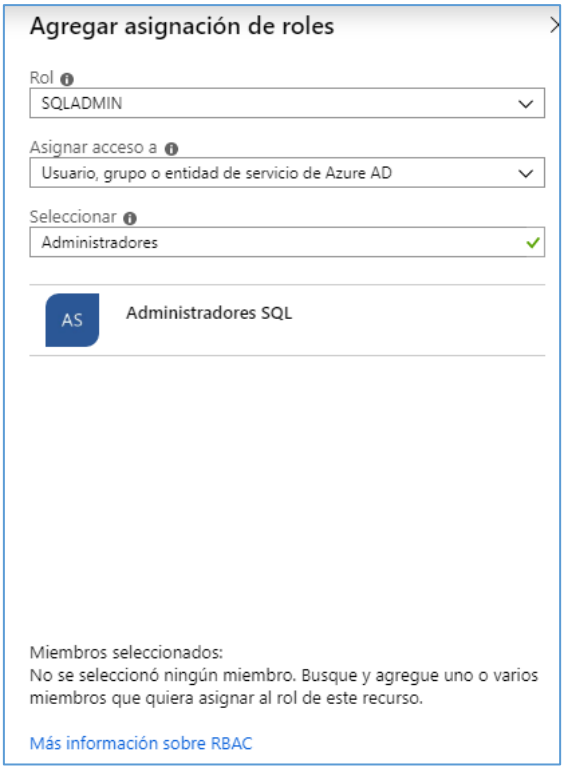
Desde ahí se puede ver el rol.

Asignación del nuevo rol

1. Pulsar en [todos los recursos].
2. Seleccionar la base de datos.
3. Pulsar en [Control de acceso/Agregar]



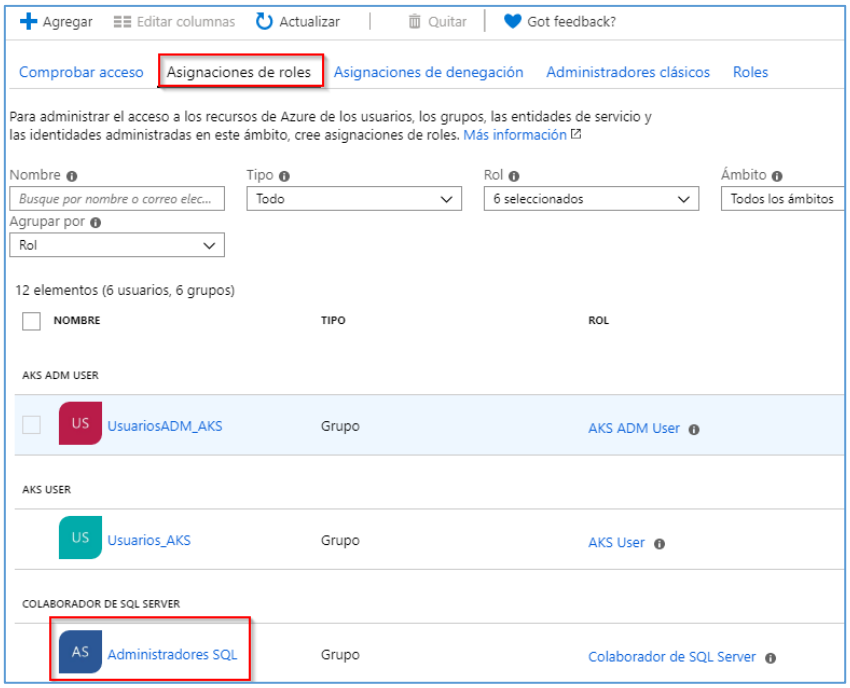
4. Completar los siguientes campos.



- **Rol:** Seleccionar el nuevo rol.
- **Asignar acceso:** Usuarios, grupos o entidades de servicio de Azure AD.
- **Seleccionar** el grupo de Administradores SQL.

5. Para finalizar pulsar en [agregar].

Puede consultar los roles en la pestaña [Asignación de roles].



Nota: *Esto es solo un ejemplo de la asignación de roles mediante **RBAC** los aplique desde el portal de Azure o los personalice.*

Nota: *Para una gestión más avanzada hay que recurrir al apartado [3.1.1.1 Requisitos de acceso/Control de acceso basado en roles] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.1.1.3 Segregación de funciones y tareas

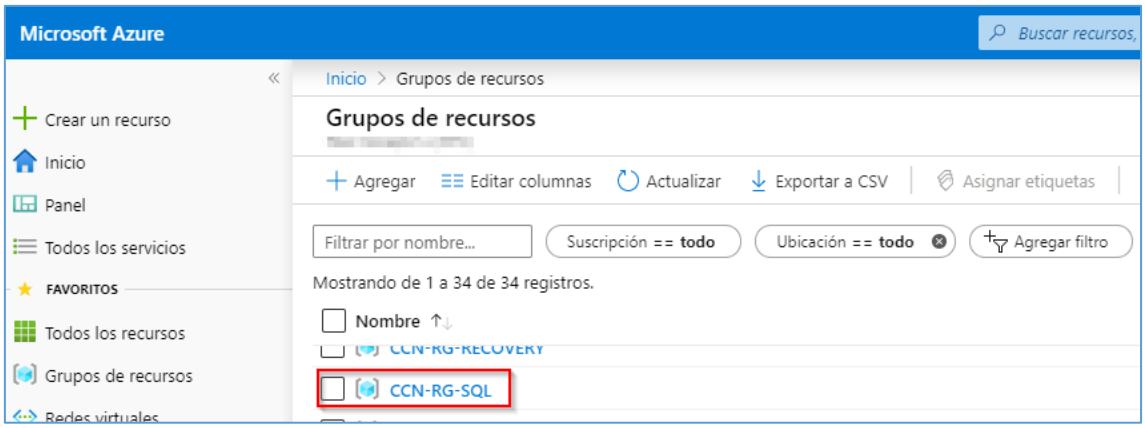
Para la segregación de funciones y tareas se recomienda que se aplique un control de acceso basado en rol **(RBAC)** como se ha mencionado anteriormente ya que tiene varios roles integrados para recursos de Azure que se pueden asignar a usuarios, grupos, entidades de servicio e identidades administradas.

Las asignaciones de roles sirven para controlar el acceso a los recursos de Azure.

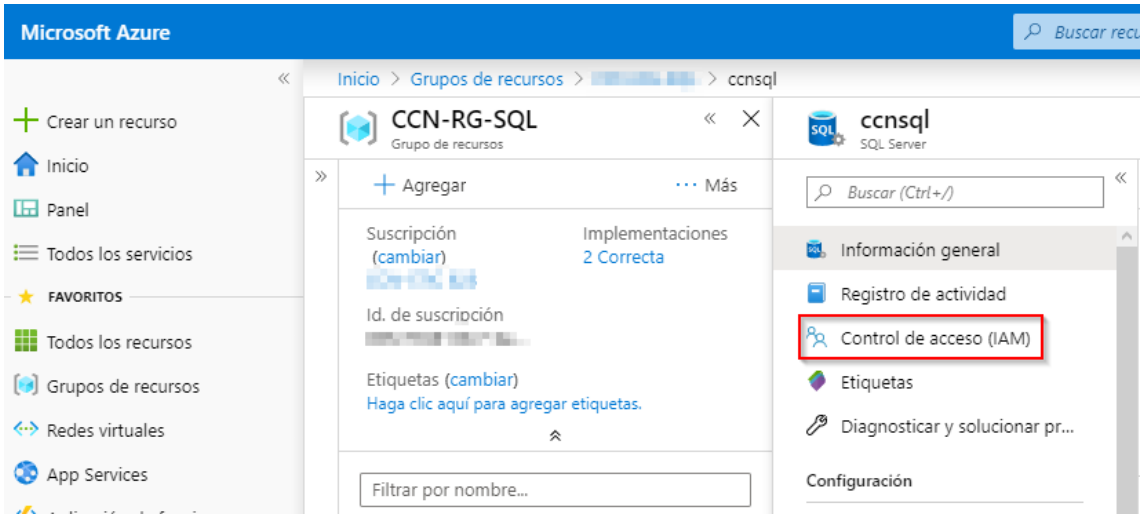
Si los roles integrados no cumplen las necesidades específicas de su organización, puede crear sus propios roles personalizados para los recursos de Azure.

