CCN
centro criptológico nacional

ICT Security Guide
CCN-STIC 884B

Secure Configuration Guide for Kubernetes Services

JANUARY 2020

MINISTERIO DE DEFENSA

Edit:

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
2020.09.23 16:06:34 +02'00'

National Cryptologic Centre, 2020

NIPO: 083-20-196-0

Date of Edition: january 2020

Plain Concepts has participated in the creation and modification of this document and its annexes. Sidertia Solutions S.L. has participated in the revision of this guide.

FOREWORD

The current national and international scenario is dominated by developments in Information and Communication Technologies (ICT) and by risks emerging from their use. The Administration is fully aware of this scenario and it is necessary for this body to develop, acquire, conserve and secure use of ICTs to guarantee that its services run effectively for the citizen's and the country's best interests.

Working from the Centre's knowledge and experience on threats and vulnerabilities in terms of emerging risks, Law 11/2002, dated 6th May, regulating the National Intelligence Centre, entrusts the National Intelligence Centre the functions related to information technology security, according to the Article 4.e), and to the protection of classified information, according to the Article 4.f). It also gives, through the Article 9.2.f), its Secretary of State-Director the responsibility of managing the National Cryptologic Centre.

One of the most outstanding functions that it assigns to it, in Royal Decree 421/2004, dated 12th March, regulating the National Cryptologic Centre is to draw up and disseminate standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technologies.

Royal Decree 3/2010, dated 8th January, develops the National Security Framework (hereinafter called ENS) in the field of Electronic Administration which is also referred in the second section of Article 156 of Law 40/2015, dated 1st October, of the Public Sector Legal System. The National Security Framework establishes the security policy, in matters of use of electronic means, which ensures the protection of information.

Indeed, Royal Decree 3/2010, dated 8th January, updated by Royal Decree 951/2015, dated 23rd October, sets the basic principles and minimum requirements as well as any protection measures to be introduced in Administration systems. In article 29, it authorises the CCN to develop CIS guidelines to ease the fulfilment of these minimum requirements.

The CCN-STIC documents series was drawn up to comply with this function and the ENS, aware of the importance of establishing a frame of reference on this matter that can be used as support so that Administration staff can carry out their difficult and occasionally thankless task of providing security for ICT systems within their responsibility.

July 2019

Felix Sanz Roldan
Secretary of State
Director of the National Cryptologic Centre

INDEX

1. AZURE KUBERNETES SERVICES SECURE CONFIGURATION GUIDE 6
1.1 DESCRIPTION OF THE USE OF THIS GUIDE 6
1.2 SERVICE DEFINITION 6
1.3 PREREQUISITES FOR DEPLOYMENT 6
1.3.1 WINDOWS OPERATING SYSTEM 6
1.3.2 LINUX OPERATING SYSTEM 7
2. DEPLOYMENT OF AZURE KUBERNETES SERVICES 7
2.1 AKS CLUSTER SETTINGS 12
2.1.1 CLUSTER NODE SCALING. 12
2.1.1.1 FROM THE PORTAL OF AZURE 12
2.1.1.2 FROM POWERSHELL 13
2.1.2 UPDATE CLUSTER 14
2.1.2.1 FROM THE PORTAL OF AZURE 14
2.1.2.2 UPDATE CLUSTER FROM POWERSHELL 15
3. CONFIGURATION OF AZURE KUBERNETES SERVICES 15
3.1 OPERATING FRAMEWORK 15
3.1.1 PLANNING 15
3.1.1.1 SECURITY ARCHITECTURE 15
3.1.2 ACCESS CONTROL 16
3.1.2.1 IDENTIFICATION 16
3.1.2.2 SEGREGATION OF FUNCTIONS AND TASKS 17
3.1.2.3 AUTHENTICATION MECHANISMS 18
3.1.2.4 LOCAL ACCESS (LOCAL LOGON) 20
3.1.2.5 REMOTE ACCESS (REMOTE LOGIN) 20
3.1.3 EXPLOITATION 20
3.1.3.1 RECORDING USER ACTIVITY 20
3.1.3.2 PROTECTION OF CRYPTOGRAPHIC KEYS 23
3.1.4 CONTINUITY OF SERVICE 24
3.1.4.1 CONTINUITY PLAN 24
3.1.5 SYSTEM MONITORING 25

3.1.5.1 INTRUSION DETECTION 25
3.1.5.2 METRIC SYSTEM 25
3.2 PROTECTIVE MEASURES 27
3.2.1 PROTECTION OF COMMUNICATIONS 27
3.2.1.1 NETWORK SEGREGATION 27
3.2.1.2 SECURE PERIMETER 29
3.2.2 PROTECTION OF INFORMATION 34
3.2.2.1 RATING OF INFORMATION 34
3.2.2.2 BACKUP 34
4. GLOSSARY AND ABBREVIATIONS 34
4.1 GLOSSARY AND ABBREVIATIONS 34
5. SUMMARY TABLE OF SECURITY MEASURES 36

1. Azure Kubernetes Services Secure Configuration Guide

1.1 DESCRIPTION OF THE USE OF THIS GUIDE

The purpose of this guide is to indicate the steps to follow for the secure configuration of Kubernetes in compliance with the security requirements for the container orchestrator.

This guide will address the **essential configuration of kubernetes**, it should be consulted together with the CCN-STIC 884A - Azure Secure Configuration Guide.

1.2 SERVICE DEFINITION

Azure Kubernetes is a rapidly evolving platform for managing container-based applications and their associated network and storage components. The focus is on application workloads.

It provides a declarative approach to implementations, backed by a strong set of APIs for management operations.

1.3 PREREQUISITES FOR DEPLOYMENT

For the configuration of Kubernetes, through Powershell, the installation of the Azure CLI module is required.

Azure CLI is designed to facilitate the use of scripts, with query data, support for long term operations, etc. The installation can be done for several operating systems.

Minimum system requirements

Use a 64-bit version of Windows. Support for the 32-bit version of Microsoft Azure Active Directory Module for Windows PowerShell is obsolete since October 2014.

