Guía de Seguridad de las TIC
CCN-STIC 884B

Guía de configuración segura para Kubernetes Services

ENERO 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN 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 12:12:48 +01'00'

NIPO: 083-19-258-2

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

INDICE

1. GUÍA DE CONFIGURACIÓN SEGURA AZURE KUBERNETES SERVICES 6
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA 6
1.2 DEFINICIÓN DEL SERVICIO.....6
1.3 PRERREQUISITOS PARA EL DESPLIEGUE 6
1.3.1 SISTEMA OPERATIVO WINDOWS 6
1.3.2 SISTEMA OPERATIVO LINUX.....7
2. DESPLIEGUE DE AZURE KUBERNETES SERVICES..... 7
2.1 CONFIGURACIONES DEL CLÚSTER AKS 12
2.1.1 ESCALAR NODOS DEL CLÚSTER. 12
2.1.1.1 DESDE EL PORTAL DE AZURE 12
2.1.1.2 DESDE POWERSHELL.....13
2.1.2 ACTUALIZAR CLÚSTER 14
2.1.2.1 DESDE EL PORTAL DE AZURE 14
2.1.2.2 ACTUALIZAR CLÚSTER DESDE POWERSHELL 15
3. CONFIGURACIÓN DE AZURE KUBERNETES SERVICES..... 15
3.1 MARCO OPERACIONAL.....15
3.1.1 PLANIFICACIÓN.....15
3.1.1.1 ARQUITECTURA DE SEGURIDAD 15
3.1.2 CONTROL DE ACCESO 16
3.1.2.1 IDENTIFICACIÓN.....16
3.1.2.2 SEGREGACIÓN DE FUNCIONES Y TAREAS 17
3.1.2.3 MECANISMOS DE AUTENTICACIÓN.....18
3.1.2.4 ACCESO LOCAL (LOCAL LOGON) 20
3.1.2.5 ACCESO REMOTO (REMOTE LOGIN).....20
3.1.3 EXPLOTACIÓN 20
3.1.3.1 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS.....20
3.1.3.2 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS.....23
3.1.4 CONTINUIDAD DEL SERVICIO 25
3.1.4.1 PLAN DE CONTINUIDAD.....25
3.1.5 MONITORIZACIÓN DEL SISTEMA.....25
3.1.5.1 DETECCIÓN DE INTRUSIÓN.....25

3.1.5.2 SISTEMA DE MÉTRICAS 26
3.2 MEDIDAS DE PROTECCION 28
3.2.1 PROTECCIÓN DE LAS COMUNICACIONES 28
3.2.1.1 SEGREGACIÓN DE REDES 28
3.2.1.2 PERÍMETRO SEGURO 30
3.2.2 PROTECCIÓN DE LA INFORMACIÓN 35
3.2.2.1 CALIFICACIÓN DE LA INFORMACIÓN 35
3.2.2.2 COPIAS DE SEGURIDAD (BACKUP) 35
4. GLOSARIO Y ABREVIATURAS 35
4.1 GLOSARIO Y ABREVIATURAS 35
5. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD 37

1. Guía de configuración segura Azure Kubernetes Services

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es indicar los pasos a seguir para la configuración segura de Kubernetes cumpliendo con los requisitos de seguridad para el orquestador de contenedores.

En esta guía se abordarán la **configuración esencial de kubernetes**, se debe consultar junto con la guía CCN-STIC 884A – Guía de configuración segura de Azure.

1.2 DEFINICIÓN DEL SERVICIO

Azure Kubernetes es una plataforma de rápida evolución para administrar aplicaciones basadas en contenedores, además de sus componentes de red y almacenamiento asociados. El foco está en las cargas de trabajo de la aplicación.

Proporciona un enfoque declarativo en las implementaciones, respaldado por un sólido conjunto de APIs para las operaciones de administración.

1.3 PRERREQUISITOS PARA EL DESPLIEGUE

Para la configuración de Kubernetes, a través de Powershell, se requiere la instalación del módulo de Azure CLI.

Azure CLI está diseñado para facilitar el uso de scripts, con datos de consulta, compatibilidad con operaciones de larga duración, etc. La instalación se puede realizar para diversos sistemas operativos.

Requisitos mínimos del sistema

Usar una versión de 64 bits de Windows. La compatibilidad con la versión de 32 bits de Módulo de Microsoft Azure Active Directory para Windows PowerShell se encuentra obsoleto desde octubre de 2014.

Es necesario usar la versión 5.1 o posterior de PowerShell. Más información sobre requerimientos previos de plataformas en el siguiente enlace:

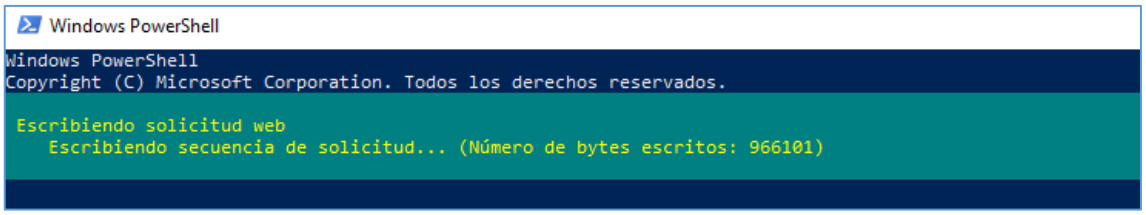
https://docs.microsoft.com/es-es/powershell/azure/azurerm/install-azurerm-ps?view=azurermps-6.13.0

1.3.1 Sistema operativo Windows

1. Para sistemas operativos Windows se debe abrir una consola de PowerShell y ejecutar el siguiente comando:

```
# Invoke-WebRequest -Uri https://aka.ms/installazurecliwindows -OutFile .\AzureCLI.msi; Start-Process msiexec.exe -Wait -ArgumentList '/I AzureCLI.msi /quiet'
```

Se descarga e instala la versión más reciente de la CLI de Azure para Windows. Si ya existe instalada una versión, se actualiza la versión existente.



2. Una vez completada la instalación, se tiene que volver a abrir una consola de PowerShell para usar la CLI de Azure.
3. Ejecutar el comando *az login* para iniciar sesión en Azure.

```
# az login
```

1.3.2 Sistema operativo Linux

Si se está ejecutando una distribución con el gestor de paquetes **apt**, como Ubuntu o Debian, existe un paquete x86_64 disponible para la CLI de Azure. Este paquete se ha probado y es compatible con:

Ubuntu trusty, xenial, bionic.

Para instalar los **prerrequisitos** ejecutar los siguientes pasos:

1. Obtener los paquetes necesarios para el proceso de instalación:

```
# sudo apt-get update
# sudo apt-get install ca-certificates curl apt-transport-https lsb-release gnupg
```

2. Descargar e instalar la clave de firma de Microsoft:

```
# curl -sL https://packages.microsoft.com/keys/microsoft.asc | \
#     gpg --dearmor | \
#     sudo tee /etc/apt/trusted.gpg.d/microsoft.asc.gpg > /dev/null
```

3. Agregar el repositorio de software de la CLI de Azure:

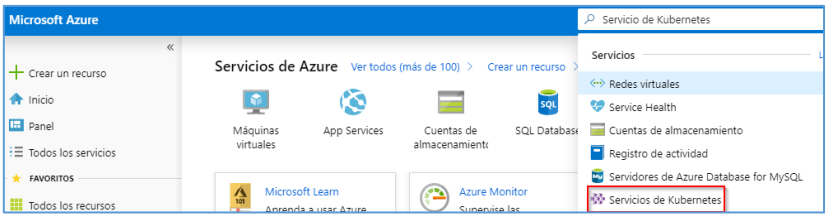
```
# AZ_REPO=$(lsb_release -cs)
# echo "deb [arch=amd64] https://packages.microsoft.com/repos/azure-cli/ $AZ_REPO main" |
\
#     sudo tee /etc/apt/sources.list.d/azure-cli.list
```

4. Para actualizar la información del repositorio e instalar el paquete azure-cli:

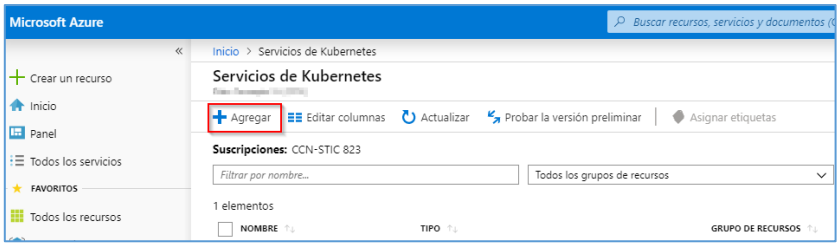
```
# sudo apt-get update
# sudo apt-get install azure-cli
```

2. DESPLIEGUE DE Azure Kubernetes Services

1. Buscar el Servicio de Kubernetes desde el portal de Azure.



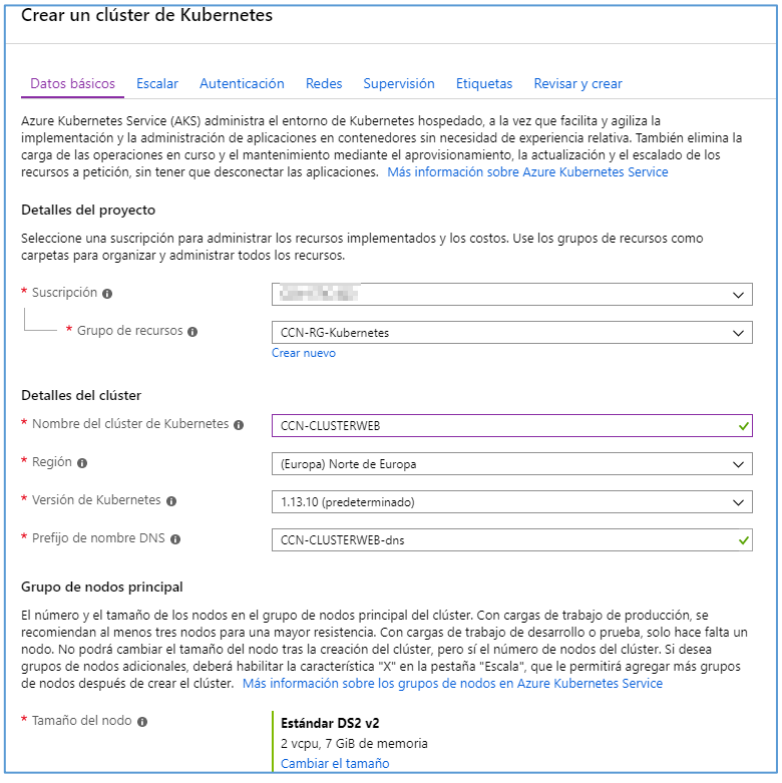
2. Pulsar en [agregar].



En este primer panel se completan los campos obligatorios para el despliegue.

A continuación, se detallan cada uno de ellos.

3. Pulsar en [Datos Básicos].

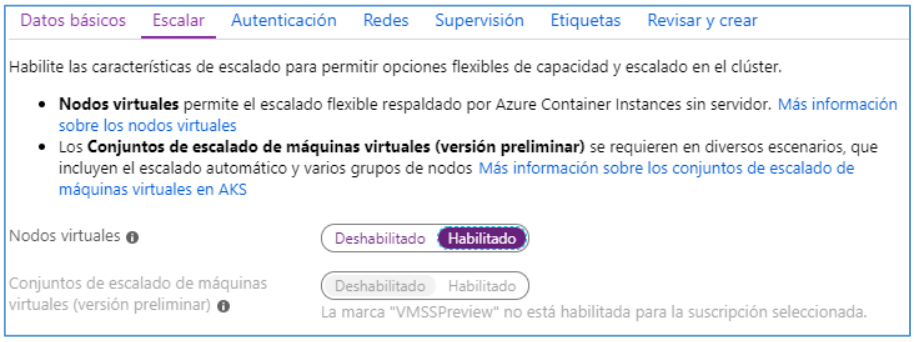


- **Suscripción:** Suscripción donde se crea el servicio.
- **Grupo de Recursos:** Se puede elegir uno ya creado o crear uno nuevo.
- **Nombre del clúster Kubernetes:** Nombre del clúster de Kubernetes.
- **Región:** Por defecto aparece EEUU, se debe cambiar a Norte de Europa.
- **Versión de Kubernetes:** En esta primera instalación se debe dejar por defecto.

- **Prefijo de nombre DNS:** Prefijo del nombre DNS que se usa con el FQDN del servidor API.