A continuación, algunos ejemplos que puede aplicar para delegar las funciones y tareas.

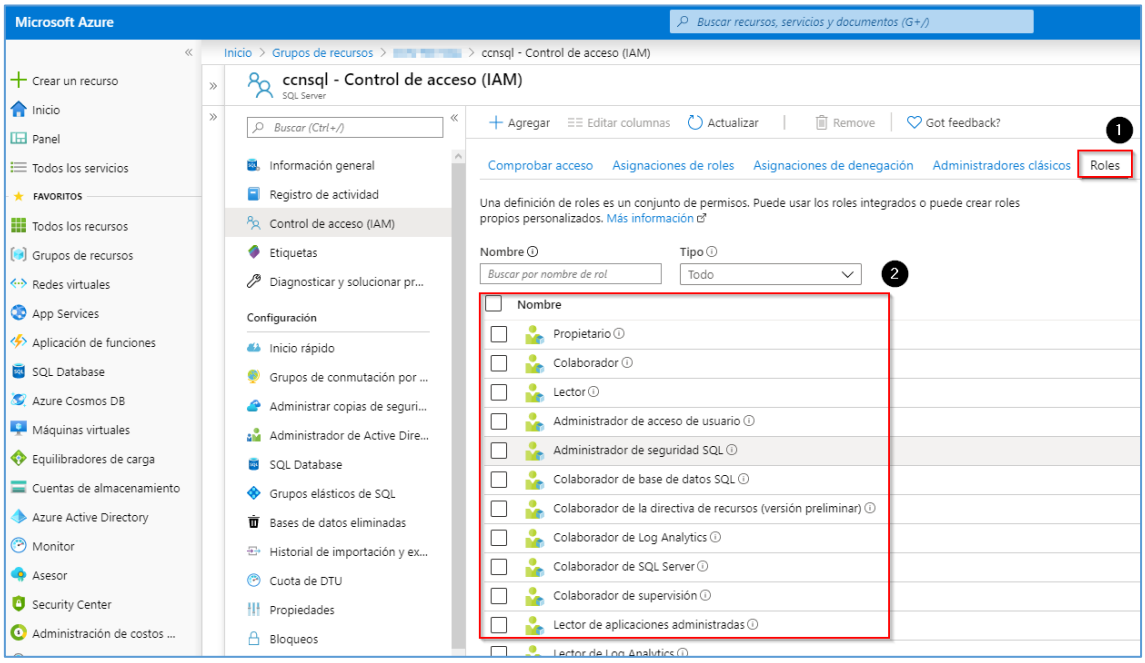
1. Desde el portal de Azure pulsar en [grupo de recursos].



2. Pulsar en [base de datos/Control de acceso (IAM)]



3. Pulsar en [Roles].



Nota: *Desde esta pestaña puede ver todos los roles que puede asignar desde el portal de Azure.*

Nota: *Para una gestión más avanzada hay que recurrir al apartado [3.1.1.1 Requisitos de acceso/Control de acceso basado en roles] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

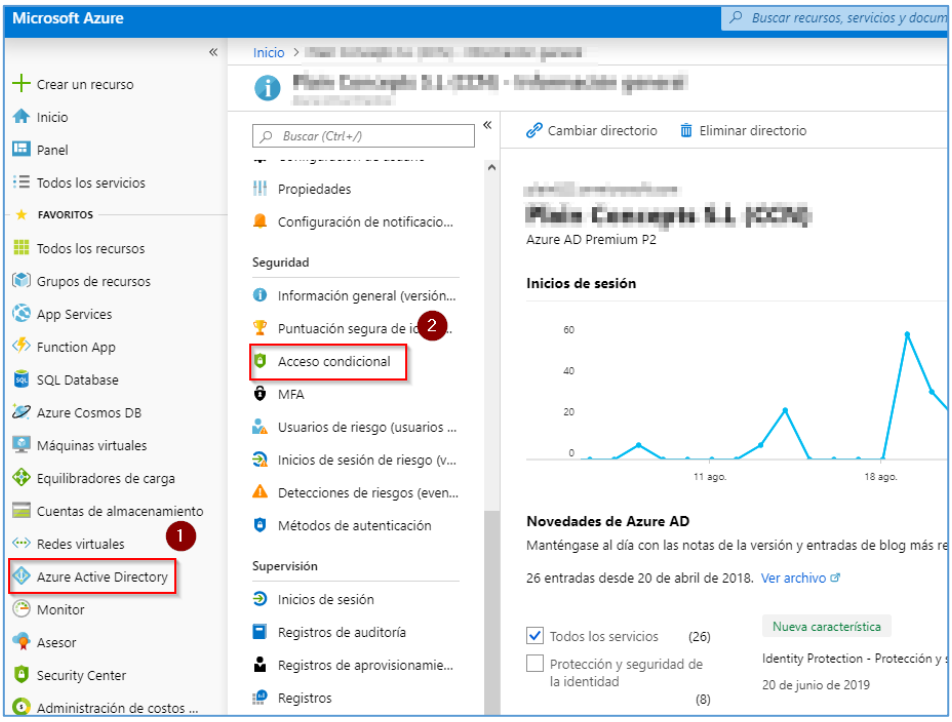
Nota: *También se recomienda seguir el siguiente enlace de Microsoft https://docs.microsoft.com/es-es/azure/role-based-access-control/role-assignments-portal*

3.1.1.4 Mecanismo de autenticación

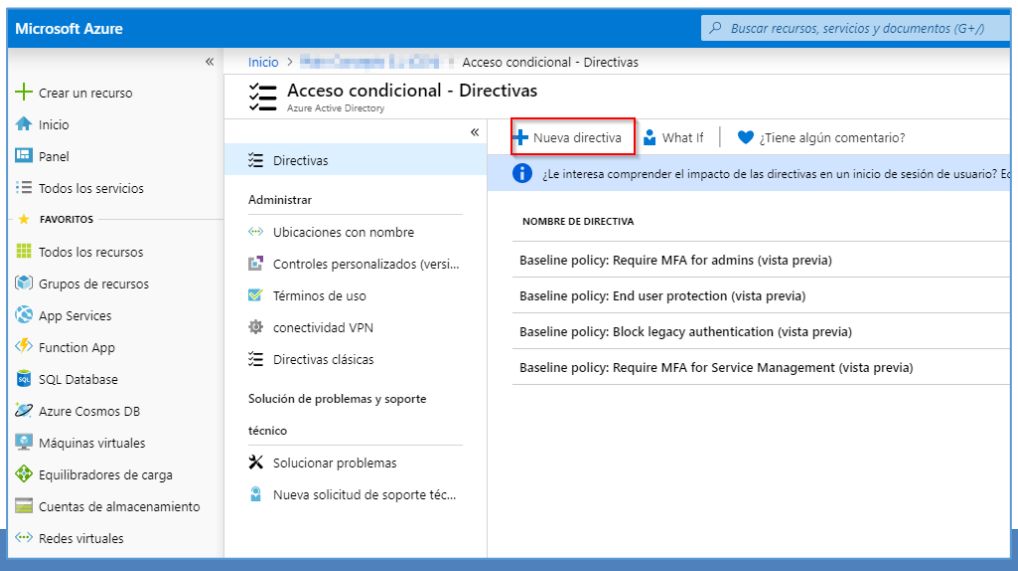
Es importante destacar la integración de Azure Multi-Factor como un mecanismo seguro de autenticación. A su vez se recomienda crear una directiva de acceso condicional para los administradores de SQL.

Para ello, debe seguir estas directrices.