It is necessary to use the PowerShell version 5.1 or later. More information on platform prerequisites can be found at the following link:

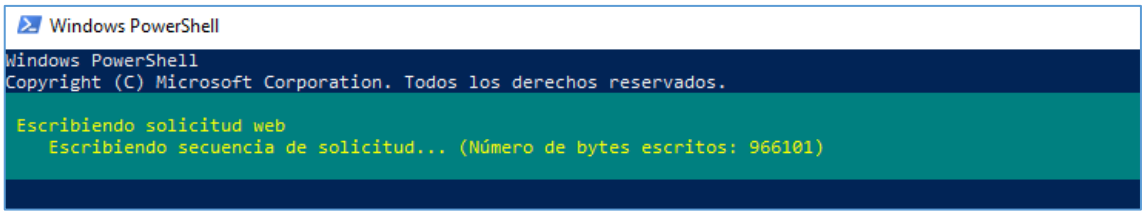
https://docs.microsoft.com/es-es/powershell/azure/azurerm/install-azurerm-ps?view=azurermps-6.13.0

1.3.1 Windows operating system

1. For Windows operating systems, open a PowerShell console and execute the following command:

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

Download and install the latest version of Azure's CLI for Windows If a version is already installed, update the existing version.



2. After the installation is completed, you need to reopen a PowerShell console to use the Azure CLI.
3. Execute the *az login* command to log in to Azure.

```
# az login
```

1.3.2 Linux Operating System

If you are executing a distribution with the **apt** package manager, such as Ubuntu or Debian, there is an x86_64 package available for Azure's CLI. This package has been tested and is compatible with:

Ubuntu trusty, xenial, bionic.

To install the **prerequisites,** execute the following steps:

1. Obtain the necessary packages for the installation process:

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

2. Download and install the Microsoft signature key:

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

3. Add the Azure CLI software repository:

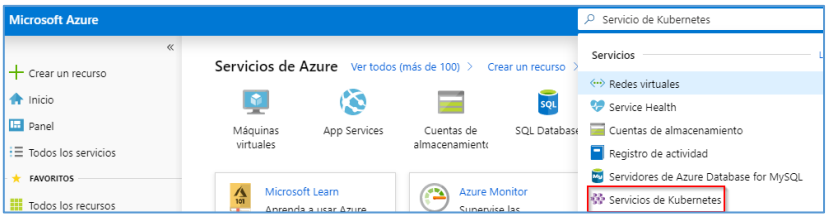
```
# AZ_REPO=$(lsb_release -cs)
# echo "deb [arch=amd64] https://packages.microsoft.com/repos/azure-cli/ $AZ_REPO main" \
#     sudo tee /etc/apt/sources.list.d/azure-cli.list
```

4. To update the information in the repository and install the azure-cli package:

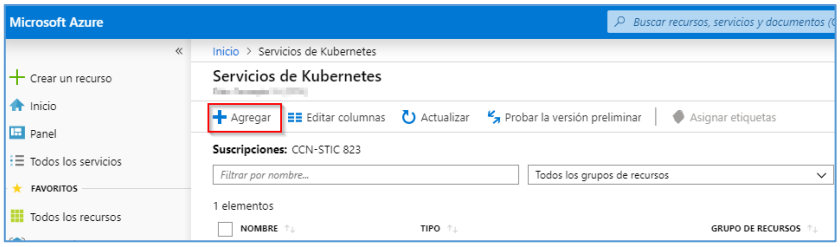
```
# sudo apt-get update
# sudo apt-get install azure-cli
```

2. DEPLOYMENT OF Azure Kubernetes Services

1. Search the Kubernetes Service from the Azure portal.



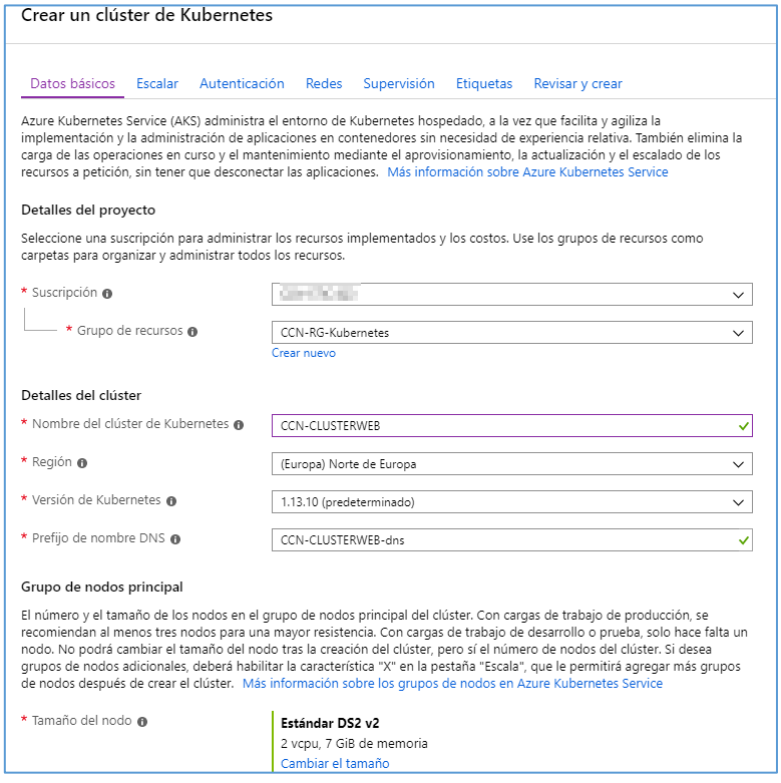
2. Click on [add].



In this first panel, the required fields for deployment are filled in.

Then each of them is detailed below.