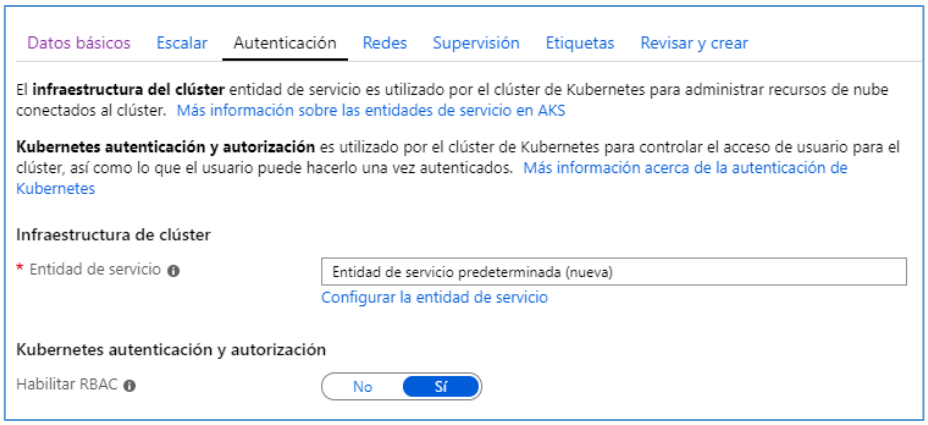
Por último, se puede elegir el número de nodos. Al ser desplegado por redes CNI el límite lo marca el tamaño de la subnet, como se explica en el apartado [3.2.1.1 Segregación de redes] de esta guía.

4. Pulsar en la pestaña [Escalar] y habilitar los nodos virtuales. Con esta opción se puede implementar rápidamente el balanceo y cargas de trabajo en un clúster de Azure Kubernetes Service (AKS). Además, tiene un aprovisionamiento rápido de pods.



5. Pulsar en [Autenticación].

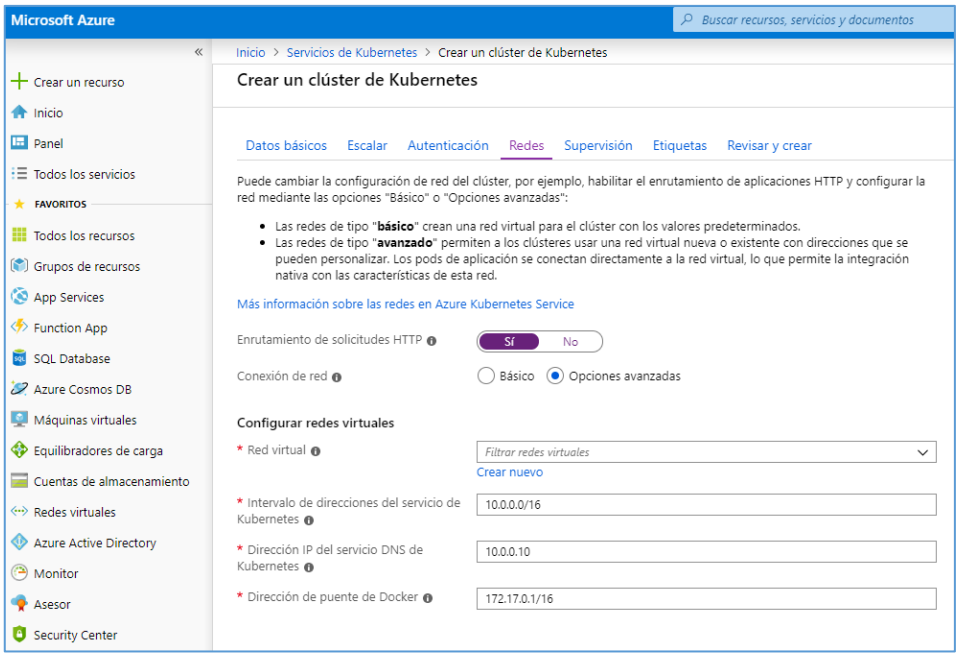
En la pestaña de autenticación se debe activar RBAC ya que en esta guía recomendamos este método en el acceso de la aplicación Kubernetes.



Entidad de servicio: Por defecto se crea una nueva.

- Habilitar RBAC: Se recomienda habilitar RBAC ya que mencionamos la configuración de esta guía en el apartado [3.1.2.2 Segregación de funciones y tareas]

6. A continuación, en la pestaña de [redes], realizar los siguientes pasos:



- **Enrutamiento de solicitudes HTTP:** El complemento de enrutamiento de aplicaciones HTTP está diseñado para permitir crear rápidamente un controlador de entrada y acceder a sus aplicaciones. Este complemento no se recomienda para el uso en producción. **Se debe dejar deshabilitado.**
  Para entornos de producción se recomienda utilizar un controlador de entrada HTTPS. Para más información consultar: https://docs.microsoft.com/es-es/azure/aks/ingress-tls

  Conexión de red: Pulsar en opciones avanzadas. De esta manera se crea una red CNI para el clúster de Kubernetes, siendo esta la opción recomendada.

  Nota: *Para obtener más información sobre la creación de redes en Azure consultar el apartado [3.2.1.1 Segregación de redes] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

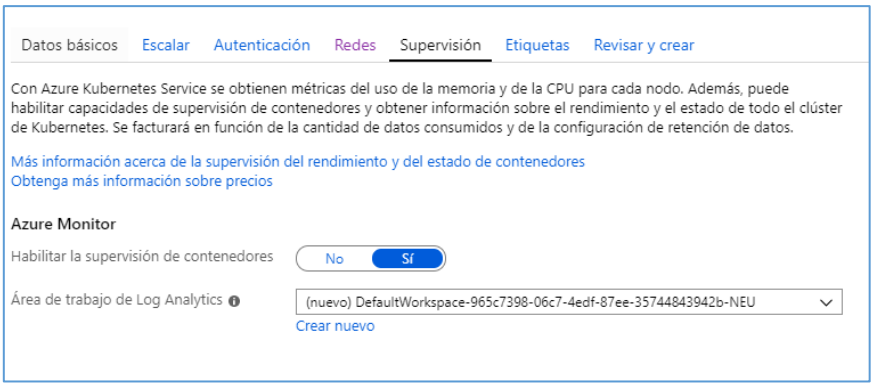
  Configuración de redes virtuales

  Seguir los siguientes pasos:

  - **Red Virtual:** Crear una nueva red virtual para este despliegue.
  - **Intervalo de direcciones del servicio Kubernetes:** Asignar las direcciones IP del clúster del servicio. No se debe superponer con ningún intervalo IP de subred.
  - **Dirección IP del servicio DNS de Kubernetes:** Una dirección IP asignada al servicio DNS de Kubernetes. Debe estar en el intervalo de direcciones del servicio de Kubernetes.
  - **Dirección de puente de Docker:** Una dirección IP y la máscara de red asignadas al puente de Docker. No debe estar

en un intervalo IP de subred ni en el intervalo de direcciones del servicio de Kubernetes.

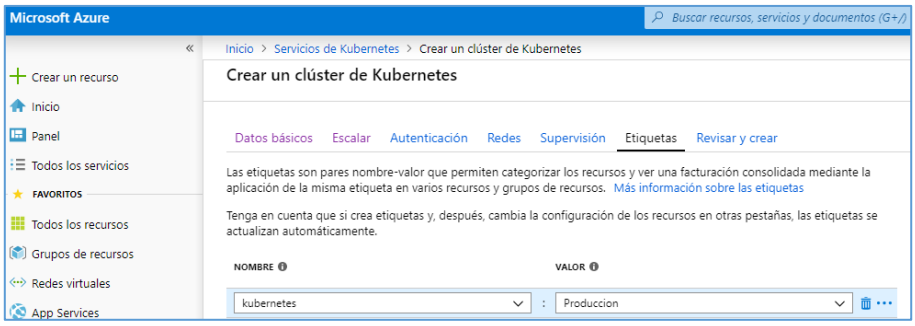
7. A continuación, pulsar en la pestaña de [supervisión].



Se recomienda habilitar **Azure Monitor** para contenedores, ya que es una herramienta diseñada para supervisar el rendimiento de las cargas de trabajo de los contenedores implementados en Azure.

La supervisión de los contenedores es fundamental, sobre todo cuando se ejecuta un clúster de producción, a escala, con varias aplicaciones. Puede encontrar más información en el apartado [3.1.5 Monitorización del sistema de esta guía].

8. A continuación, pulsar en la pestaña de [Etiquetas].



Se debe aplicar etiquetas a los recursos de Azure para proporcionar metadatos y organizarlos de forma lógica. Cada etiqueta consta de un nombre y un valor.

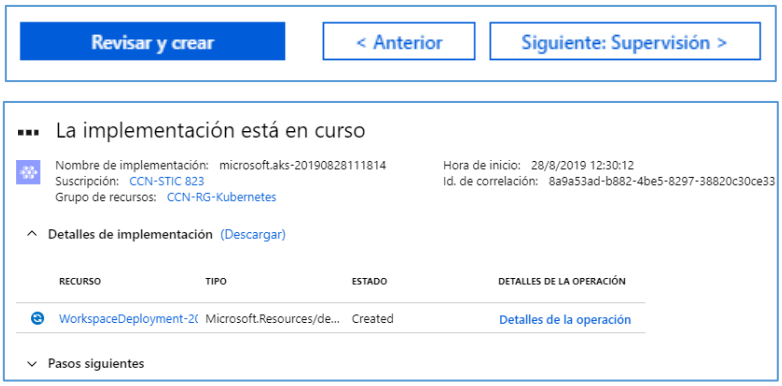
Por ejemplo, se puede aplicar el nombre "Kubernetes" y el valor "Producción" a todos los recursos en producción.

Después de aplicar las etiquetas, se puede recuperar todos los recursos de la suscripción que tengan ese nombre y valor de etiqueta.

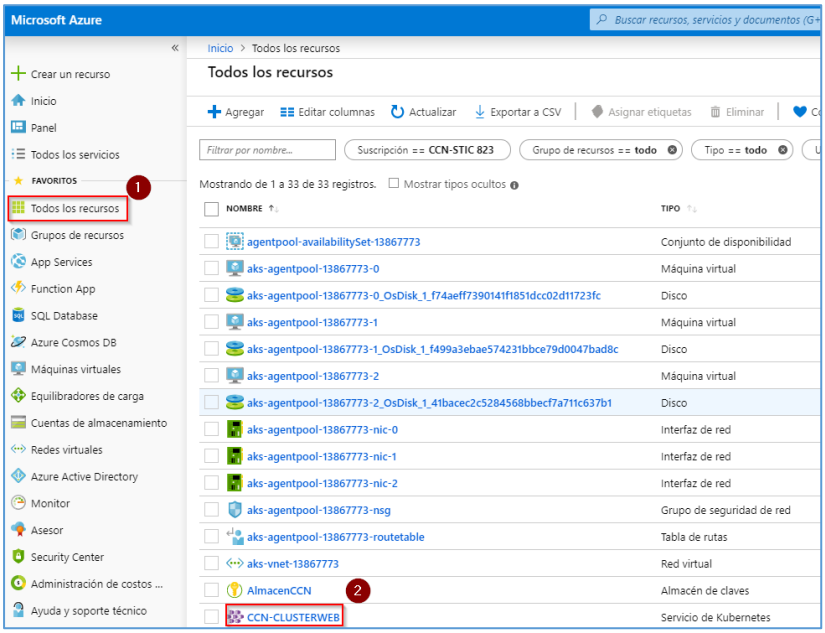
Este enfoque puede resultar útil si se necesita organizar recursos para la administración.

Nota: *Para obtener más información sobre las etiquetas en Azure consultar el apartado [3.2.2.1 Calificación]* ***de la guía*** *[CCN-STIC-884A – Guía de configuración segura de Azure].*

9. Por último, pulsar en [revisar y crear].



10. Para comprobar el nuevo clúster desde el portal de Azure pulsar en [todos los recursos] para encontrar el nuevo clúster de Kubernetes.