1. Desde el portal de Azure Pulsar en [Azure Active Directory]
2. Pulsar en [acceso condicional].

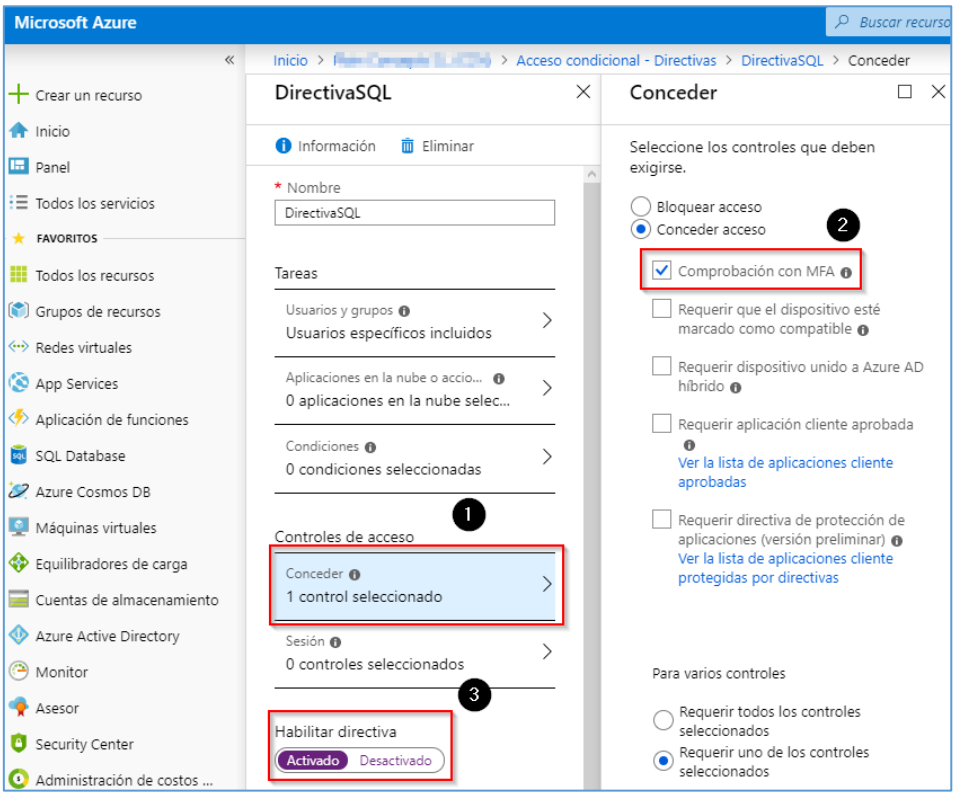


3. Pulsar en [nueva directiva].



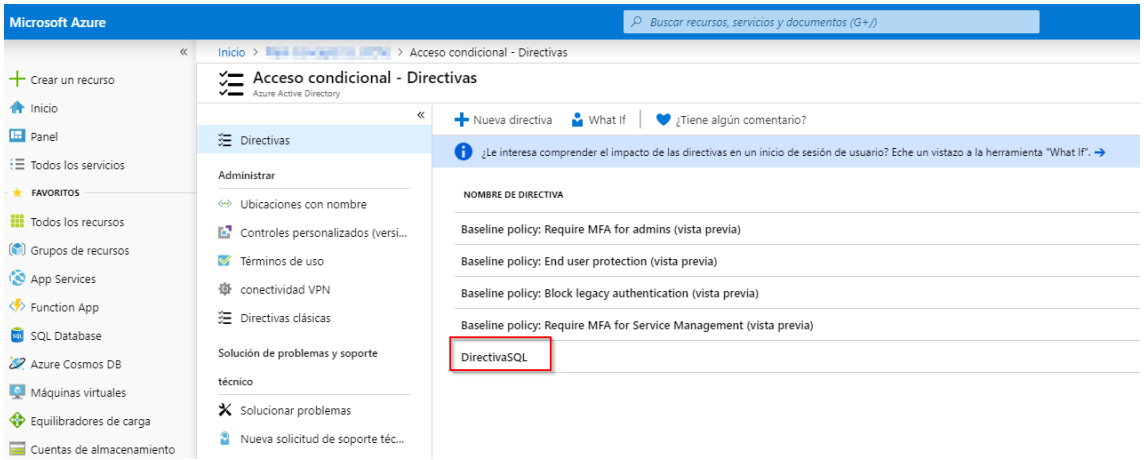
4. En usuarios y grupos pulsar en seleccionar [usuarios y grupos].
5. Seleccionar Usuarios y grupos.
6. En el nuevo menú escribir y seleccionar Administradores SQL.
7. Para finalizar, pulsar en [aceptar].

A continuación, pulsar en [control de acceso].



1. Seleccionar la casilla de comprobación MFA.
2. Pulsar en [aceptar].
3. Por último, pulsar en [guardar] para que se cree la nueva directiva.

Aparecerá la nueva directiva de acceso condicional para los usuarios Administradores de SQL. Esto fuerza a que el grupo de Administradores de SQL utilicen doble factor de autenticación.



Es importante conocer los conceptos del acceso condicional ya que puede asignar diversas condiciones de autenticación.

Se pueden agregar distintas condiciones desde una directiva de acceso condicional. Atendiendo dispositivos autorizados, ubicaciones geográficas, rangos de ips, grupos de usuarios entre otros.

Nota: *Para una gestión más avanzada hay que recurrir al apartado [3.1.1.1 Requisitos de acceso/Acceso condicional] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.2 Explotación

3.2.1 Registro de la actividad de los usuarios

El registro de actividad contiene todas las operaciones de escritura (PUT, POST, DELETE) para los recursos.

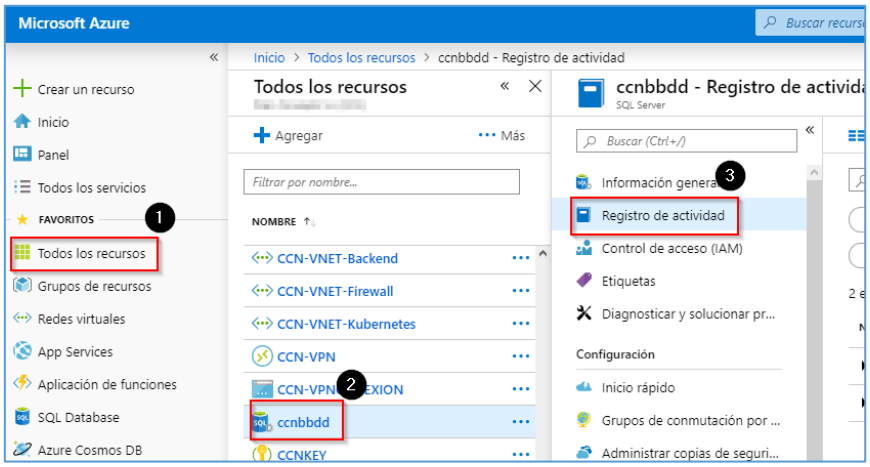
Los registros de actividad se conservan 90 días. Puede consultar cualquier intervalo de fechas, siempre que no hayan transcurrido más de 90 días desde la fecha inicial.

Mediante los registros de actividad, puede determinar:

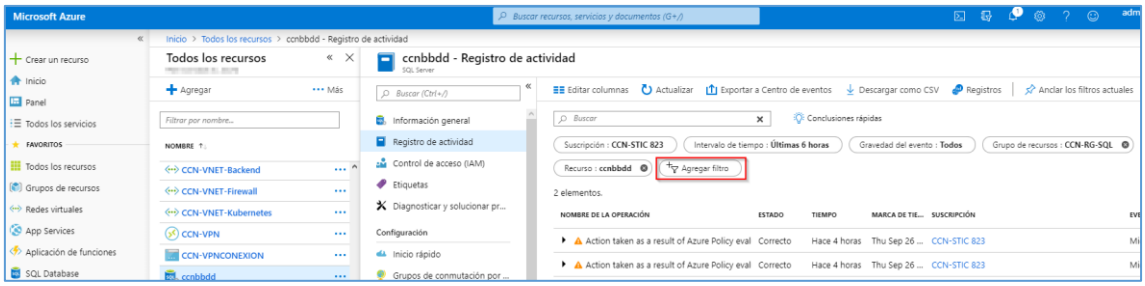
- Qué operaciones se realizaron en los recursos en la suscripción.
- Quién inició la operación.
- Cuando tuvo lugar la operación.
- El estado de la operación.
- Los valores de otras propiedades que podrían ayudarle en la investigación de la operación.