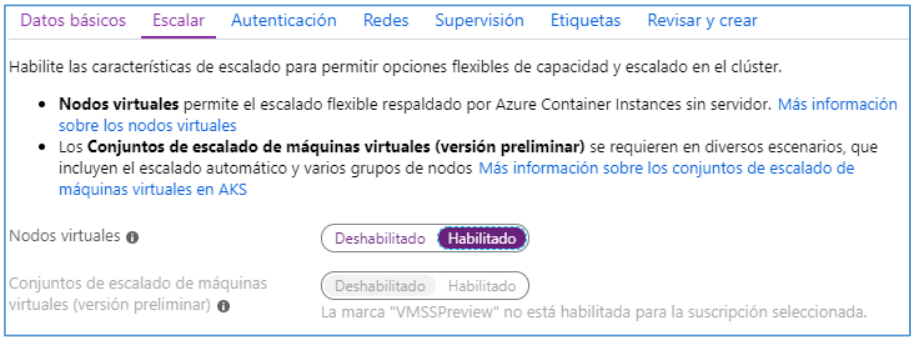
3. Click on [Basic Data].



- **Subscription:** Subscription where the service is created.
- **Resource Group:** You can choose an already created one or create a new one.
- **Kubernetes cluster name:** Kubernetes cluster name.
- **Region:** It appears USA by default, you must change it to North Europe.
- **Kubernetes version:** In this first installation it should be left by default.
- **DNS Name Prefix:** Prefix of the DNS name used with the API server FQDN.

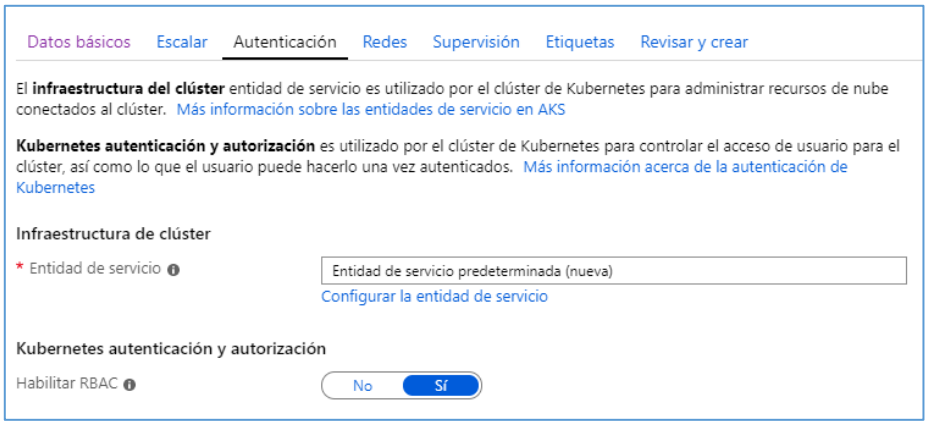
Finally, you can choose the number of nodes. When it's deployed by CNI networks the limit is set by the size of the subnet, as explained in section [3.2.1.1 Network Segregation] of this guide.

4. Click on the [Scale] tab and enable the virtual nodes. With this option, balancing and workloads can be quickly implemented in an Azure Kubernetes Service (AKS) cluster. It also has a fast supply of pods.



5. Click on [Authentication].

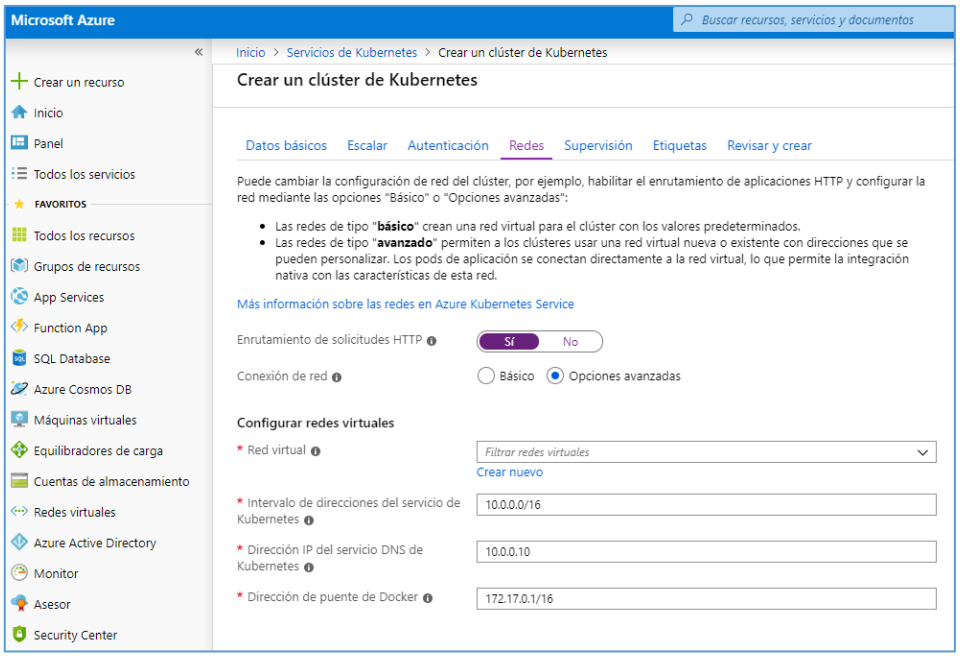
On the authentication tab, RBAC must be activated as we recommend this method in this guide when accessing the Kubernetes application.



Service Entity: A new one is created by default.

- Enable RBAC: It is recommended to enable RBAC since we mention the configuration of this guide in the section [3.1.2.2 Segregation of functions and tasks]

6. Then, on the [networks] tab, perform the following steps:



- **HTTP Request Routing:** The HTTP Application Routing Plug-in is designed to allow you to quickly create an input controller and access your applications. This plug-in is not recommended for the use in production. **It should be left disabled.**
  For production environments, the use of an HTTPS input controller is recommended. For more information: https://docs.microsoft.com/es-es/azure/aks/ingress-tls

  Network connection: Click on advanced options. This will create a CNI network for the Kubernetes cluster. This is the recommended option.