2.1 Configuraciones del clúster AKS

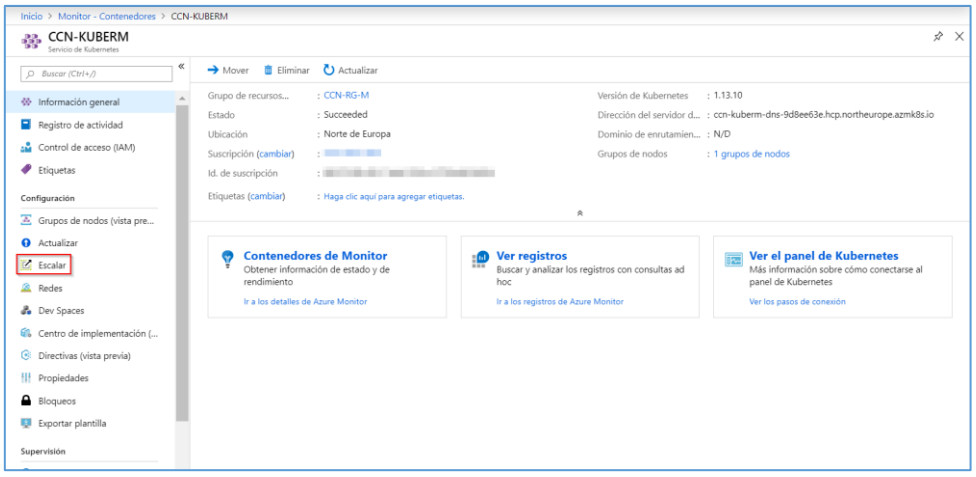
2.1.1 Escalar nodos del clúster.

2.1.1.1 Desde el portal de Azure

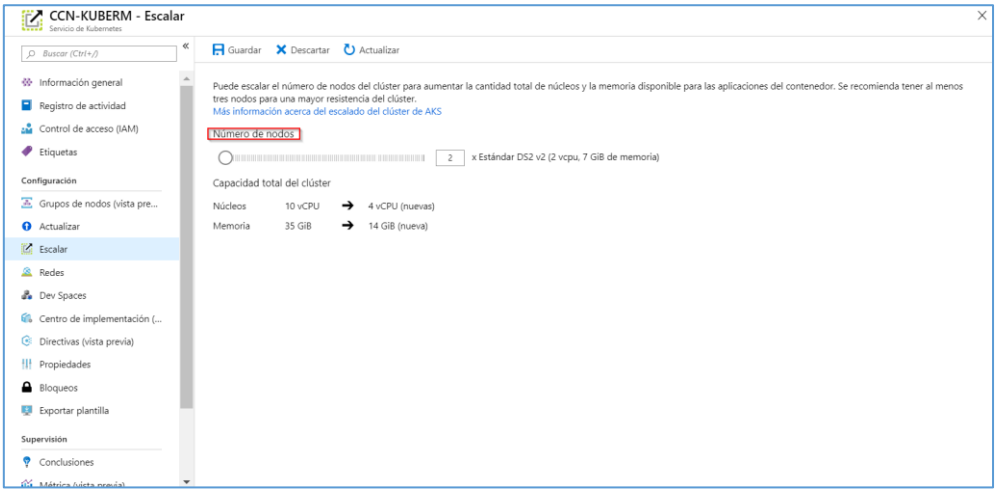
Una vez se haya desplegado el servicio de Kubernetes se pueden ampliar los nodos que forman el clúster en el caso que sea necesario.

Para ello, se realizan los siguientes pasos:

1. Buscar Azure Kubernetes Service
2. Pulsar en el clúster deseado y pulsar en el menú [Escalar].



3. Se añaden tantos nodos como sean necesarios. Se muestra también el tamaño del clúster antes de actualizar y los recursos que serán añadidos.



2.1.1.2 Desde Powershell

Para escalar los nodos a través de powershell realizar los siguientes pasos:

1. Obtener la información del clúster.

```
#    az aks show --resource-group Nombre_Grupo_Recursos --name Nombre_Servicio_AKS --
     query agentPoolProfiles
```

Se muestra toda la información del clúster, el campo count indica el nº de nodos del clúster.


```
{
  "availabilityZones": null,
  "count": 5,
  "enableAutoScaling": null,
  "maxCount": null,
  "maxPods": 30,
  "minCount": null,
  "name": "agentpool",
  "orchestratorVersion": "1.14.6",
  "osDiskSizeGb": 100,
  "osType": "Linux",
  "provisioningState": "Succeeded",
  "type": "VirtualMachineScaleSets",
  "vmSize": "Standard_DS2_v2",
  "vnetSubnetId": "/subscriptions/[redacted]/resourceGroups/CCN-RG-M/providers/Microsoft.Network/virtualNetworks/(
CN-RG-M-vnet/subnets/default"
 }
```

2. Se escala el clúster con el número de nodos que sea necesario. Puede ser mayor o menor el número. En el ejemplo lo reduciremos de 5 a 3 nodos.

```
#    az aks scale --resource-group Nombre_Grupo_Recursos        --name Nombre_Servicio_AKS    --
     node-count 3 --nodepool-name "Nombre_grupo_nodos"
```

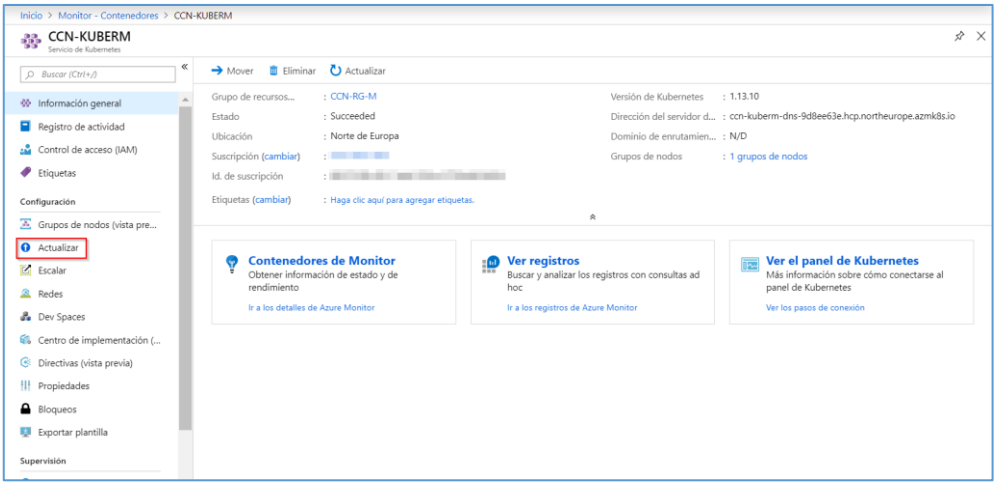
3. Se comprueba que el clúster tenga ahora tres nodos, utilizando el mismo comando que en el paso 1.

2.1.2 Actualizar clúster

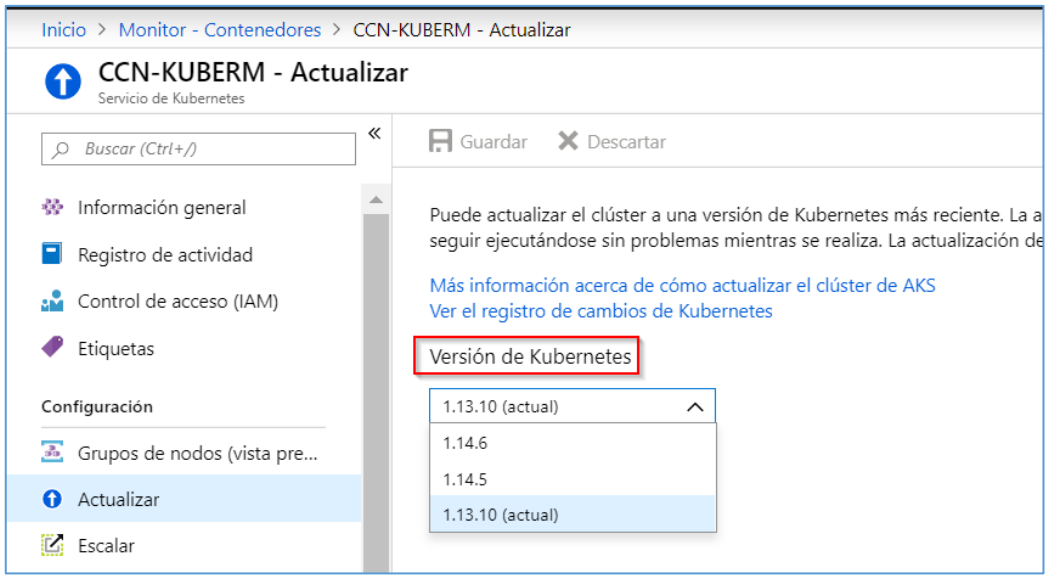
2.1.2.1 Desde el portal de Azure

Para actualizar el clúster de AKS a una versión más reciente se deben seguir los siguientes pasos.

1. Buscar Azure Kubernetes Service
2. Seleccionar el clúster deseado y pulsar en el menú [Actualizar].



3. Seleccionar la versión de AKS que se desea implementar en el clúster.



Nota: *Esta operación tarda dependiendo del número de nodos que tenga el clúster. Puede tardar hasta 10 minutos por nodo.*

2.1.2.2 Actualizar clúster desde Powershell

Para actualizar el clúster desde Powershell realizar los siguientes pasos:

1. Comprobar las actualizaciones del clúster, devolverá la salida en formato tabla.

```
#   az aks get-upgrades --resource-group Nombre_Grupo_Recursos --name Nombre_Servicio_AKS
--output table
```

Nota: *Si no hay ninguna actualización disponible mostrará el siguiente error: "ERROR: Table output unavailable. Use the --query option to specify an appropriate query. Use --debug for more info."*

2. Se actualiza el clúster con la versión deseada, y que se muestra con el paso anterior.

```
#   az aks upgrade --resource-group CCN-RG-M --name CCN-KUBERM --kubernetes-version 1.14.6
```

3. Se comprueba que se ha actualizado el clúster.

```
#   az aks show --resource-group Nombre_Grupo_Recursos --name Nombre_Servicio_AKS          --
    output table
```

3. CONFIGURACIÓN DE Azure Kubernetes Services

3.1 MARCO OPERACIONAL

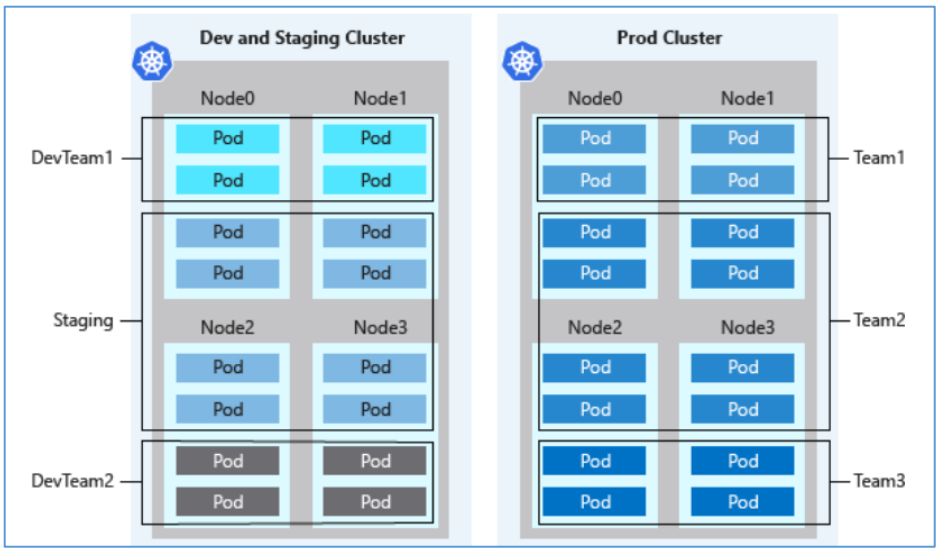
3.1.1 Planificación

3.1.1.1 Arquitectura de seguridad

Los entornos de Kubernetes, tanto en AKS como en cualquier otro lugar, no están completamente seguros ante el uso de varios inquilinos hostiles. En un entorno multiinquilino, varios inquilinos trabajan en una infraestructura compartida común. Como resultado, si no se puede confiar en todos los inquilinos, debe realizar una

planeación adicional para evitar que un inquilino afecte a la seguridad y el servicio de otro. Utilizar otras características de seguridad adicionales, como la directiva de seguridad de pod, y controles de acceso basados en roles (RBAC) más específicos puede dificultar las vulnerabilidades de seguridad. Sin embargo, para que la seguridad resulte efectiva cuando se ejecutan cargas de trabajo multiinquilino hostiles, el hipervisor es el único nivel de seguridad en el que debe confiar. El dominio de seguridad de Kubernetes se convierte en todo el clúster, no en un nodo específico.

En el caso de estos tipos de cargas de trabajo multiinquilino hostiles, debe usar clústeres que estén físicamente aislados.