Portal de Azure

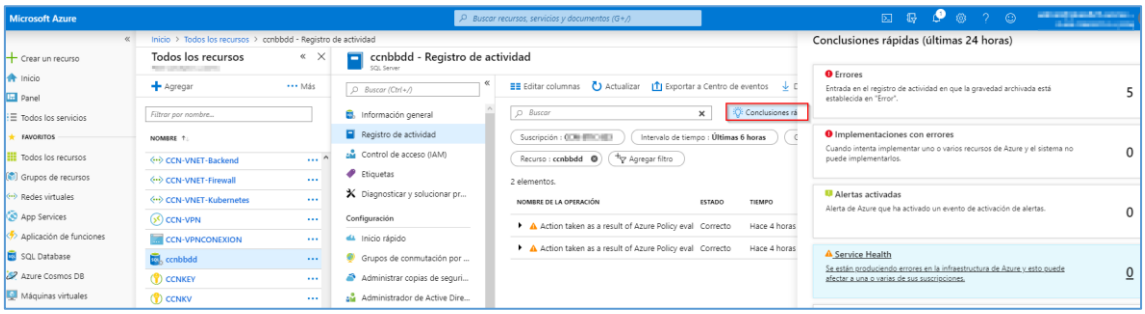
1. Para ver los registros de actividad mediante el portal, pulsar en todos los recursos.
2. Pulsar en su [base de datos].



3. En este panel encontrar varios filtros que puede aplicar.



4. Pulsar en [conclusiones rápidas] puede visualizar los eventos de las ultimas 24 hs. Así mismo, desde este panel, puede personalizar filtros de búsqueda de eventos.

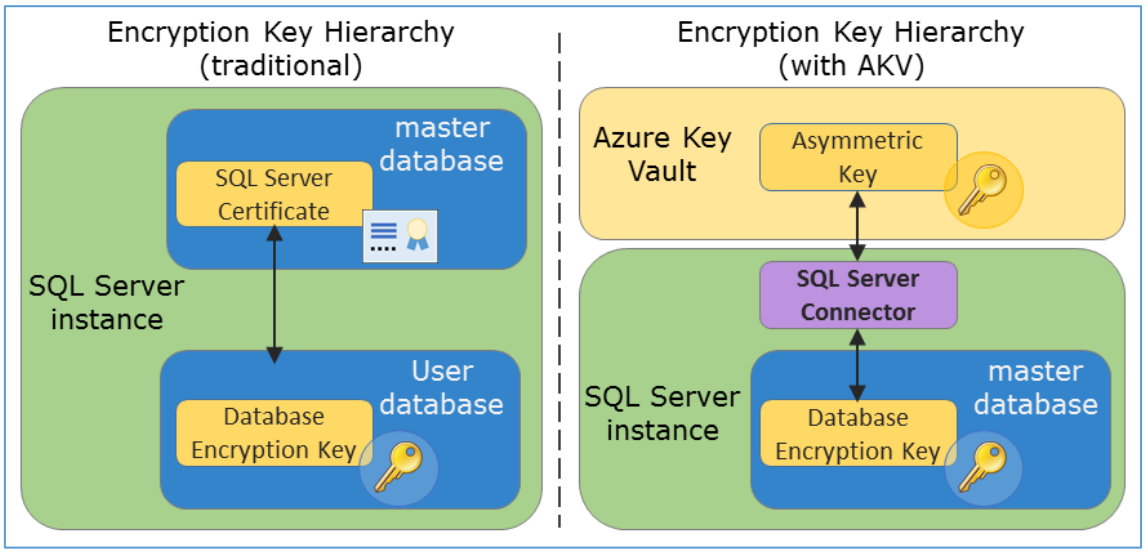


3.2.2 Protección de claves criptográficas

Azure SQL proporciona varios tipos de cifrado que ayudan a proteger información confidencial, como cifrado de datos transparente (TDE).

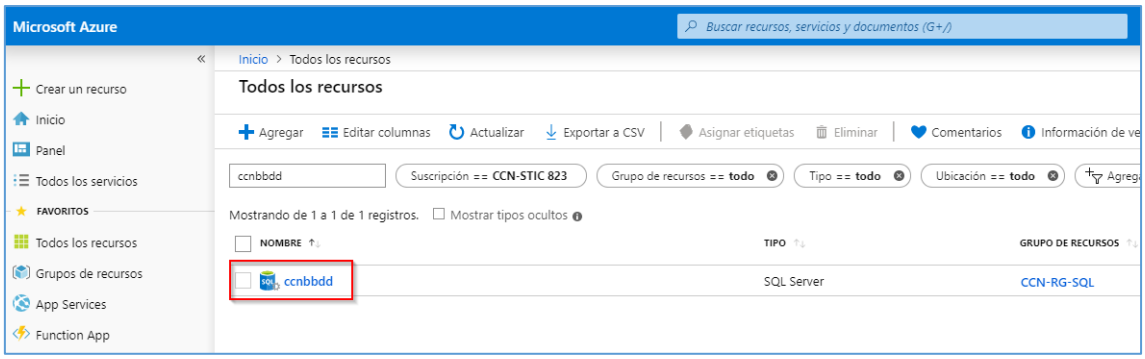
La clave de cifrado de datos simétrica se protege, además, cifrándose con una jerarquía de claves almacenadas en SQL Server.

En la imagen siguiente se compara la jerarquía de claves de administración y servicio tradicional con el sistema del Almacén de claves de Azure.

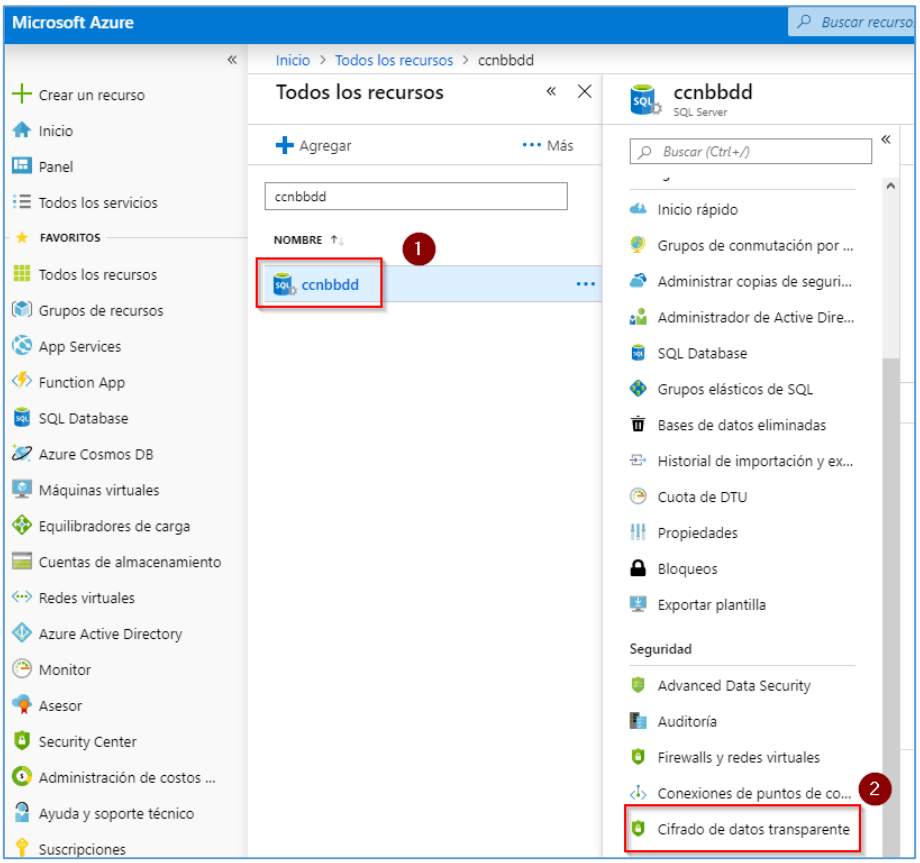


A continuación, se describen los pasos que se debe realizar para cifrar su base de datos utilizando Azure Key Vault.