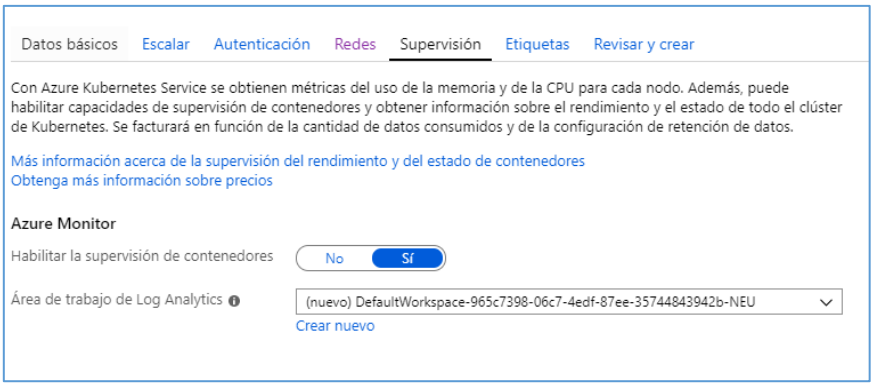
  Note: *For more information on networking in Azure, see section [3.2.1.1 Network Segregation] of the [CCN-STIC-884A - Azure Secure Configuration Guide].*

  Virtual Networking Configuration

  Follow the next steps:

  - **Virtual Network:** Create a new virtual network for this deployment.
  - **Kubernetes service address range:** Assign the IP addresses of the service's cluster. It should not overlap with any subnet IP range.
  - **Kubernetes DNS Service IP Address:** An IP address assigned to the Kubernetes DNS service. It must be in the address range of the Kubernetes service.
  - **Docker Bridge Address:** An IP address and netmask assigned to the Docker Bridge It must not be in a subnet IP range or in the Kubernetes service address range.

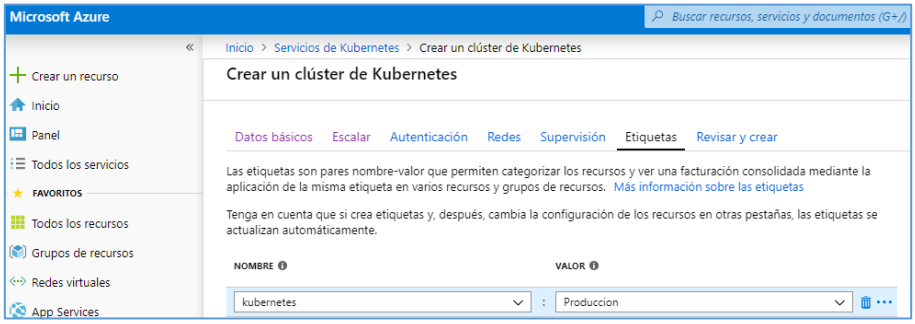
7. Then click on the [monitoring] tab.



It is recommended to enable **Azure Monitor** for containers, since it is a tool designed to monitor the performance of the workloads of the containers implemented in Azure.

Container monitoring is critical, especially when executing a production cluster, at scale, with multiple applications. More information can be found in the section [3.1.5 System Monitoring] this guide.

8. Then click on the [Labels] tab.



Azure's resources must be tagged to provide metadata and to organize them in a logical way. Each tag consists of a name and a value.

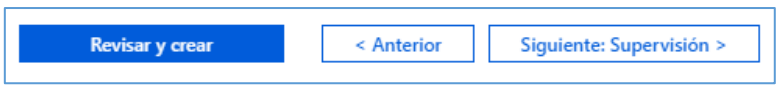
For example, the name "Kubernetes" and the value "Production" can be applied to all the resources in production.

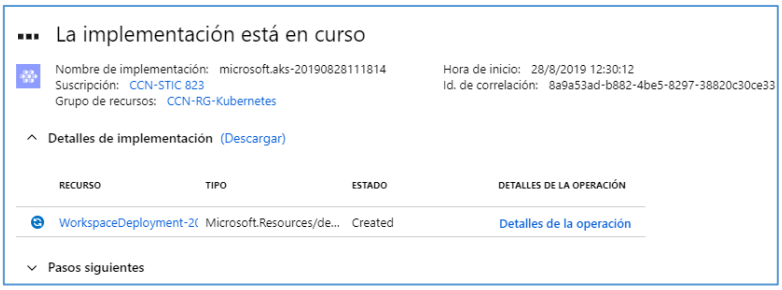
After applying the tags, all the subscription resources with that name and tag value can be retrieved.

This approach can be useful if resources need to be organized for management.

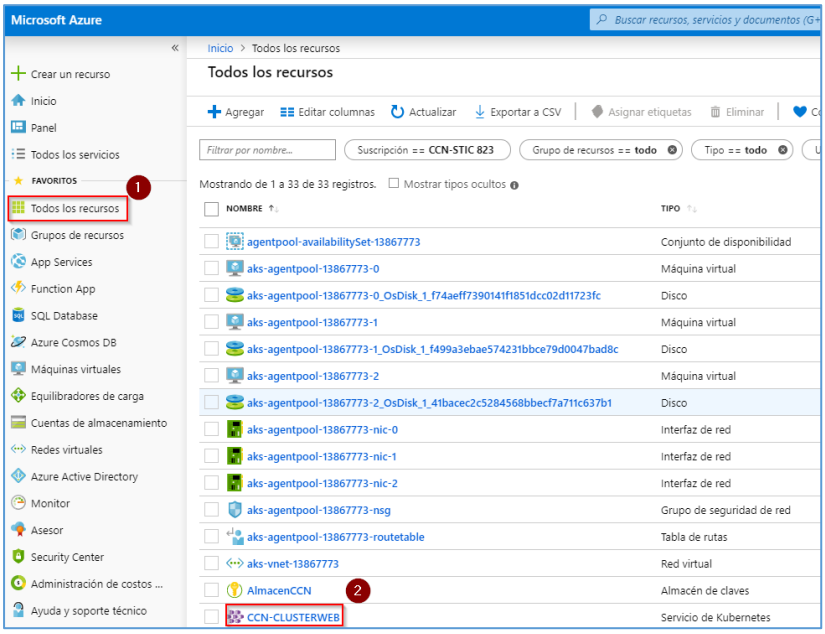
Note: *For more information on Azure labels, see section [3.2.2.1 Rating] of the [CCN-STIC-884A - Azure Secure Configuration Guide].*