Se recomienda el aislamiento físico para cada equipo independiente. En este modelo de aislamiento, los equipos o las cargas de trabajo se asignan a su propio clúster de AKS. Conlleva una sobrecarga financiera y administración adicional debido al mantenimiento que se debe realizar en cada nodo de los clústeres.

3.1.2 Control de acceso

3.1.2.1 Identificación

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

Nota: *Para obtener más información sobre identidades en Azure consultar el apartado [3.1.1 Identificación] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

Como recomendación, se debe asignar un rol RBAC de administrador de clústeres de Azure Kubernetes service a un grupo ya definido para los administradores de la API.

A continuación, desde la consola de Azure CLI siga estas instrucciones:

1. Obtener el ID del recurso de clúster de Kubernetes. Para ello, mediante la consola de *Azure CLI* ejecutar.

```
#   AKS_CLUSTER=$(az aks show --resource-group myResourceGroup --name myAKSCluster --query
    id -o tsv)
```

2. Obtener el ID del grupo al cual se asigna el rol de Administrador de clúster.

```
#   az ad group show --group UsuariosADM_AKS --query objectId -o tsv
```

3. Por último, asignar el rol al grupo.

```
#   az role assignment create \
#       --assignee $GROUP_ID \
#       --scope $AKS_CLUSTER \
#       --role "Azure Kubernetes Service Cluster Admin Role"
```

Nota: *Para obtener más información sobre los roles en Azure consultar el apartado [3.1.1.1 Requisitos de Acceso] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.2.2 Segregación de funciones y tareas

Es posible configurar Azure Kubernetes Service (AKS) para utilizar Azure Active Directory (AD) para la autenticación de usuarios. En esta configuración se inicia sesión en un clúster de AKS mediante un token de autenticación de Azure AD. También se puede configurar el control de acceso basado en roles (RBAC) de Kubernetes para limitar el acceso a los recursos de clúster en función de la identidad de los usuarios o la pertenencia a un grupo.

Se debe crear roles personalizados para la gestión y administración del clúster de Kubernetes.

Existen diferentes roles que se deben emplear.

- **Rol administrador de clúster de Kubernetes**

Utilizado para administrar el clúster de Kubernetes, se compone del siguiente permiso:

Microsoft.ContainerService/managedClusters/listClusterAdminCredential/action

- **Rol de usuario de clúster de Kubernetes**

Utilizado para tener permisos de lectura sobre el clúster de Kubernetes, se compone del siguiente permiso:

Microsoft.ContainerService/managedClusters/listClusterUserCredential/action

- **Redes**

Para usar redes avanzadas en las que la red virtual y la subred o las direcciones IP públicas se encuentran en otro grupo de recursos. Asignar los siguientes permisos de rol:

Microsoft.Network/virtualNetworks/subnets/join/action
Microsoft.Network/virtualNetworks/subnets/read
Microsoft.Network/virtualNetworks/subnets/write
Microsoft.Network/publicIPAddresses/join/action

Microsoft.Network/publicIPAddresses/read
Microsoft.Network/publicIPAddresses/write

O bien, asignar el rol integrado Colaborador de la red en la subred dentro de la red virtual.

- **Storage**

Es posible que sea necesario acceder a los recursos de disco existentes en otro grupo de recursos. Asignar los siguientes permisos de rol:

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write

O bien, asignar el rol integrado Colaborador de la cuenta de almacenamiento en el grupo de recursos.

Nota: *Además, seguir el enlace: https://docs.microsoft.com/es-es/azure/aks/operator-best-practices-cluster-security#app-armor donde se añaden más recomendaciones de protección como AppArmor, seccomp (secure computing) y Pod Security Policies.*

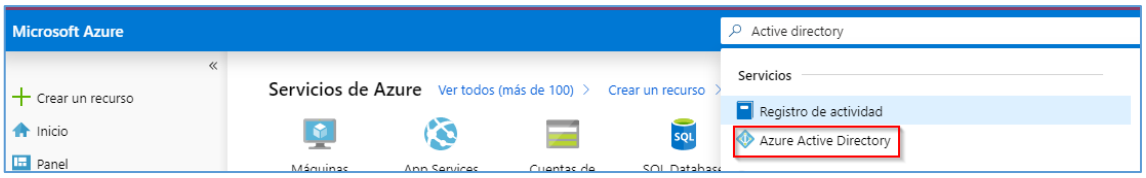
Nota: *Para obtener más información sobre los roles en Azure consultar el apartado [3.1.1.1 Requisitos de Acceso] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.2.3 Mecanismos de autenticación

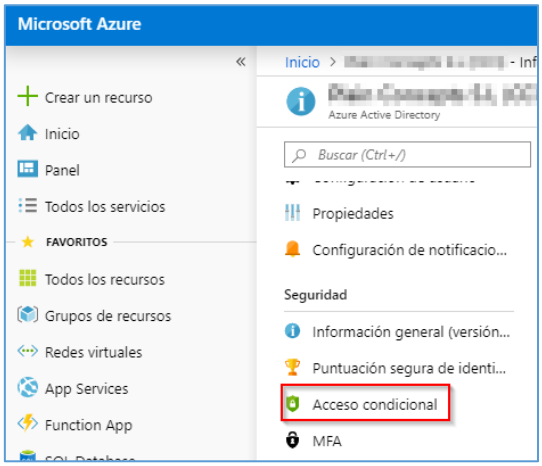
En los mecanismos de autenticación se recomienda crear una nueva condición política que estará integrada en los mecanismos de autenticación.

Para ello, se deben realizar estas instrucciones.

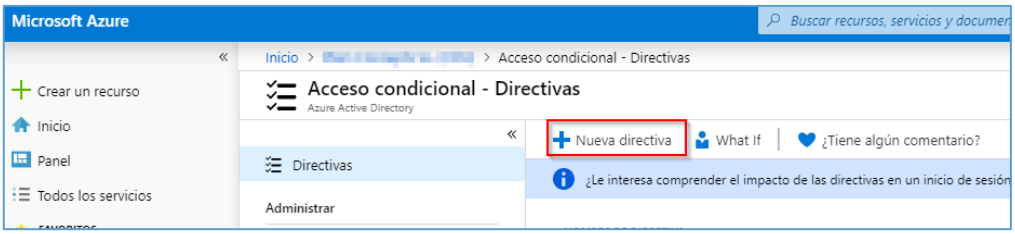
1. En el buscador del portal Azure buscar Active Directory.



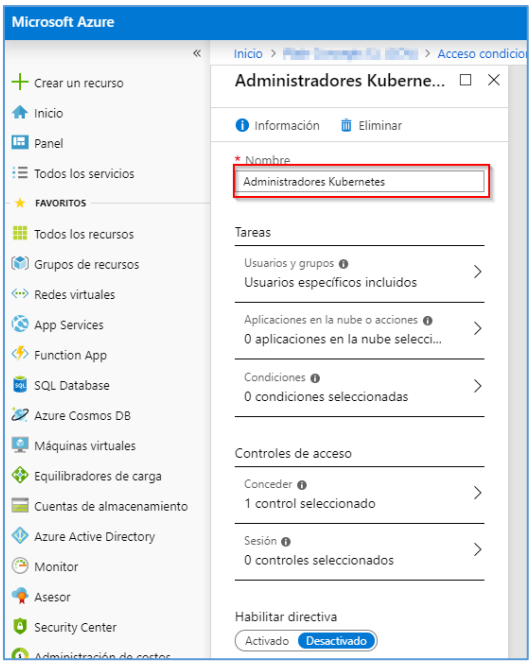
2. A continuación, [acceso condicional].



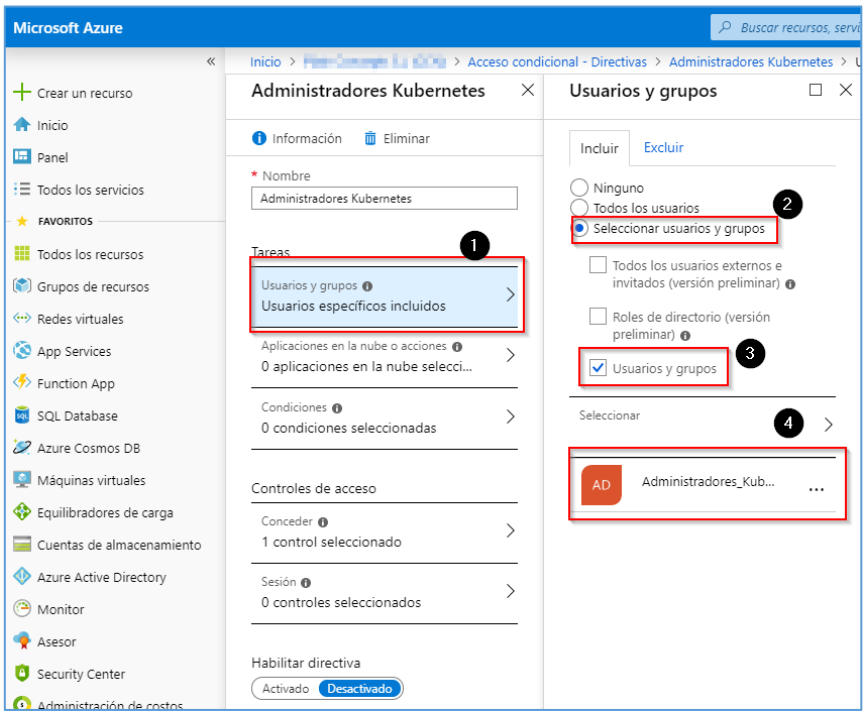
3. Pulsar en [nueva directiva].



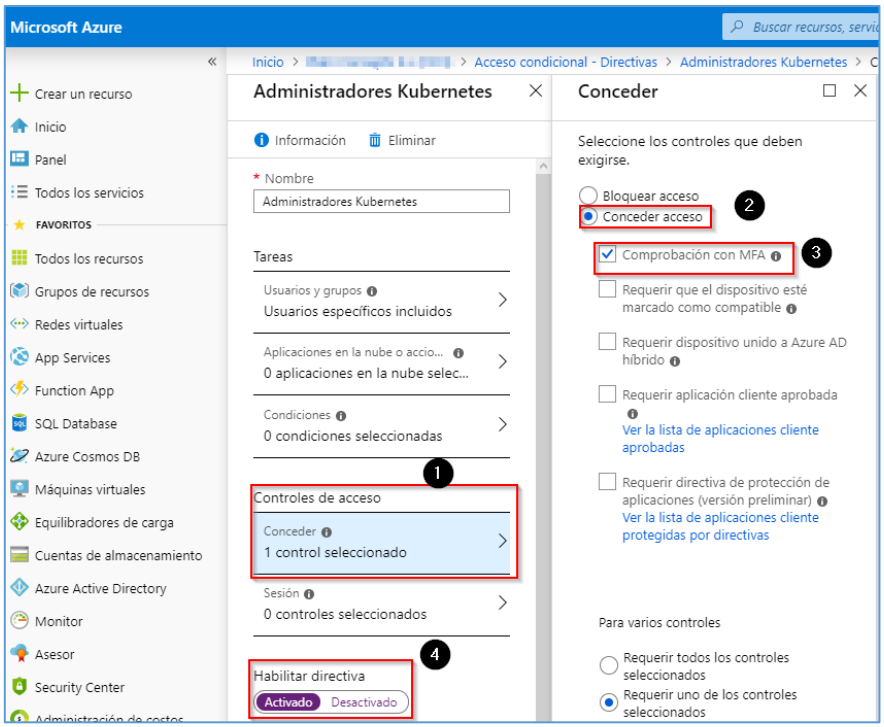
4. A continuación, se debe definir un nombre para la directiva.



5. A continuación, elegir el grupo de administradores al que se le aplica este método de autenticación.



6. Pulsar en [Controles de Acceso], luego [conceder acceso/Comprobaciones con MFA]



7. Habilitar la directiva y pulsar en [crear].

Al finalizar ya tendrá creada la nueva directiva que aplicará la autenticación multi-factor para los administradores de Kubernetes.

3.1.2.4 Acceso local (local logon)

Para el acceso local se recomienda aplicar una directiva de acceso condicional. Donde se puede definir que rangos de ips tienen acceso a sus aplicaciones como desde la ubicación geográfica desde donde se conectan.

Nota: *Para obtener más información sobre el acceso condicinal en Azure consultar el apartado [3.1.1.1 Requisitos de Acceso] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.2.5 Acceso remoto (remote login)

Kubernetes es una solución *cloud* accesible por el usuario final a través de internet.

Se recomienda que todos los dispositivos físicos estén unidos Azure AD, MFA.