1. Desde el portal de Azure pulsar en [todos los recursos].
2. Seleccionar su [base de datos].

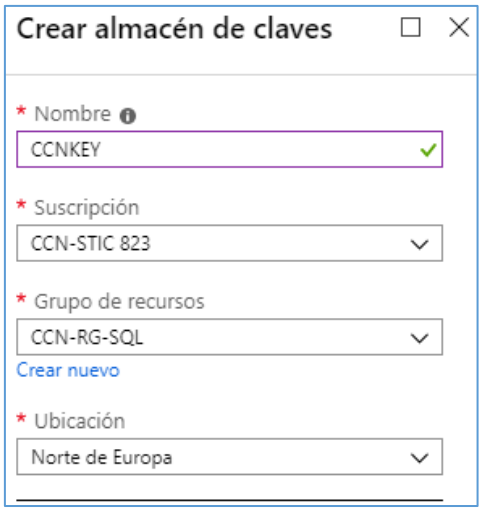


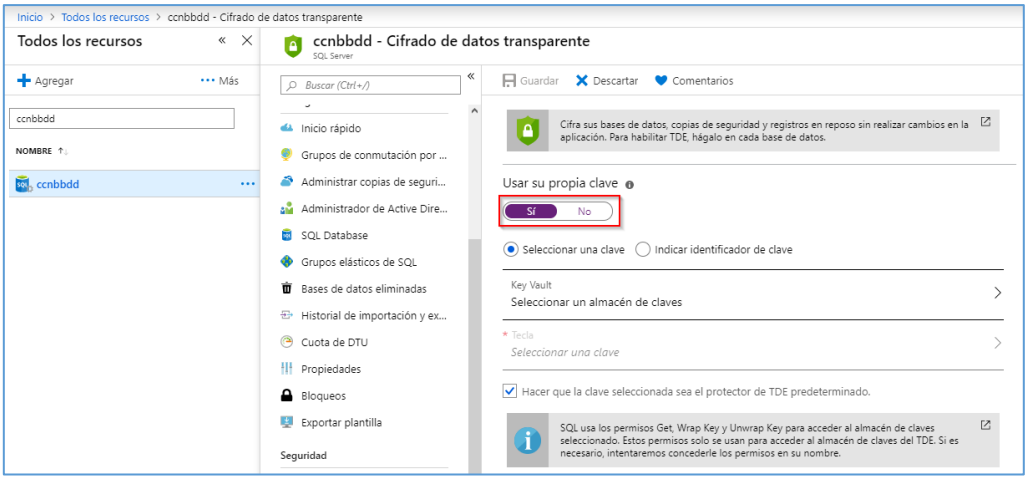
Pulsar en [cifrado de datos transparente].



En este panel debe activa su propia clave, ya que utilizará Key Vault.

3. Pulsar en usar su propia clave.
4. Pulsar en seleccionar almacén de llaves.
5. Pulsar en crear un nuevo almacén. Deberá completar los siguientes campos.
    - **Nombre:** Definir el nombre que se va a utilizar para el nuevo almacén.
    - **Suscripción:** Seleccionar su suscripción.
    - **Grupo de recursos:** Se recomienda crear un nuevo grupo que estará dedicado para este Almacén. Solo le pedirá un nombre para definirlo.
    - **Ubicación:** Seleccionar Norte de Europa.





6. Para finalizar pulsar en [guardar].

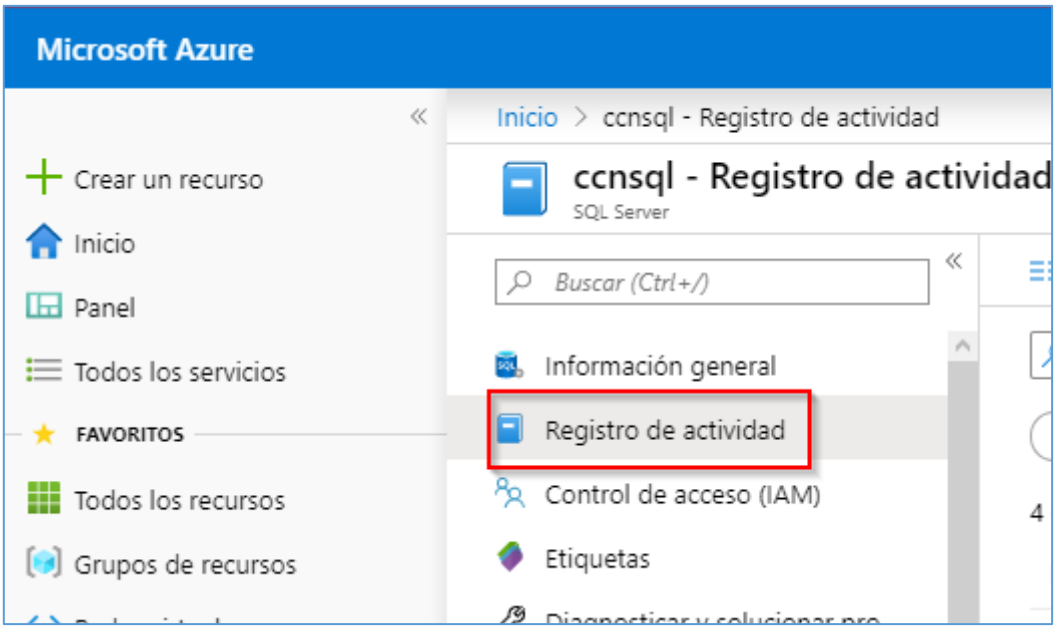
Nota: *Para una gestión más avanzada hay que recurrir al apartado [3.1.2.4 Protección de claves] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.2.3 Monitorización del sistema

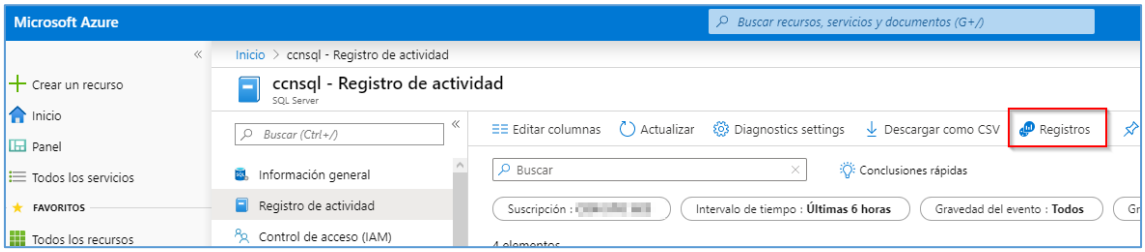
Log Analytics de Azure Monitor es una herramienta que se debe usar para obtener información detallada de los registros de Azure Monitor.

Para ello, debe seguir estas instrucciones de configuración:

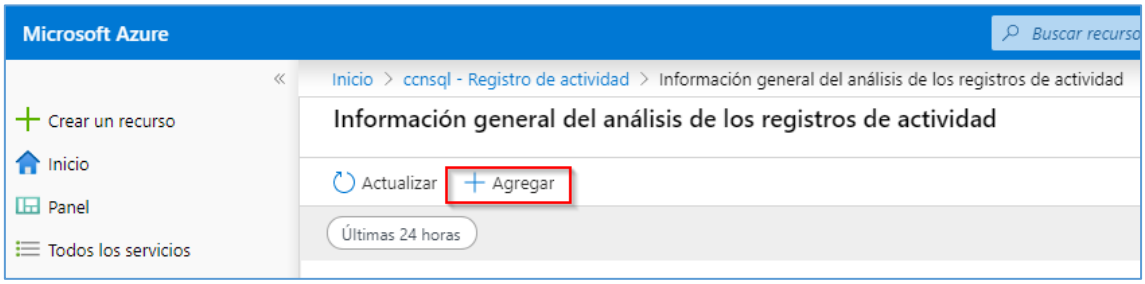
1. Desde la base de datos de SQL pulsar en [Registro de actividad]



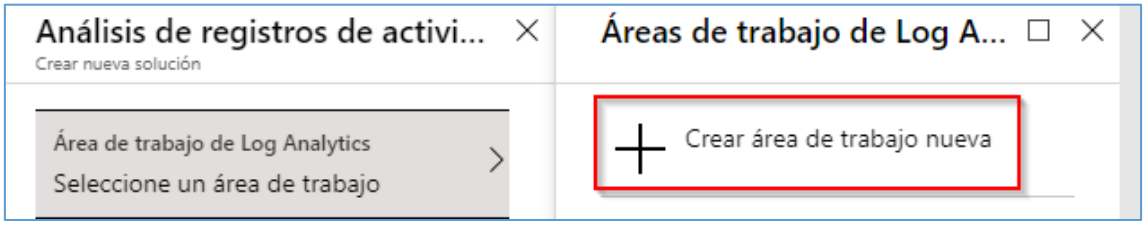
2. Después pulsar en [Registros].