9. Finally, click on [review and create].





10. To check the new cluster from the Azure's portal, click on [all resources] to find the new Kubernetes cluster.



2.1 AKS cluster settings

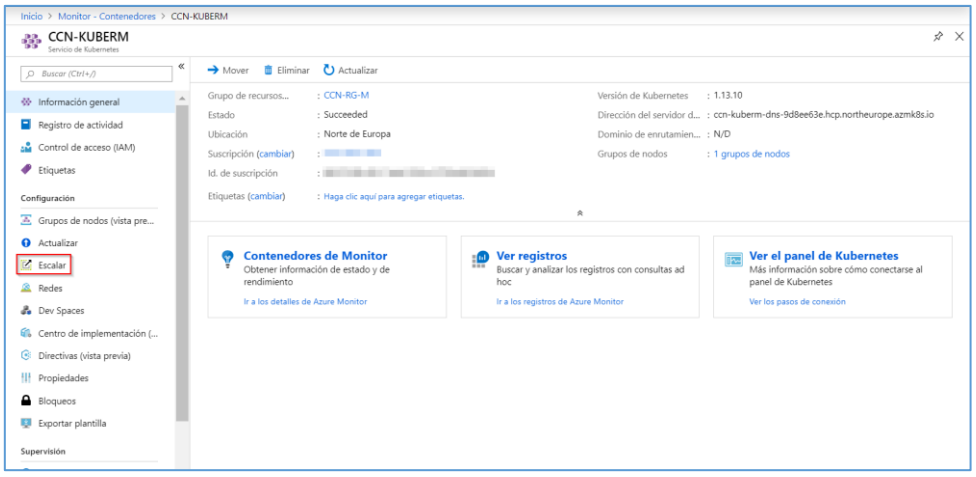
2.1.1 Cluster node scaling.

2.1.1.1 From the portal of Azure

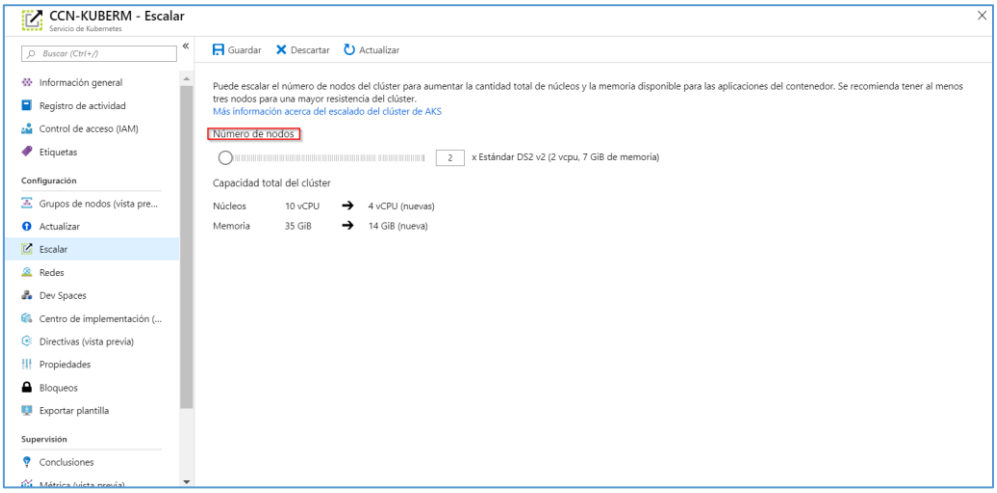
Once the Kubernetes service has been deployed, the nodes that form the cluster can be expanded if necessary.

To do this, the following steps are taken:

1. Search Azure Kubernetes Service
2. Click on the desired cluster and click on the [Scale] menu.



3. Add as many nodes as necessary. The size of the cluster before updating and the resources to be added are also shown.



2.1.1.2 From Powershell

To scale the nodes via powershell, perform the following steps:

1. Get the cluster information.

```
# az aks show --resource-group Name_Resource_Group --name Name_Service_AKS --query agentPoolProfiles
```

All the cluster information is displayed, the count field indicates the number of nodes in the cluster.

```
{
  "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/CCN-RG-M-vnet/subnets/default"
}
```

2. The cluster is scaled to the number of nodes required. The number may be higher or lower. In the example we will reduce it from 5 to 3 nodes.

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

3. Verify that the cluster now has three nodes, using the same command as in step 1.

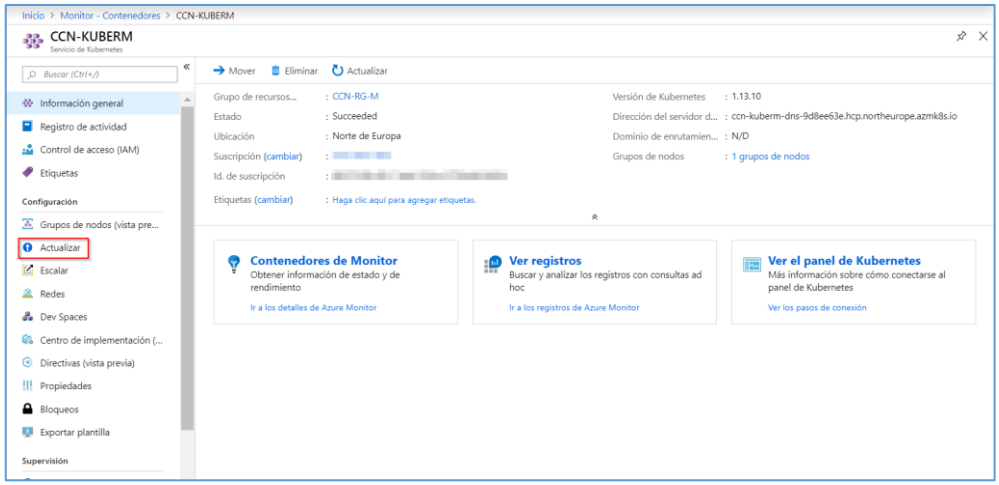

```
{
  "availabilityZones": null,
  "count": 3,
  "enableAutoScaling": null,
  "maxCount": null,
  "maxPods": 30,
  "minCount": null,
  "name": "agentpool",
  "orchestratorVersion": "1.14.6",
  "osDiskSizeGb": 100,
  "osType": "Linux",
  "provisioningState": "Succeeded",
  "type": "VirtualMachineScaleSets",
  "vmSize": "Standard_DS2_v2",
  "vnetSubnetId": "/subscriptions/[redacted]/resourceGroups/CCN-RG-M/providers/Microsoft.Network/virtualNetworks
N-RG-M-vnet/subnets/default"
}
```