Nota: *Para obtener más información sobre MFA en Azure consultar el apartado [3.1.1.4 Mecanismos de autenticación] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.3 Explotación

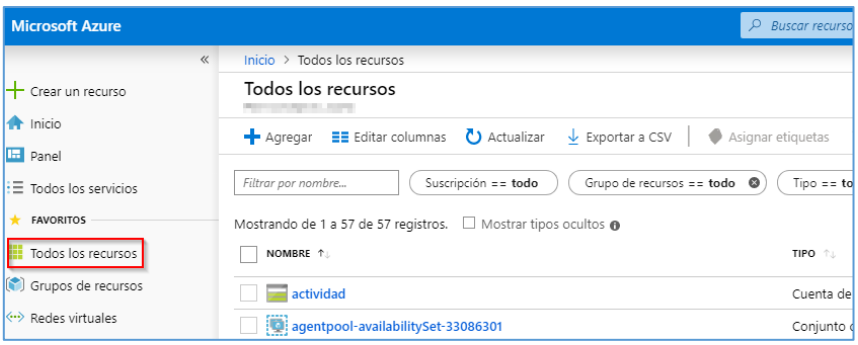
3.1.3.1 Registro de la actividad de los usuarios

Mediante los registros de actividad, se puede determinar:

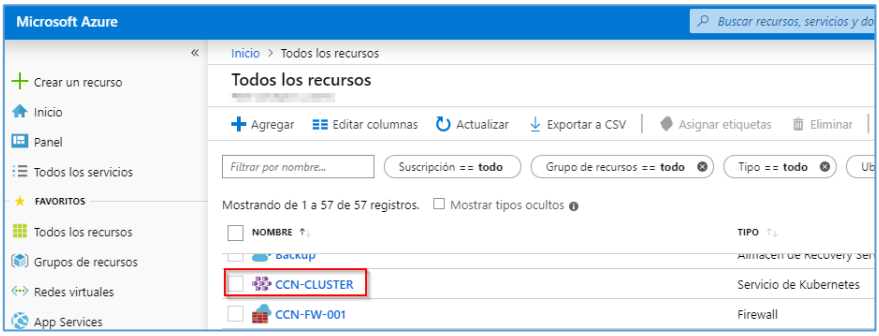
- Qué operaciones se realizaron en los recursos en la suscripción.
- Quién inició la operación.
- Cuando tuvo lugar la operación.
- El estado de la operación.
- Los valores de otras propiedades que podrían ayudar en la investigación de la operación.

Para ello, seguir los siguientes pasos:

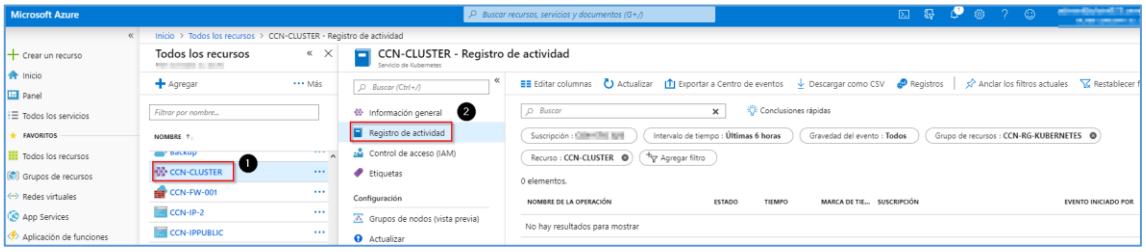
1. Desde el portal del Azure pulsar en [todos los recursos].



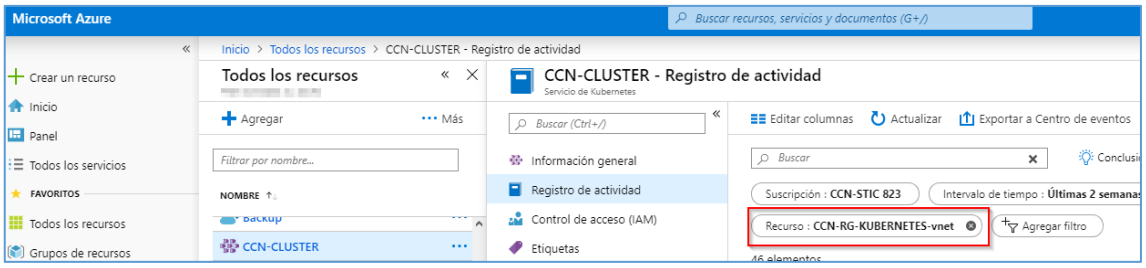
2. Se debe buscar el clúster de Kubernetes.



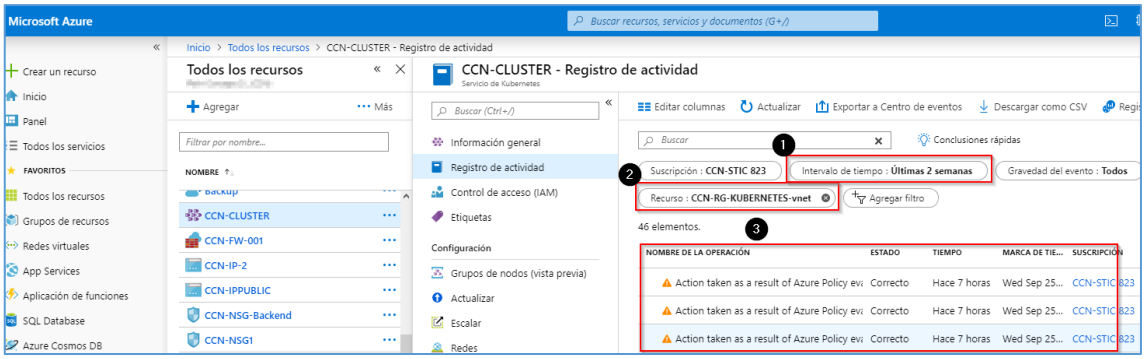
3. Desde el cluster de Kubernetes, pulsar en [Registro de actividad].



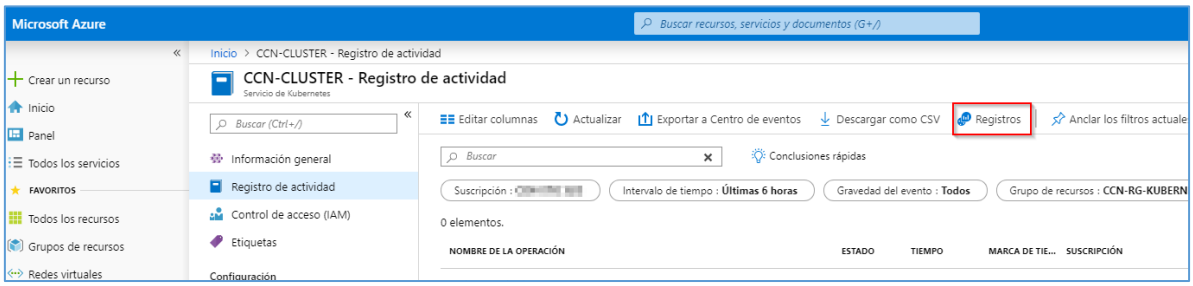
4. Desde este panel se puede filtrar los registros. Por ejemplo, en [Recurso] seleccionar el cluster.



5. Se muestran los resultados de búsqueda.

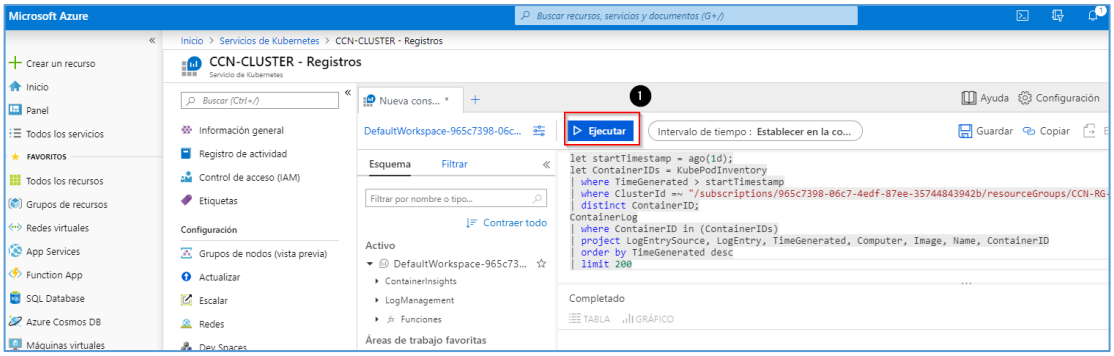


6. Además, se puede personalizar una búsqueda desde el Workspace. Para ello pulsar en [registro].



7. Se puede ejecutar la siguiente query para ver todos los usuarios que realizaron una acción en Kubernetes.
8. Copie el contenido y pulsar en ejecutar.

```
#   let startTimestamp = ago(1d);
#   let ContainerIDs = KubePodInventory
#   | where TimeGenerated > startTimestamp
#   |       where       ClusterId       =~       "/subscriptions/965c7398-06c7-4edf-87ee-35744843942b/resourceGroups/CCN-RG-KUBERNETES/providers/Microsoft.ContainerService/managedClusters/CCN-CLUSTER"
#   | distinct ContainerID;
#   ContainerLog
#   | where ContainerID in (ContainerIDs)
#   | project LogEntrySource, LogEntry, TimeGenerated, Computer, Image, Name, ContainerID
#   | order by TimeGenerated desc
#   | limit 200
```



Nota: *Para obtener más información sobre el registro de actividad de los usuarios en Azure. Consultar el apartado [3.1.2.1 Registro de actividad de los usuarios] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.3.2 Protección de claves criptográficas

Para mejorar la seguridad y el cumplimiento de las máquinas virtuales, se debe cifrar los discos virtuales en Azure. Los discos se cifran mediante claves criptográficas que están protegidas en Azure Key Vault. Esto se puede aplicar tanto para los discos virtuales de Kubernetes como cualquier otro disco del *Tenant*.

En este primer paso se debe crear un almacén de Azure Key Vault para almacenar las claves criptográficas. En Azure Key Vault puede almacenar claves, secretos o contraseñas que permiten la implementación segura en las aplicaciones y los servicios.

Para el cifrado de discos virtuales, crear una instancia de Key Vault para almacenar una clave criptográfica que se usa para cifrar o descifrar los discos virtuales.

1. Desde el módulo de PowerShell crear una clave criptográfica en Azure Key Vault.

```
#   $rgName = "myResourceGroup"
#   $location = " North Europe"
#
#   Register-AzResourceProvider -ProviderNamespace "Microsoft.KeyVault"
#   New-AzResourceGroup -Location $location -Name $rgName
```

El almacén de Azure Key Vault que contiene las claves criptográficas y los recursos de proceso asociados, como el almacenamiento y la propia máquina virtual, tienen que encontrarse en la misma región.

2. Se debe crear una instancia de Azure Key Vault con New-AzKeyVault y habilitar Key Vault para usarlo con el cifrado de discos.

```
#   $keyVaultName = "myKeyVault$(Get-Random)"
#   New-AzKeyVault -Location $location `
#       -ResourceGroupName $rgName `
#       -VaultName $keyVaultName `
#       -EnabledForDiskEncryption
```

3. Se debe tener acceso para solicitar las claves criptográficas cuando la máquina virtual arranca para descifrar los discos virtuales. Para ello crear una clave criptográfica en la instancia de Key Vault con Add-AzureKeyVaultKey.

```
#   Add-AzKeyVaultKey -VaultName $keyVaultName `
#       -Name "myKey" `
#       -Destination "Software"
```

Cifrado de una máquina virtual

1. Se debe cifrar la máquina virtual con Set-AzVMDiskEncryptionExtension mediante la clave de Azure Key Vault.

Consola PowerShell

```
#   $keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $rgName;
#   $diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
#   $keyVaultResourceId = $keyVault.ResourceId;
#   $keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName $keyVaultName -Name myKey).Key.kid;
#
#   Set-AzVMDiskEncryptionExtension -ResourceGroupName $rgName `
#       -VMName "myVM" `
#       -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl `
#       -DiskEncryptionKeyVaultId $keyVaultResourceId `
#       -KeyEncryptionKeyUrl $keyEncryptionKeyUrl `
#       -KeyEncryptionKeyVaultId $keyVaultResourceId
```

Nota: *La máquina virtual se reinicia durante el proceso.*

2. Una vez finalizado el proceso de cifrado y se reinicie la máquina virtual, revisar el estado del cifrado con el siguiente comando de PowerShell Get-AzVmDiskEncryptionStatus.

```
# Get-AzVmDiskEncryptionStatus -ResourceGroupName $rgName -VMName "myVM"
```

Nota: *Se puede aplicar la misma configuración en servidores Linux. Para ello, realizar los pasos de este enlace:*

https://docs.microsoft.com/es-es/azure/virtual-machines/linux/encrypt-disks

Nota: *Para obtener más información sobre Azure Key Vault consultar el apartado [3.2.2.2 Cifrado] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.4 Continuidad del servicio

3.1.4.1 Plan de continuidad

A medida que los clústeres en Azure Kubernetes Service (AKS) son administrados, el tiempo de actividad de la aplicación pasa a ser importante.