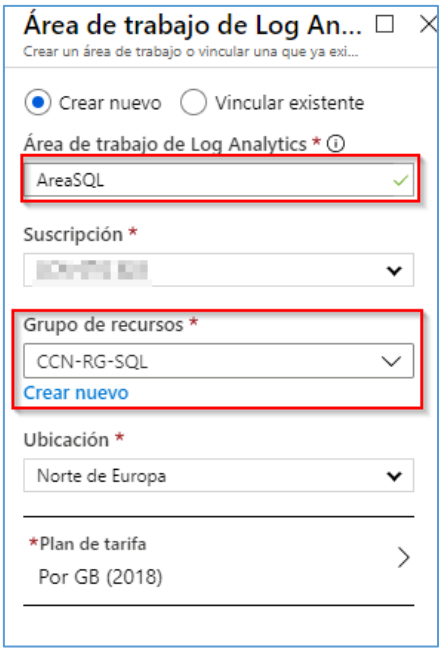
3. Pulsar en [Agregar].



4. Ahora aparece un asistente donde hay que crear un nuevo área de trabajo para los registros. Pulsar en [crear área de trabajo nueva].



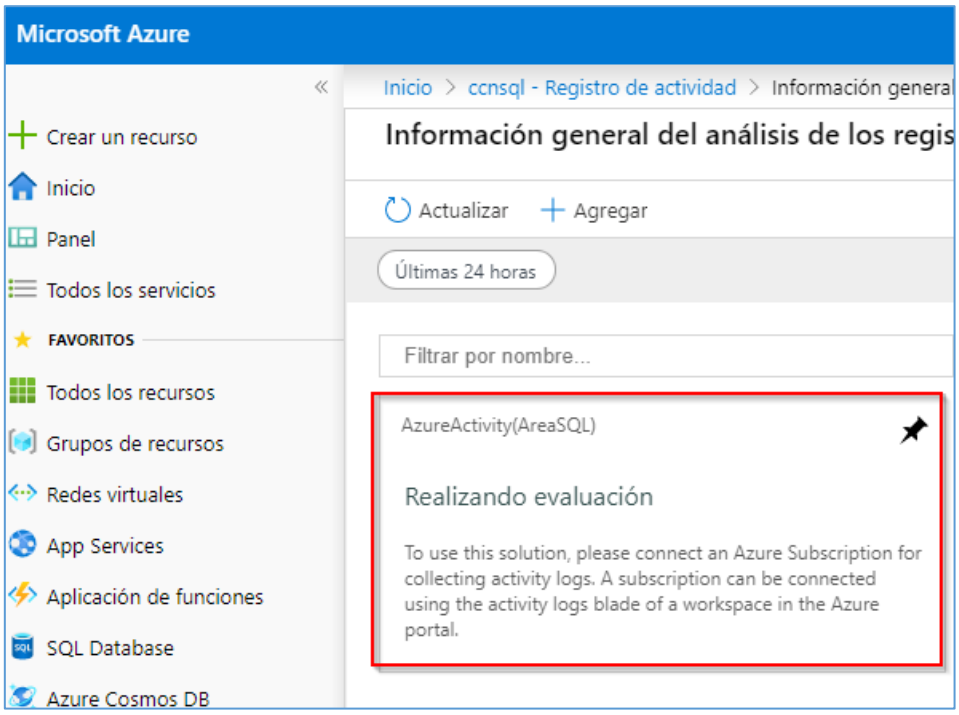
5. En el asistente identificar un nombre y un grupo de recursos. El grupo de recursos puede ser nuevo o elegir alguno existente. Se recomienda que sea un nuevo grupo.



6. Para finalizar, pulse en [Aceptar].

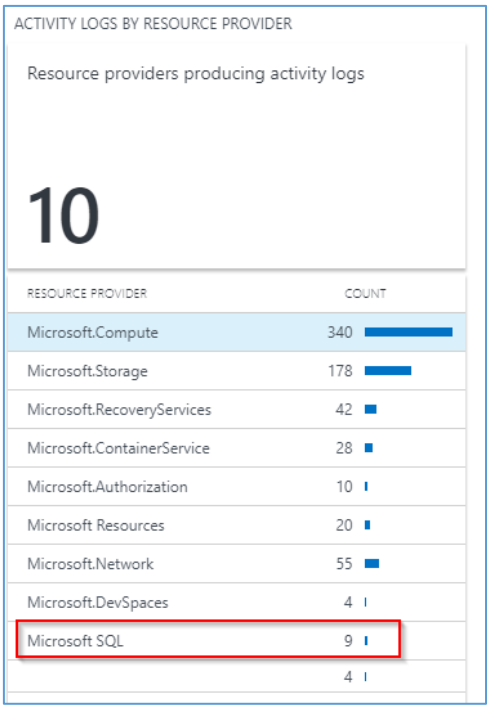
Nota: *Este proceso puede tardar unos minutos.*

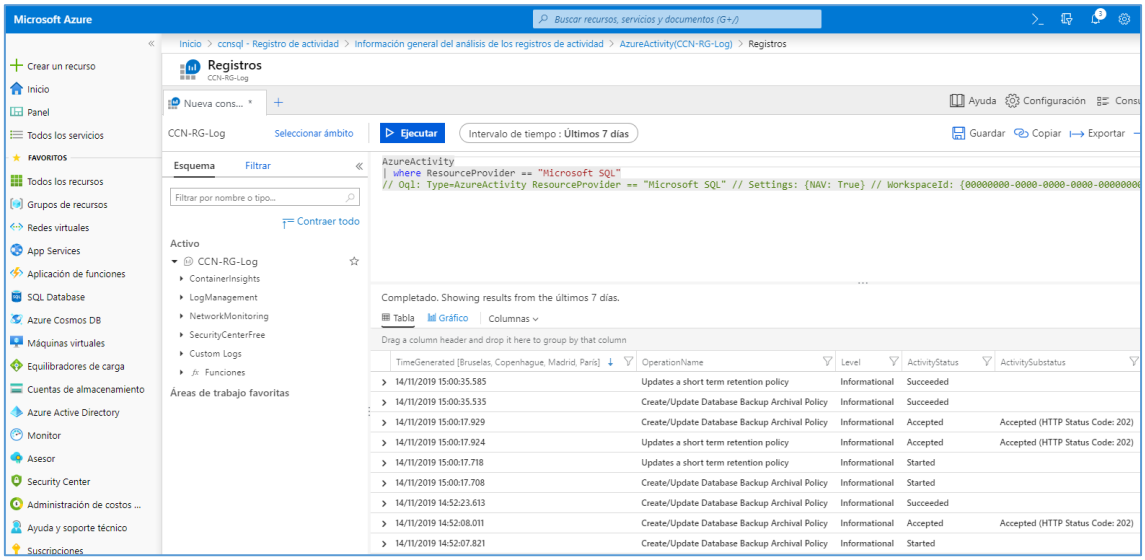
Al finalizar aparece un nuevo panel.



Importante: En el momento que se crea esta nueva área. Puede tardar un tiempo en la recolección de logs.

Un ejemplo gráfico.





Nota: *Para una gestión más avanzada hay que recurrir al apartado [3.1.6Monitorizacion de sistema] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.3 Medidas de protección

3.3.1 Protección de las comunicaciones

3.3.1.1 Perímetro seguro

Existe una separación de los roles de seguridad en la administración de puntos de conexión de servicio de red virtual. Se requiere una acción de cada uno de los roles siguientes:

Existen dos niveles.