2.1.2 Update Cluster

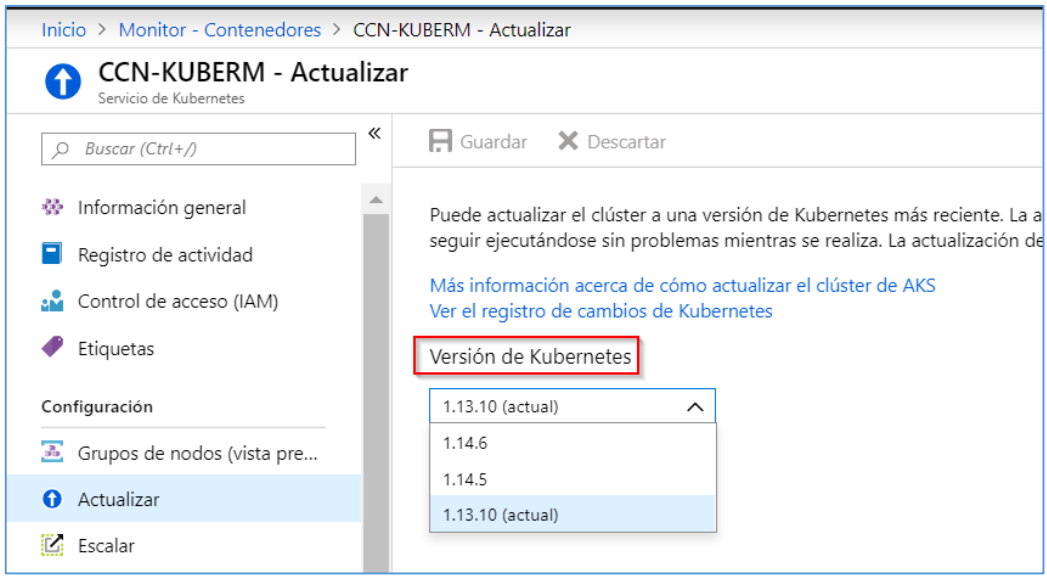
2.1.2.1 From the portal of Azure

To upgrade the AKS cluster to a more recent version, the following steps must be taken:

1. Search Azure Kubernetes Service
2. Select the desired cluster and click on the [Update] menu.



3. Select the version of AKS to be implemented in the cluster.



Note: *This operation takes time depending on the number of nodes in the cluster. It can take up to 10 minutes per node.*

2.1.2.2 Update cluster from Powershell

To update the cluster from Powershell perform the following steps:

1. Check the cluster updates, it will return the output in table format.

```
# az aks get-upgrades --resource-group Recursos_Grupo_Number --name AKS_Servicio_Number
--output table
```

Note: *If no update is available, it will display the following error: "ERROR: Table output unavailable. Use the --query option to specify an appropriate query. Use --debug for more info. ”*

2. The cluster is updated with the desired version, which is shown with the previous step.

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

3. Check that the cluster has been updated.

```
#    az aks show --resource-group Name_Resource-group --name Name_Service_AKS --output table
```

3. CONFIGURATION OF Azure Kubernetes Services

3.1 OPERATING FRAMEWORK

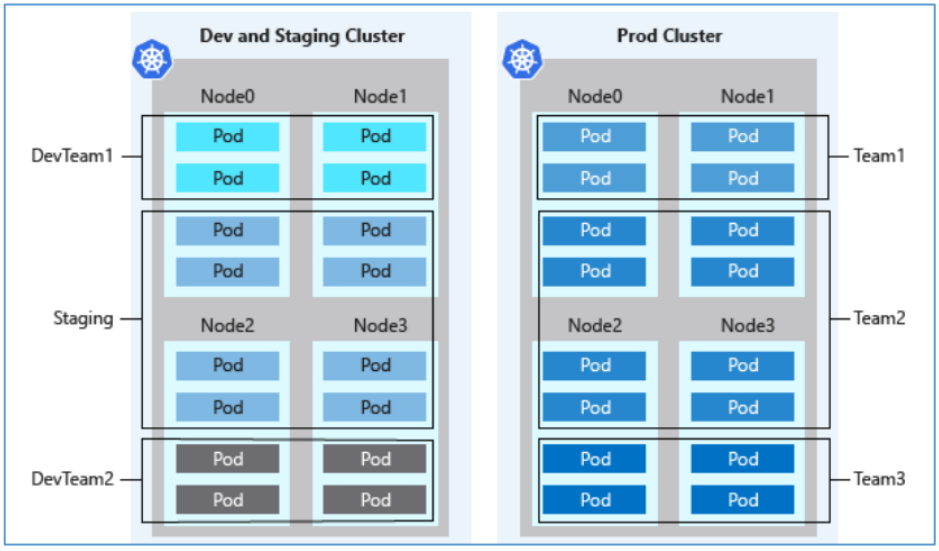
3.1.1 Planning

3.1.1.1 Security architecture

Kubernetes' environments, both at AKS and elsewhere, are not completely secure from the use of multiple hostile tenants. In a multi-tenant environment, several tenants work on a common shared infrastructure. As a result, if all tenants cannot be trusted, you should make additional planning to prevent one tenant from

affecting the security and service of another. Using additional security features, such as the pod security policy, and more specific role-based access controls (RBAC) can make security vulnerabilities more difficult. However, for security to be effective when executing hostile multi-tenant workloads, the hypervisor is the only level of security you should rely on. Kubernetes' security domain becomes the entire cluster, not a specific node.

For these types of hostile multi-tenant workloads, you should use clusters that are physically isolated.



Physical isolation is recommended for each separate piece of equipment. In this isolation model, equipment or workloads are assigned to their own AKS cluster. It entails additional financial and management burden due to the maintenance that must be performed on each node of the clusters.