Kubernetes proporciona alta disponibilidad mediante el uso de varios nodos en un conjunto de disponibilidad. Pero estos múltiples nodos no protegen al sistema frente a un error de la región.

Se puede implementar la aplicación en varios clústeres de AKS en diferentes regiones.

Existen dos servicios:

- **Disponibilidad por región de AKS:** Se puede elegir regiones cerca de los usuarios. AKS se expande continuamente en nuevas regiones.
- **Regiones emparejadas de Azure:** Para el área geográfica, se puede elegir dos regiones que estén emparejadas entre sí. Las regiones emparejadas coordinan las actualizaciones de la plataforma y dan prioridad a los esfuerzos de recuperación cuando resulta necesario.

Nota: *Para obtener más información sobre el plan de continuidad consultar el apartado [3.1.4 Plan de continuidad] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.5 Monitorización del sistema

3.1.5.1 Detección de intrusión

Para mantener el entorno protegido, se debe bloquear el inicio de sesión de los usuarios sospechosos. Es necesario que cree una nueva política de autenticación.

Nota: *Para obtener más información sobre detección de intrusión consultar el apartado [3.1.6.1 Detección de intrusión] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.1.5.2 Sistema de métricas

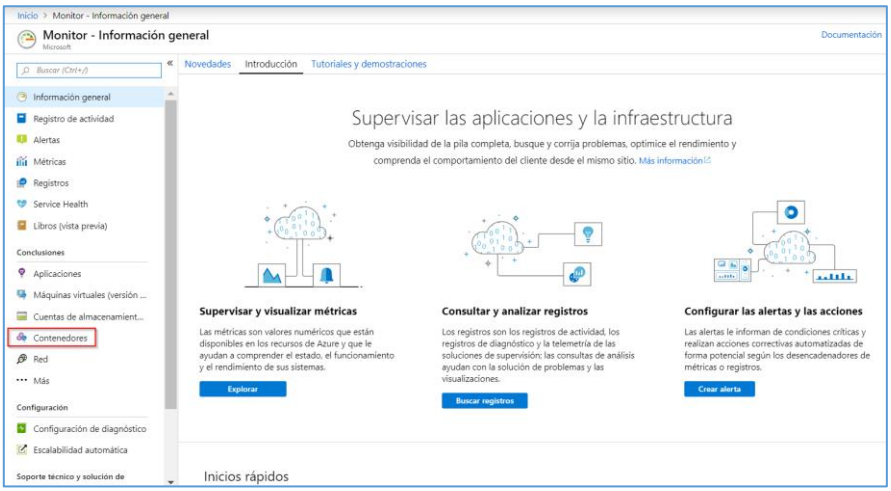
Para obtener métricas de rendimiento y un control de los contenedores de Kubernetes, se debe crear una nueva área de trabajo en Log Analytics.

La capacidad de supervisar el rendimiento se basa en un agente de Log Analytics en contenedores para Linux, desarrollado específicamente para Azure Monitor. Este agente especializado recopila datos de rendimiento y de eventos de todos los nodos del clúster, y el agente se implementa y registra automáticamente en el área de trabajo de Log Analytics.

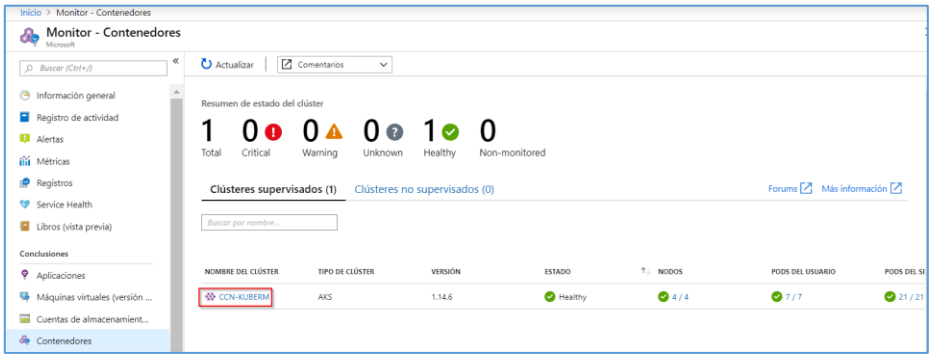
Nota: *Para obtener más información sobre log analytics consultar el apartado [3.1.2.2 Protección de los registros de actividad] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

Para ver las métricas de Kubernetes seguir los siguientes pasos:

1. Desde el buscador del portal de Azure buscar Monitor.
2. Pulsar en [Contenedores].

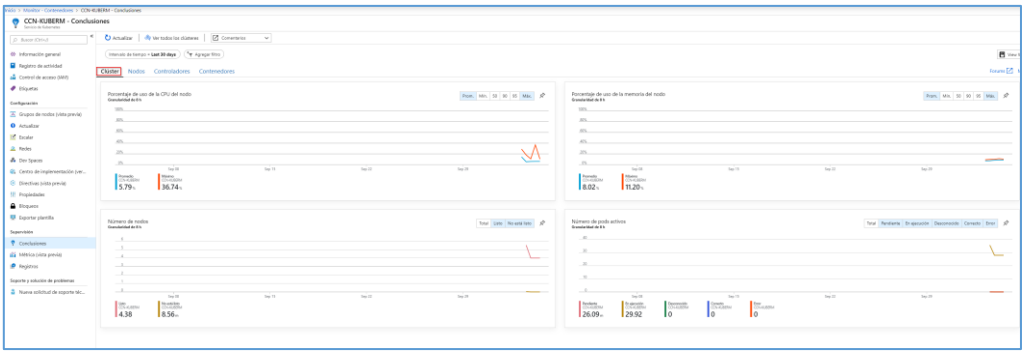


3. Aparecen todos los clústeres existentes con una visión general de cada uno, para obtener más información seleccionar el clúster para ver su monitorización.

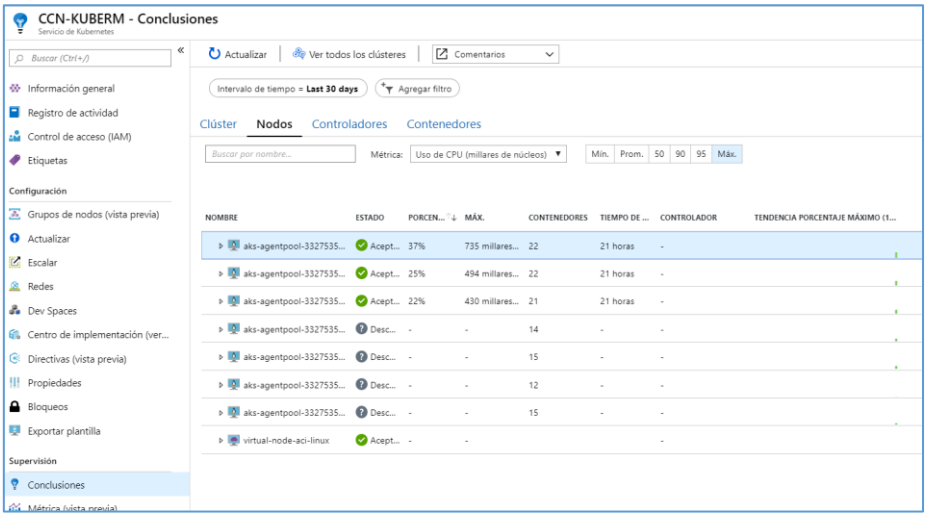


4. Una vez dentro del clúster las métricas se dividen en varios campos:

   Clúster: Métricas generales del clúster, como son: CPU, RAM de los nodos, nº de nodos en el clúster y nº de pods activo.

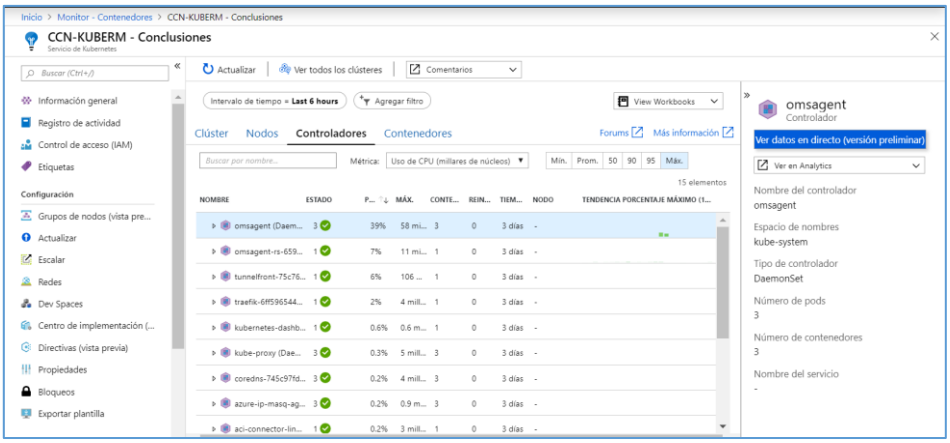


Nodos: Muestra métricas de cada nodo y de los procesos que están siendo ejecutados. Para desplegar los procesos de un nodo tan solo hay que pulsar en el nodo que se quiere desplegar.

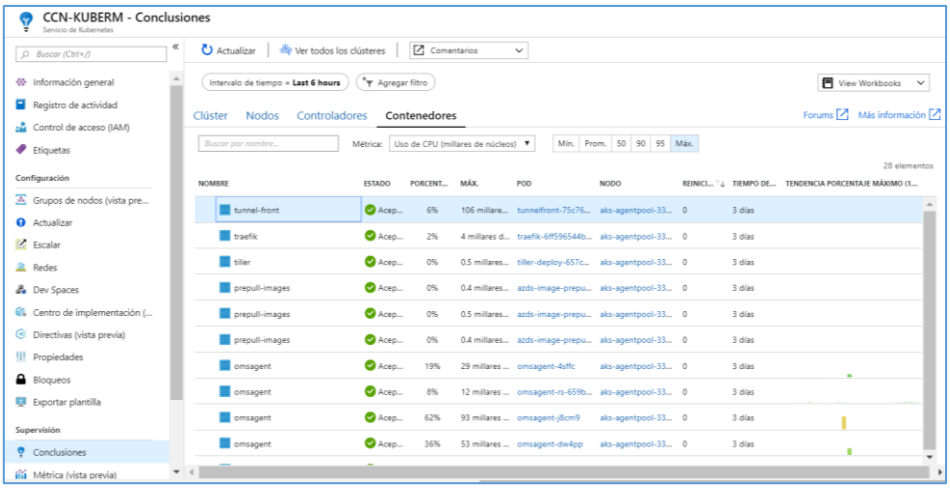


Controladores: Del mismo modo que con los nodos se puede ver las métricas de los controladores de Kubernetes.

Si se pulsa en el botón **Ver datos en directo**, en el caso de que este ejecutando alguna operación le saldrá la información al momento, en tiempo real.



Contenedores: Muestra qué contenedores están en ejecución, qué imagen de contenedor están ejecutando y dónde se ejecutan los contenedores.



3.2 MEDIDAS DE PROTECCION

3.2.1 Protección de las comunicaciones

3.2.1.1 Segregación de redes

Con Azure Container Networking Interface (CNI) cada pod obtiene una dirección IP de la subred, pudiendo acceder a él directamente. De esta forma evitamos realizar la traducción de direcciones de red que se realiza con las redes clásicas.

Este direccionamiento debe ser único y requiere de una planificación, ya que existe la posibilidad de agotar las direcciones IP a medida que crecen las aplicaciones.