1. **Reglas nivel base de datos individuales.**
   Estas reglas permiten a los usuarios acceder a determinadas bases de datos (seguras) dentro del mismo servidor de SQL Database. Debe crear estas reglas para cada base de datos y se almacenan en las bases de datos individuales.
2. **Reglas nivel servidor.**
   Estas reglas permiten a los usuarios obtener acceso a toda la instancia de Azure SQL Server (es decir, a todas las bases de datos que se encuentren en el mismo servidor de SQL Database). Estas reglas se almacenan en la base de datos **principal**. Las reglas de firewall de IP de nivel de servidor.

Nota: *Es importante saber que esta regla de firewall aplica específicamente a las comunicaciones de las bases de datos.*

A continuación, ejecutar estos comandos mediante PowerShell:

1. Creación de regla nivel base de datos individuales en SQL.

```
# EXECUTE sp_set_database_firewall_rule N'Example DB Rule','0.0.0.4','0.0.0.4';
```

2. Creación de regla de firewall indicando el rango de ip origen y destino para que se apliquen en el servidor.

```
# New-AzSqlServerFirewallRule -ResourceGroupName "myResourceGroup" `
#     -ServerName $servername `
#     -FirewallRuleName "AllowSome" -StartIpAddress "0.0.0.0" -EndIpAddress "0.0.0.0"
```

Existen otros tipos de recomendaciones para el aislamiento de la base de datos, así como la configuración de Azure firewall y NSG.

Nota: *Para esta gestión más avanzada, hay que recurrir al apartado [3.2.1 Proteccion de las comunicaciones/3.2.1.2 Perímetro seguro] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.3.2 Protección de la información

3.3.2.1 Calificación de la información

Para la clasificación de la información se recomienda el uso de etiquetas.

Se componen de clave-valor definidos por el usuario, se pueden colocar directamente en un recurso o un grupo de recursos.

Actualmente, Azure admite un máximo de 15 etiquetas por recurso y grupo de recursos.

Las etiquetas se pueden colocar en un recurso en el momento de su creación, o bien se pueden agregar a un recurso existente.

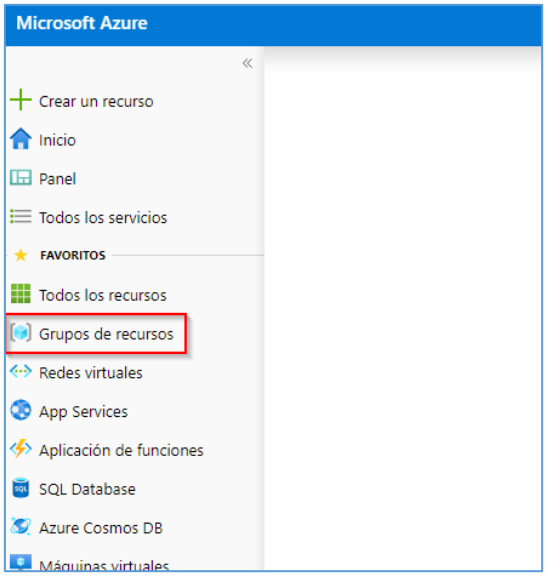
En Azure SQL se recomienda el uso de estas etiquetas que se deben emplear en las máquinas virtuales, grupo de recursos, base de datos.

Nota: *Para para conocer más el uso de etiquetas y su configuración hay que recurrir al apartado [3.2.2 Protección de la información/3.2.2.1 Clasificación de la información] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

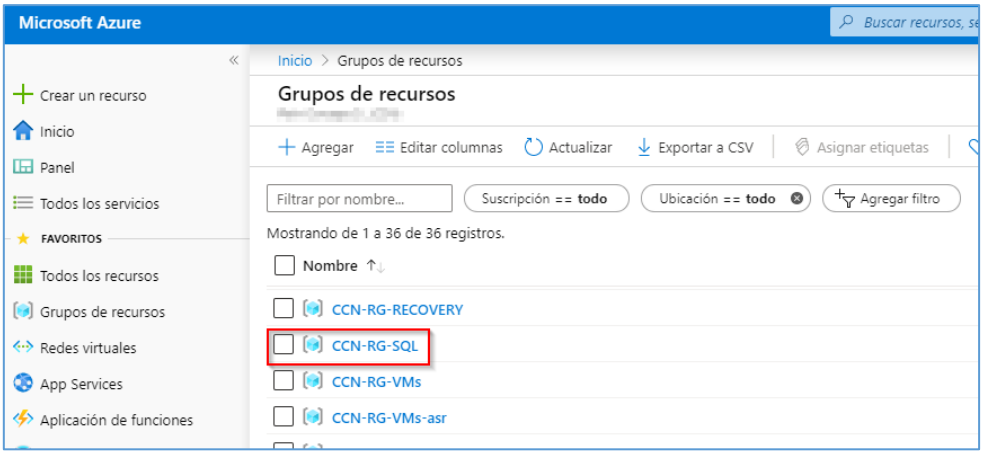
3.3.2.2 Copias de seguridad (backup)

Existen distintos métodos desde Azure para realizar backups. En este caso debe utilizar como primera medida una retención de su base de datos.
A continuación, se describe las instrucciones que debe seguir para configurar la retención en sus bases de datos.

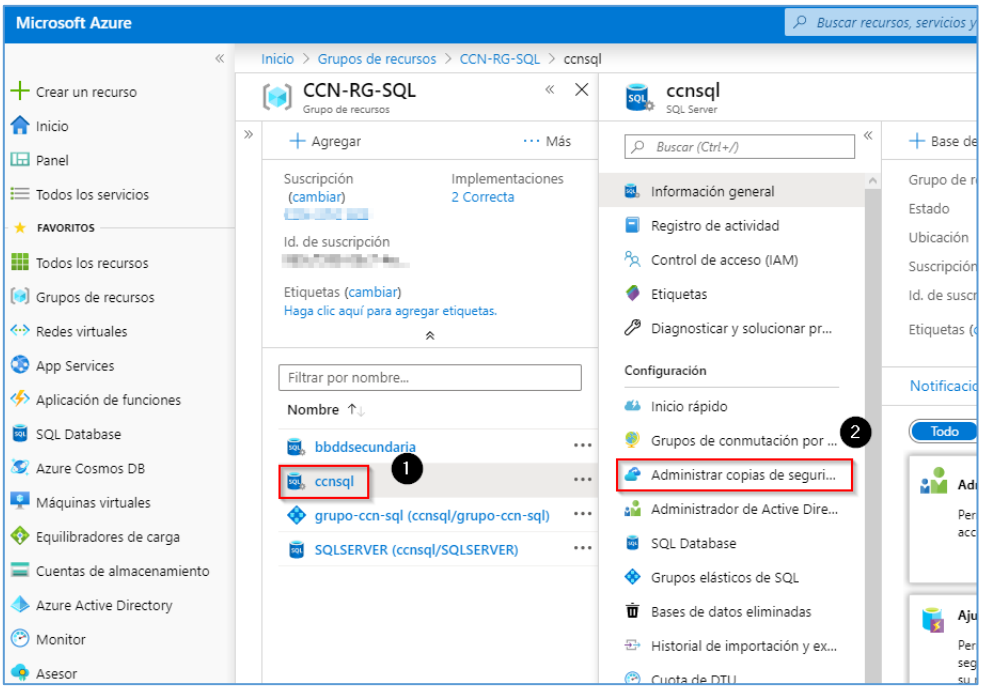
1. Desde el portal de Azure pulsar en [Grupo de recursos]



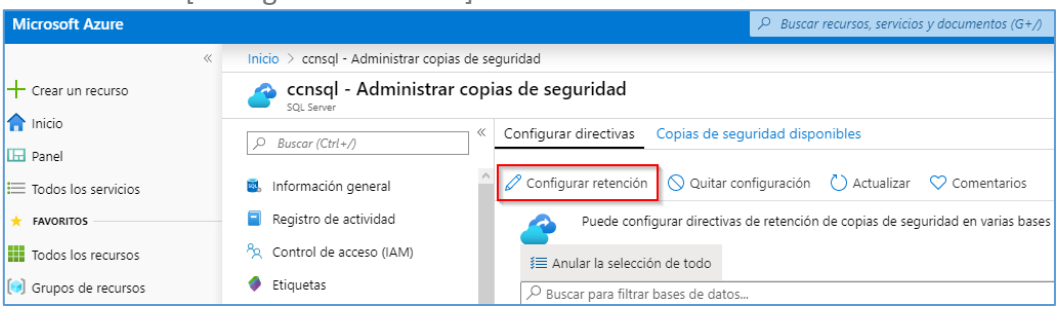
2. Pulsar en el grupo de recursos donde se encuentra su base de datos.