3.1.2 Access Control

3.1.2.1 Identification

Azure AD provides cloud-based identity management and allows a single identity to be used across all Tenant and access applications in Azure.

Note: *For more information on Azure identities, see section [3.1.1 Identification] of the [CCN-STIC-884A - Azure Secure Configuration Guide].*

As a recommendation, an Azure Kubernetes service cluster manager RBAC role should be assigned to a group already defined for API managers.

Then, from the Azure CLI console follow these instructions:

1. Obtain the Kubernetes cluster resource ID. To do this, use the *Azure CLI* console execute.

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

2. Obtain the ID of the group to which the Cluster Manager role is assigned.

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

3. Finally, assign the role to the group.

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

Note: *For more information on Azure roles, see section [3.1.1.1 Access Requirements] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.2.2 Segregation of functions and tasks

Azure Kubernetes Service (AKS) can be configured to use Azure Active Directory (AD) for user authentication. In this configuration, you are logged into an AKS cluster using an Azure AD authentication token. Kubernetes' role-based access control (RBAC) can also be configured to limit access to cluster resources based on the user identity or the group membership.

Customized roles must be created for the management and administration of the Kubernetes cluster.

There are different roles to be employed.

- **Kubernetes Cluster Manager Role**

Used to manage the Kubernetes cluster, it consists of the following permission:

Microsoft.ContainerService/managedClusters/listClusterAdminCredential/action

- **Kubernetes Cluster User Role**

Used for reading permissions on the Kubernetes cluster, it consists of the following permission:

Microsoft.ContainerService/managedClusters/listClusterUserCredential/action

- **Networks**

To use advanced networks where the virtual network and subnet or public IP addresses are in another resource group. Assign the following role permissions:

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

Or, assign the integrated role of the Network Contributor in the subnet within the virtual network.

- **Storage**

It may be necessary to access the existing disk resources in another resource group. Assign the following role permissions:

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write

Or, assign the integrated role Storage Account Contributor in the resource group.

Note: *Also, follow the link: https://docs.microsoft.com/es-es/azure/aks/operator-best-practices-cluster-security#app-armor where more protection recommendations such as AppArmor, seccomp (secure computing) and Pod Security Policies are added.*

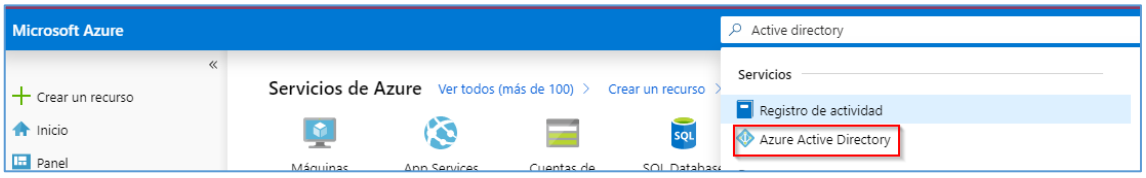
Note: *For more information on Azure roles, see section [3.1.1.1 Access Requirements] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.2.3 Authentication mechanisms

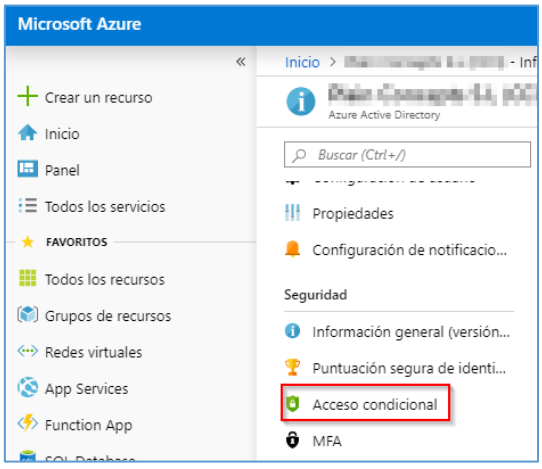
In the authentication mechanisms it is recommended to create a new political condition that will be integrated in the authentication mechanisms.

To do this, the following instructions must be carried out.

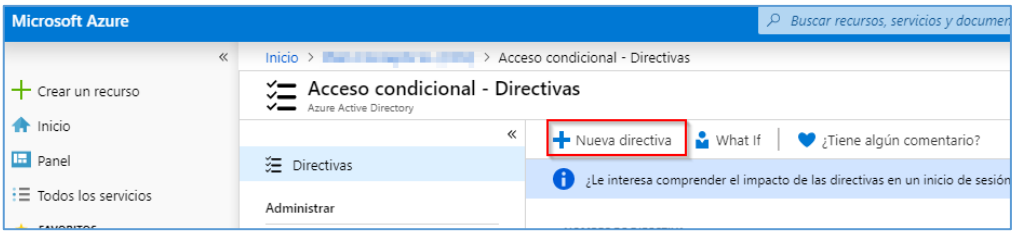
1. In the search engine of the Azure's portal search for Active Directory.



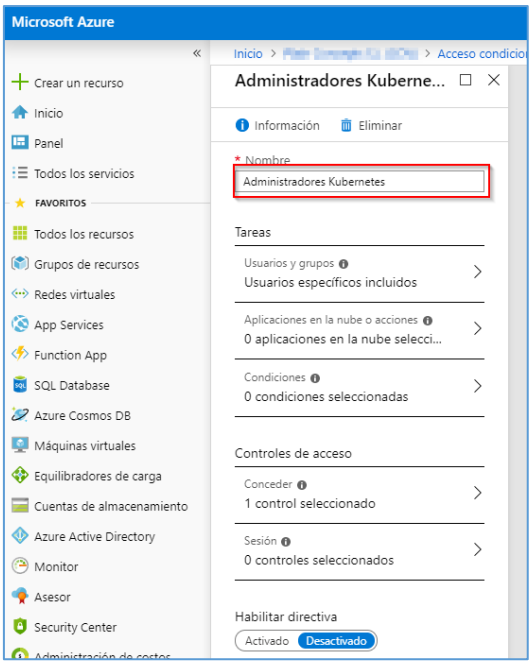
2. Next, [conditional access].