Requisitos

- La red virtual del clúster debe permitir la conectividad saliente con internet.
- No se puede crear más de un clúster por subred.
- Los clústeres **no** pueden utilizar los rangos de direcciones **169.254.0.0/16, 172.31.0.0/16, 172.30.0.0/16, 192.0.2.0/24**
- La entidad de servicio utilizada por el clúster debe tener permisos de colaborador de red.

```
"Microsoft.Network/virtualNetworks/subnets/join/action"

"Microsoft.Network/virtualNetworks/subnets/read"
```

Despliegue red CNI

Al desplegar la red se debe tener en cuenta el nº de pods que se tiene previsto ejecutar, así como el nº de nodos (máximo) que puede tener el clúster, ya que se asigna una dirección IP de la red tanto a los nodos como a los pods.

Para el despliegue se necesitan los siguientes parámetros.

- Red virtual
- Subred

- Intervalo de direcciones de servicio Kubernetes: Conjunto de direcciones IP que Kubernetes asigna a servicios internos del clúster.

  No debe:
  - Estar dentro del intervalo de direcciones IP de la red virtual del clúster.
  - Superponerse con ninguna otra red virtual.
  - Superponerse con ninguna dirección IP local.
  - Estar dentro de los intervalos 169.254.0.0/16, 172.30.0.0/16, 172.31.0.0/16 ni 192.0.2.0/24

- Dirección IP del servicio DNS de Kubernetes: La dirección IP del servicio DNS del clúster. Esta dirección debe estar dentro del intervalo de direcciones del servicio Kubernetes. No utilizar la primera dirección IP en el intervalo de direcciones. La primera dirección del intervalo de la subred se usa para la dirección kubernetes.default.svc.cluster.local.
- Dirección del puente de Docker: La dirección de red del puente de Docker representa la dirección de red del puente de *docker0* predeterminada presente en todas las instalaciones de Docker. Aunque los pods o los clústeres de AKS no usan el puente de *docker0*, debe configurar esta dirección para seguir admitiendo escenarios como la *compilación de Docker* en el clúster de AKS.

  Es necesario seleccionar un CIDR para la dirección de red del puente de Docker, ya que, de lo contrario, Docker seleccionará automáticamente una subred que podría entrar en conflicto con otros CIDR. Se debe elegir un espacio de direcciones que no entre en conflicto con el resto de los CIDR de las redes, incluidos el CIDR de servicio del clúster y el CIDR del pod.

Limitaciones

Recurso Azure	Límite
Virtual Network	El tamaño puede ser de hasta /8, limitado 65536 direcciones IP.
Subnet	Debe ser lo suficientemente grande como para dar cabida a los nodos, los pods y a todos los recursos de Kubernetes y de Azure que se pueden aprovisionar en el clúster, dentro de los límites de la Virtual Network.
Intervalo de direcciones Kubernetes	Este intervalo no lo debe usar ningún elemento de red de esta red virtual o que esté conectado a ella. El CIDR de la

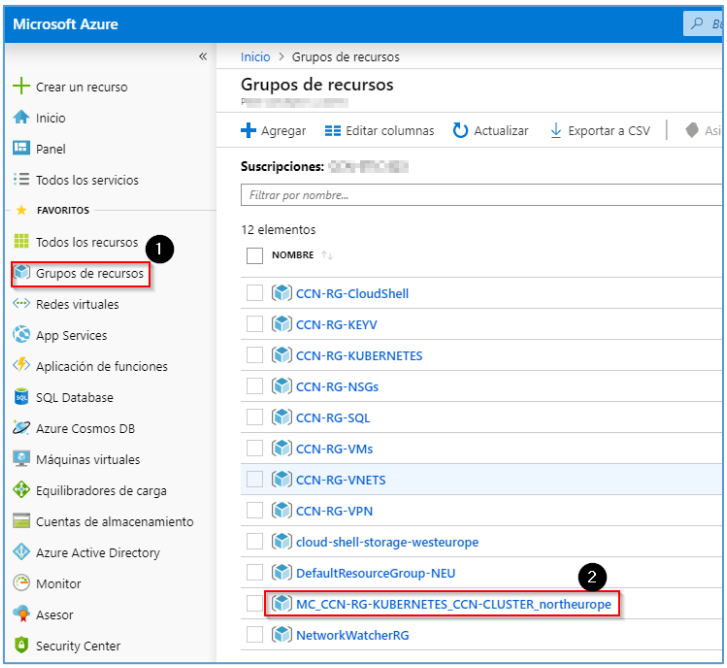
	dirección del servicio debe ser menor que /12.
Dirección IP del servicio DNS de Kubernetes	Dirección IP del intervalo de direcciones del servicio de Kubernetes que se usará en la detección de servicios de clúster. No utilizar la primera dirección IP en el intervalo de direcciones, como .1. La primera dirección del intervalo de la subred se usa para la dirección *kubernetes.default.svc.cluster.local*.
Dirección de puente de Docker	La dirección de red del puente de Docker representa la dirección de red del puente de *docker0* predeterminada presente en todas las instalaciones de Docker. Aunque los pods o los clústeres de AKS no usan el puente de *docker0*, debe configurar esta dirección para seguir admitiendo escenarios como la *compilación de Docker* en el clúster de AKS.

3.2.1.2 Perímetro seguro

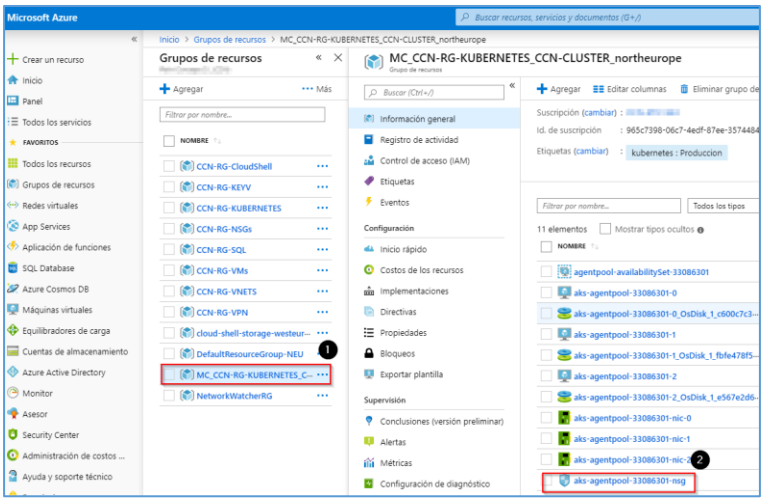
Los clústeres de **AKS** tienen acceso de salida a Internet ilimitado. Este nivel de acceso a la red permite que los nodos y servicios que ejecuta accedan a recursos externos según sea necesario. Como recomendación, se debe restringir el tráfico de salida, es necesario el acceso a un número limitado de puertos y direcciones para mantener las tareas de mantenimiento del clúster en buen estado.

A continuación, realizar los siguientes pasos.

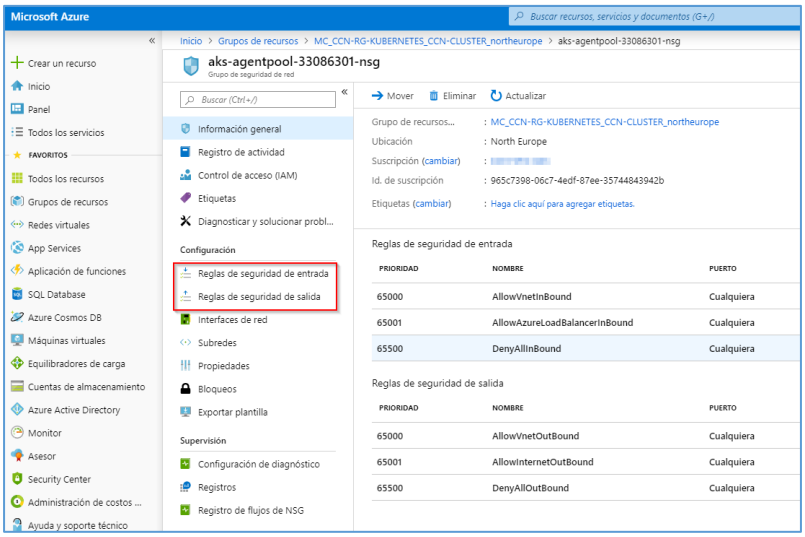
1. Pulsar en [grupo de recursos] en el portal de Azure.



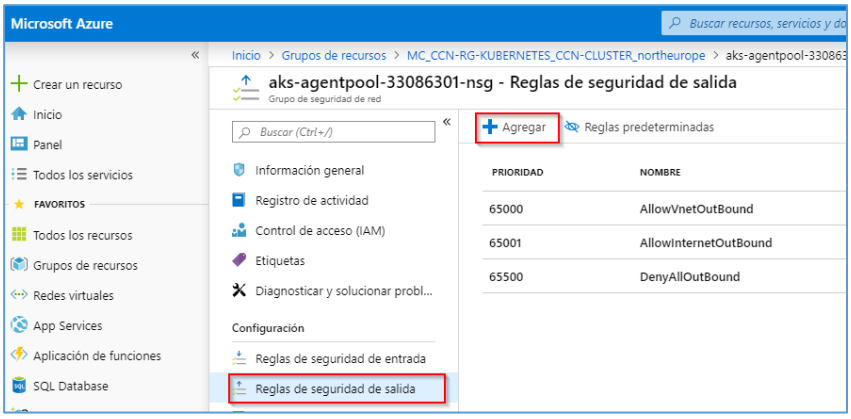
2. Pulsar en el grupo de recursos de seguridad de red de Kubernetes.



3. Pulsar en [Reglas de seguridad de salida].



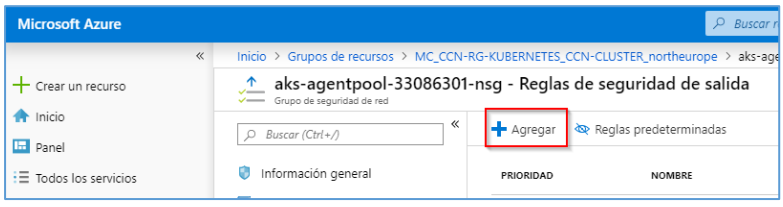
4. Pulsar en [agregar].



Nota: *Azure crea las reglas 65000, 65501 y el 65500 de forma predeterminadas en cada grupo de seguridad de red*.

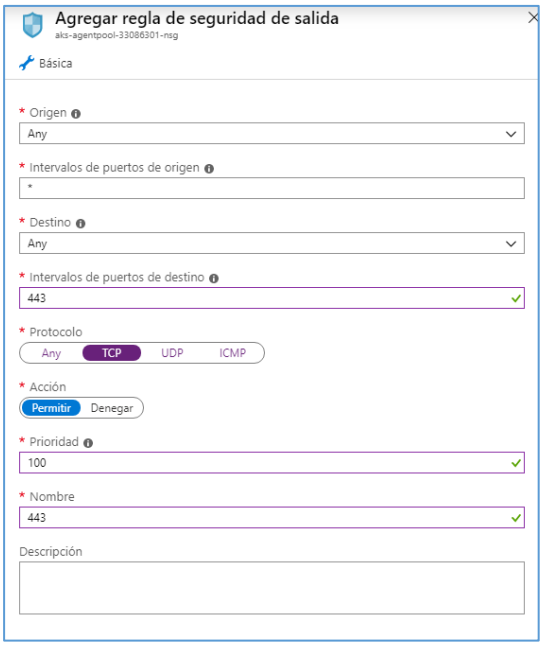
A continuación, agregar los puertos de salida recomendados para kubernetes.

5. Pulsar en [agregar].

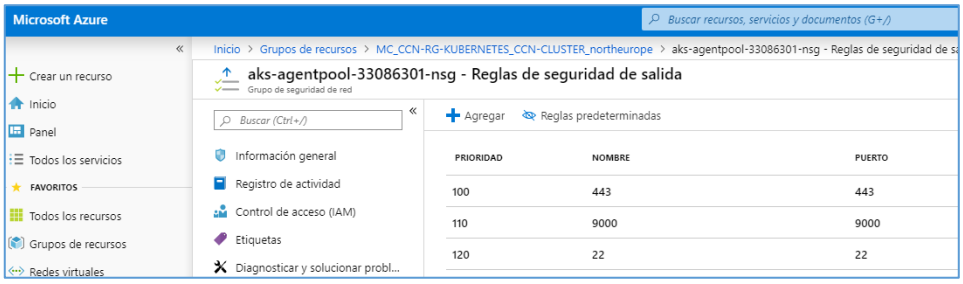


6. Agregar los siguientes puertos.

- Puerto TCP 443
- Puerto TCP 9000 y puerto TCP 22 para el pod de la parte delantera del túnel para comunicarse con el extremo de túnel en el servidor de la API.



Al finalizar, aparecerán las nuevas reglas.