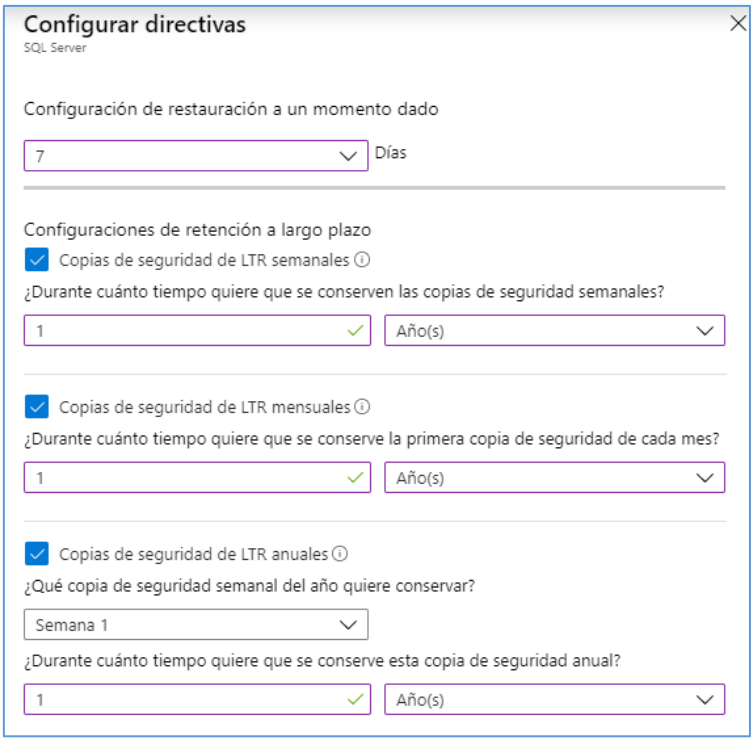
3. Pulsar en su base de datos y después pulsar en Administrar copias de seguridad.



4. Pulsar en [Configurar retención].



5. Se abre una nueva ventana donde debe completar la siguiente información.



- **Configuración de restauración a un momento dado:** Dispone
- **Configuración de retención a largo plazo:** Dispone de 7 a 35 días.
- **Copias de seguridad de LTR mensuales:** Debe asignar el tiempo que se conserven las copias de seguridad semanales
- **Copias de seguridad de LTR anuales**: Puede seleccionar desde 1 semana hasta 52 semanas al año.

6. Una vez definida la configuración pulse en [Aplicar]

Puede consultar más información en el enlace https://docs.microsoft.com/es-es/azure/sql-database/sql-database-automated-backups

Nota: *Para una gestión más avanzada hay que recurrir al apartado [2.3 Gestión de recursos Azure/Grupo de recursos] de la guía. [CCN-STIC-884A - Guía de configuración segura para Azure].*

3.4 SCRIPTS DE CONFIGURACIÓN

Se adjunta el script formato JSON para la creación de un nuevo rol personalizado PaaS en los administradores de SQL.

Puede consultar sobre mas roles en los siguientes links.

- https://docs.microsoft.com/da-dk/azure/sql-database/sql-database-manage-logins?toc=/azure/sql-data-warehouse/toc.json
- https://docs.microsoft.com/es-es/sql/relational-databases/security/authentication-access/application-roles?view=sql-server-ver15

- https://docs.microsoft.com/es-es/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver15

4. GLOSARIO Y ABREVIATURAS

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía:

Término	Definición
AAD	*Azure Active Directory (Directorio Activo de Azure).*
AD DS	*Active Directory Domain Services (Servicios de dominio de Directorio Activo).*
Grupo de Recursos	*contenedor que almacena los recursos relacionados con una solución de Azure. El grupo de recursos incluye los recursos que se desean administrar como grupo.*
Azure AD	*Azure Active Directory.*
RBAC	*RBAC es un sistema de autorización basado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure.*
JSON	*Acrónimo de JavaScript Object Notation, «notación de objeto de JavaScript») es un formato de texto sencillo para el intercambio de datos.*
ENS	*Esquema Nacional de Seguridad.*
MFA	*Multifactor Authentication (Autenticación Multifactor). Sistema de seguridad que requiere más de una forma de autenticarse, por ejemplo, a través de una app, sms, etc.*
Log Analytics	*Azure Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA) o agente Linux de OMS, se desarrolló para lograr una administración completa en las máquinas locales, en los equipos que supervisaba System Center Operations Manager y en las máquinas virtuales de cualquier nube. Los agentes de Windows y Linux se asocian a Azure Monitor y almacenan los datos de registro recopilados de diferentes orígenes en el área de trabajo de Log Analytics.*
Cifrado de datos	*El Cifrado de datos transparente (TDE) cifra los archivos de datos de SQL Server, Base de datos SQL de Azure y Azure Synapse*

transparente	*Analytics (SQL DW), lo que se conoce como cifrado de datos en reposo.*

5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio, donde la organización puede valorar qué medidas de las propuestas se cumplen.

<table>
<tr><th>Control ENS</th><th colspan="2">Configuracion</th><th>Estado</th></tr>
<tr><td>op</td><td colspan="3">Marco Operacional</td></tr>
<tr><td>op.acc</td><td colspan="3">Control de Acceso</td></tr>
<tr><td rowspan="3">op.acc.1</td><td colspan="3">Identificación</td></tr>
<tr><td rowspan="2">Se ha configurado el uso de cuentas y grupos de Azure Active directory para la administración del Tenant.</td><td>Aplica:

☐ Si ☐ No</td><td>Cumple:

☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:

☐ Si ☐ No</td><td>Observaciones:</td></tr>
</table>

<table>
<tr><td rowspan="3">op.acc.2</td><td colspan="3">Requisitos de Acceso</td></tr>
<tr><td rowspan="2">Se ha configurado el requisito tratados en el punto 3.1.1.4.</td><td>Aplica:
☐ Si ☐ No</td><td>Cumple:
☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Si ☐ No</td><td>Observaciones:</td></tr>
<tr><td rowspan="3">op.acc.3</td><td colspan="3">Segregación de funciones y tareas</td></tr>
<tr><td rowspan="2">Se han diseñado, creado y aplicado los roles a los grupos de usuarios. Mínimo han de aplicarse los roles Propietario, colaborador, lector y Administrador de acceso de usuario y administradores de bases de datos SQL, siguiendo la referencia de la guía de configuración segura de Azure.</td><td>Aplica:
☐ Si ☐ No</td><td>Cumple:
☐ Si ☐ No</td></tr>
<tr><td>Evidencias Recogidas:
☐ Si ☐ No</td><td>Observaciones:</td></tr>
</table>

op.acc.5	**Mecanismo de autenticación**		
	Se ha habilitado Multi-Factor Authentication (MFA) para los usuarios administradores de SQL utilizando una directiva de acceso condicional.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp	**Explotacion**		
op.exp.8	**Registro de la actividad de los usuarios**		
	Se ha comprobado que el registro de Auditoría está activado y capturando eventos habilitando una nueva área de trabajo.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

Op-exp.11	**Protección de claves criptográficas**		
	Se ha configurado Key Vault, límitando el acceso tan sólo a usuarios administradores. Siguiendo las instrucciones de la guia CCN-STIC-884A Configuración segura para Azure, apartado. [3.2.2.2 Cifrado]	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.mon	**Monitorizacion de sistema**		
Op.mon.2	**Sistema de métricas**		
	Se ha configurado Azure monitor aplicando los registros populares haciendo referencia a las recomendaciones de Azure SQL Database.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.com.1	**Perímetro seguro**		
	Se ha configurado el acceso restringido utilizando reglas de firewall.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.info.2	**Clasificacion de la informacion**		
	Se han configurado etiquetas para diferenciar los servicios que compone las bases de datos de SQL, Maquinas virtuales, grupos de recursos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.info.9	**Copias de seguridad**		
	Se ha configurado un politica de retencion de copias de seguridad.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**