Nota: *Para obtener más información sobre reglas de NSG consultar el apartado [3.2.1.2 Perímetro seguro] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

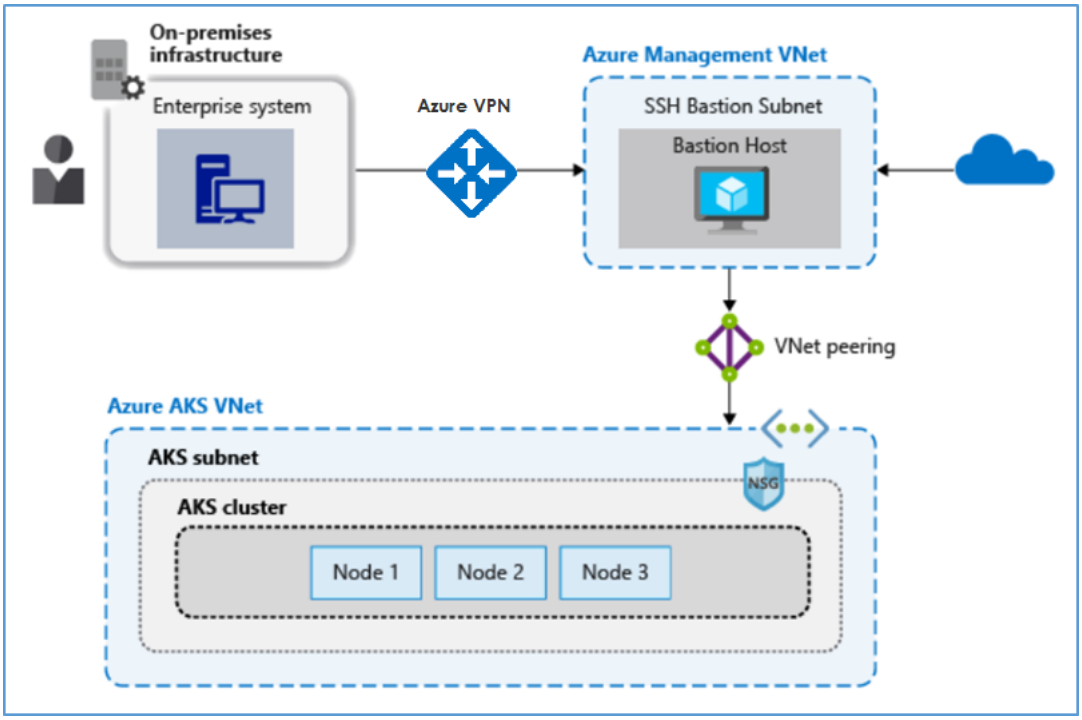
Pasarela de aplicaciones

Para la conexión con los clústeres de kubernetes se recomienda no exponer la conectividad de los nodos de AKS. Para ello, se recomienda crear una pasarela de aplicaciones desde una red de administración.

La mayor parte de las operaciones en AKS se podrán realizar con las herramientas de administración de Azure o mediante el servidor API de Kubernetes.

Los nodos pasarían a estar conectados a una red privada y para conectarse a ellos o realizar tareas de mantenimiento se debe hacer desde un host de salto en una red de administración.

A continuación, un gráfico de la arquitectura:



A su vez para conectarse a la red de administración se aconseja crear una conexión **VPN** y controlar el acceso con grupos de seguridad de red (NSG).

Realizar los siguientes pasos para configurar la pasarela (una vez creados ya el clúster de AKS y la red de administración):

1. Crear la VPN con la red de administración.
2. Proteger las comunicaciones con un grupo de seguridad de red.
3. Realizar un peering entre la red de administración y la red de los nodos.

Nota: *Para obtener más información sobre la creación de una red consultar el apartado [3.2.1.1 Segregación de redes] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

Nota: *Para obtener más información sobre los grupos de seguridad de red consultar el apartado [3.2.1.2 Perímetro seguro] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

Nota: *Para obtener más información sobre la creación de una VPN consultar el apartado [3.2.1.3 Protección de la confidencialidad] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

Directivas de red

De forma predeterminada, todos los pods de un clúster de AKS pueden enviar y recibir tráfico sin limitaciones. Para mejorar la seguridad, se puede definir reglas que controlen el flujo de tráfico.

Se pueden ver las directivas de red en acción, para ello hay que crear y expandir una directiva que defina el flujo de tráfico para:

- Denegar todo el tráfico al pod.

- Permitir el tráfico en función de las etiquetas de pod.
- Permitir el tráfico según el espacio de nombres

Se recomienda seguir las instrucciones de este enlace:

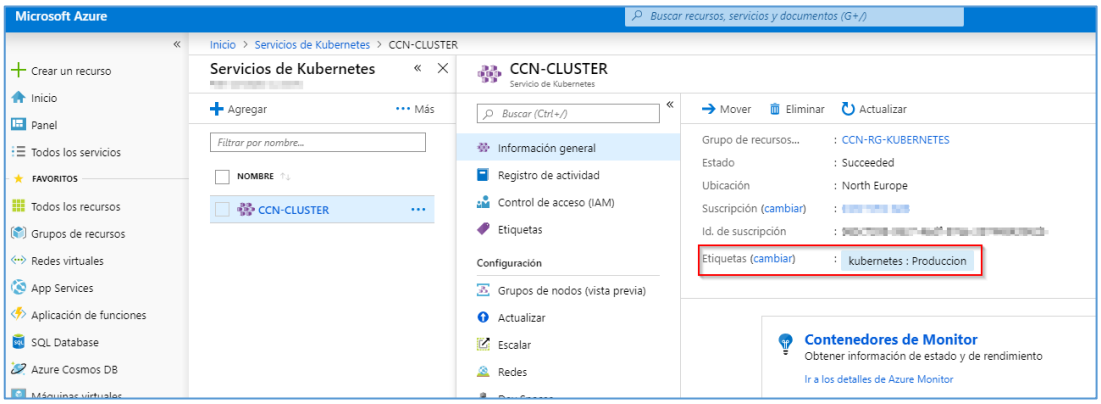
https://docs.microsoft.com/es-es/azure/aks/use-network-policies

3.2.2 Protección de la información

3.2.2.1 Calificación de la información

Aplicar etiquetas a los recursos de Azure facilita la organización de los servicios de Kubernetes. Cada etiqueta consta de un nombre y un par de valores.

Las etiquetas le permiten recuperar los recursos relacionados que se encuentran en distintos grupos de recursos. Este enfoque puede resultar útil si necesita organizar recursos para la administración.



Nota: *Para obtener más información sobre etiquetas consultar el apartado [3.2.2.1 Calificación de la información] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

3.2.2.2 Copias de seguridad (backup)

Azure Backup organiza las copias de seguridad de las máquinas y administra la configuración de los procedimientos de restauración. También tiene dos formas de hacer copia de seguridad de los datos para recuperación operativa.

El servicio Azure Backup se ejecuta en la nube y mantiene los puntos de recuperación, exige el cumplimiento de directivas y le permite administrar la protección de las aplicaciones y los datos.

Nota: *Para obtener más información sobre Azure Backup consultar el apartado [3.2.2.3 Copias de seguridad] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*

4. GLOSARIO Y ABREVIATURAS

4.1 GLOSARIO Y ABREVIATURAS

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

Término	Definición
Clúster	Son recursos físicos o virtuales, y recursos de almacenamiento utilizados por Kubernetes en donde los pods son desplegados, gestionados y replicados. Kubernetes puede ser utilizado en diferentes sistemas como: Windows Azure, Debian, Ubuntu, RedaHat, entre otros.
Pods	Son la unidad más pequeña que comprende uno o más contenedores Docker que funcionan bajo una misma unidad. En muchos casos un Pod se compone de un solo contenedor, pero su capacidad de alojar varios contenedores muy cerca uno de otro es una característica muy poderosa de Kubernetes.
Replication Controllers	Manejan el ciclo de vida del pod, se aseguran de que el número de réplicas automáticas del pod se encuentren ejecutando, creando y destruyendo los pods, como sea requerido.
Services	Los servicios (services) permiten acceder a los contenedores con un nombre único de DNS y direcciones IP estables.
FQDN	Un FQDN (sigla en inglés de fully qualified domain name) es un nombre que incluye el nombre del servidor y el nombre de dominio asociado a ese equipo.
Labels	Son fundamentales y son utilizados para organizar y seleccionar un grupo de objetos en pares del tipo key:value. Ayudan a obtener las listas de los servidores a donde el el tráfico debe pasar.

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="3">Configuracion</th><th>Estado</th></tr>
<tr><td>op</td><td colspan="4">Marco Operacional</td></tr>
<tr><td>op.acc</td><td colspan="4">Control de Acceso</td></tr>
<tr><td rowspan="3">op.acc.1</td><td colspan="4">Identificación</td></tr>
<tr><td colspan="3" rowspan="2">Para la correcta gestión de AKS, se ha configurado cuentas y grupos Azure Active directory.
Se ha consultado el apartado [3.1.1 Identificación] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].</td><td>Aplica:
☐ Si ☐ No

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

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 de acceso siguiendo los apartados 3.1.2.4. Acceso local” y “3.1.2.5</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 de Administrador y usuario de clúster, almacenamiento y redes.</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) en el Tenant.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.5	**Mecanismo de autenticación**		
	Se ha creado una directiva Multi-Factor Authentication para los administradores.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: Si No	**Observaciones:**

		☐ ☐	
op.acc.6	**Acceso local**		
	Se ha configurado acceso condicional. Atendiendo una dirección IP origen/dispositivos entre otros.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.acc.6	**Acceso remoto**		
	Se habilito la directiva de acceso condicional delimitando zonas geográficas y rangos de IPS para los accesos remotos.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas:	**Observaciones:**

		☐ Si ☐ No	
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.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
op.exp.10	**Protección de los registros de actividad**		
	Se ha habilitado el registro de actividad de los usuarios. *Consultar el apartado [3.1.2.1 Registro de actividad de los usuarios] de la guía [CCN-STIC-884A – Guía de configuración segura de Azure].*	**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.cont.2	**Plan de continuidad**		
	Se ha configurado Azure Site Recovery replicando las maquinas virtuales y base de datos para poder crear un plan de recuperacion.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No

		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.cont.3	**Pruebas periódicas**		
	Para las maquinas virtuales se ha realizado una conmutacion por error.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.mon.1	**Detección de intrusión**		
	Se ha configurado *Azure monitor* y *Azure Security Center* siguiendo las recomendaciones de la guia *CCN-STIC-884A Configuración segura para*	**Aplica:** Si No	**Cumple:** Si No

	Azure, apartado. [3.1.6 Monitorización del sistema]	☐ ☐	☐ ☐
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Op.mon.2	**Sistema de métricas**		
	Se ha configurado Azure monitor aplicando los registros populares y el despliegue de Network Watcher.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.com.1	**Perímetro seguro**		
	Se ha configurado el despliegue de NSG / Azure Firewall aplicando las	**Aplica:**	**Cumple:**

	reglas recomendadas para Kubernetes.	☐ Si ☐ No	☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.com.1	**Perímetro seguro**		
	Se ha configurado la pasarela de aplicaciones.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.com.2	**Protección de la confidencialidad**		

	Se ha desplegado el servicios de VPN en alta disponibilidad conectada a la vnet de administración.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.com.3	**Protección de la autenticidad y de la integridad**		
	Para cubrir esta medida es necesario que se apliquen los servicios de: ***Azure Security Center*** ***Azure Multi-Factor Authentication*** ***Azure DDoS Protection***	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**

<table>
<tr><td>Mp.com.4</td><td colspan="3">Segregación de redes</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Se ha configurador las recomendaciones del apartado 3.2.1.1.</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>Mp.info.2</td><td colspan="3">Calificación de la información</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Se ha configurado las Etiquetas de azure en los servicios instalado.</td><td>Aplica:

☐ Si ☐ No</td><td>Cumple:

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

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

Mp.info.3	**Cifrado**		
	Se ha configurado el cifrado para los nodos del clúster.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**
Mp.info.9	**Copias de seguridad (backup)**		
	Se ha configurado un plan de backup para los nodos del clúster de Kubernetes.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: Si No	**Observaciones:**

		☐ ☐	
Mp.s.8	**Protección frente a la denegación de servicio**		
	Se ha configurado DDOS y se han habilitado en todas las VNET.	**Aplica:** ☐ Si ☐ No	**Cumple:** ☐ Si ☐ No
		Evidencias Recogidas: ☐ Si ☐ No	**Observaciones:**