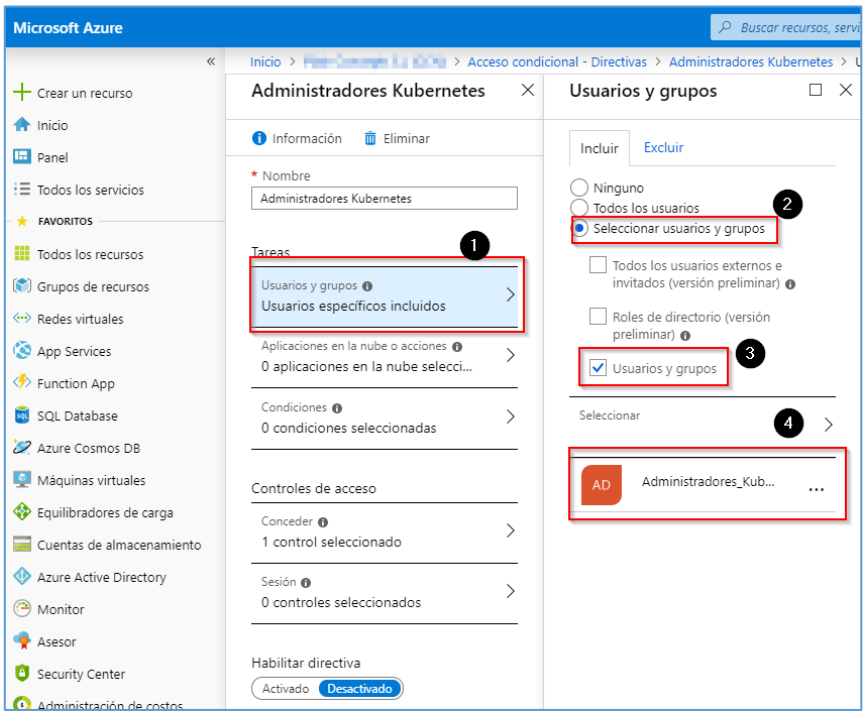
3. Click on [new policy].



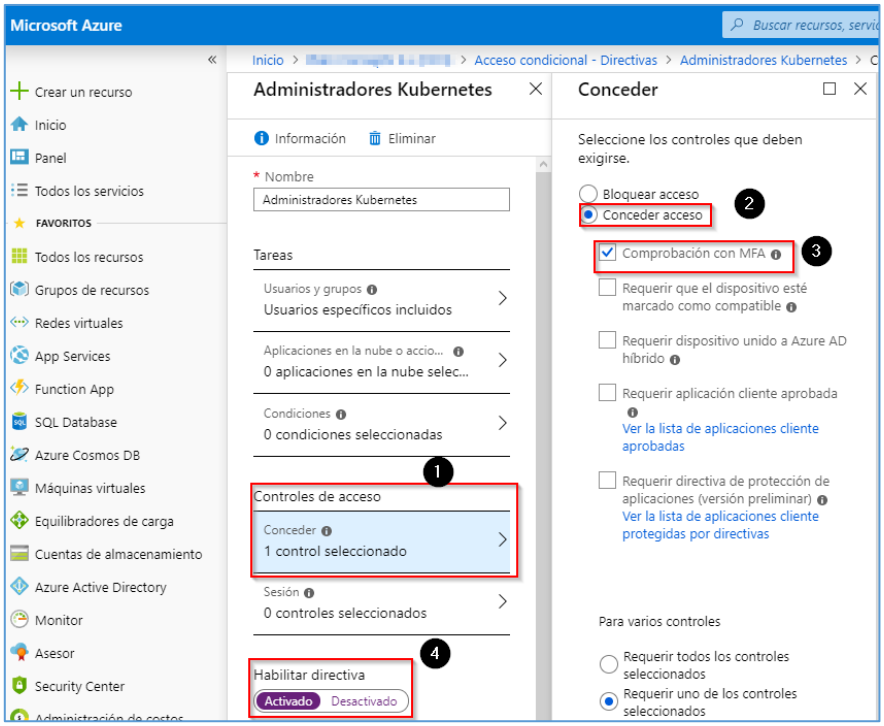
4. Next, a name must be defined for the policy.



5. Then choose the administrators group to which this authentication method applies.



6. Click on [Access Controls], then [grant access/MFA checks].



7. Enable the policy and click on [create].

At the end you will have created the new policy that will apply multi-factor authentication for Kubernetes administrators.

3.1.2.4 Local access (local logon)

For local access, a conditional access policy is recommended. Where you can define which ranges of IPs have access to your applications as from the geographic location from which they connect.

Note: *For more information on conditional access in Azure see section [3.1.1.1 Access Requirements] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.2.5 Remote access (remote login)

Kubernetes is a *cloud* solution accessible by the end user through the Internet.

It is recommended for all physical devices to be attached Azure AD, MFA.

Note: *For more information on Azure MFA, please refer to section [3.1.1.4 Authentication Mechanisms] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.3 Exploitation

3.1.3.1 Recording user activity

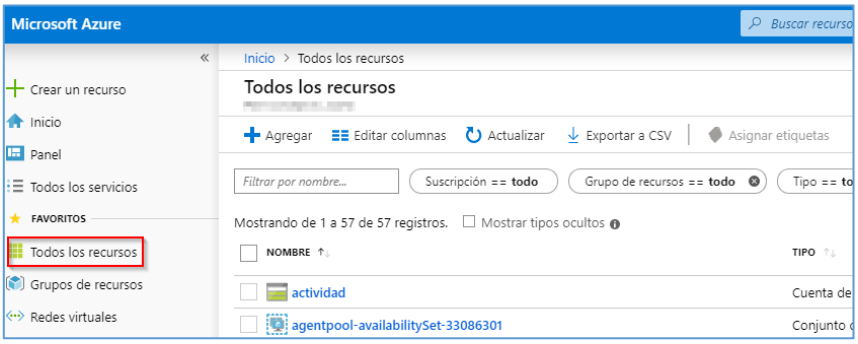
Using the activity logs, you can determine:

- What operations were performed on the resources in the subscription.
- Who initiated the operation.

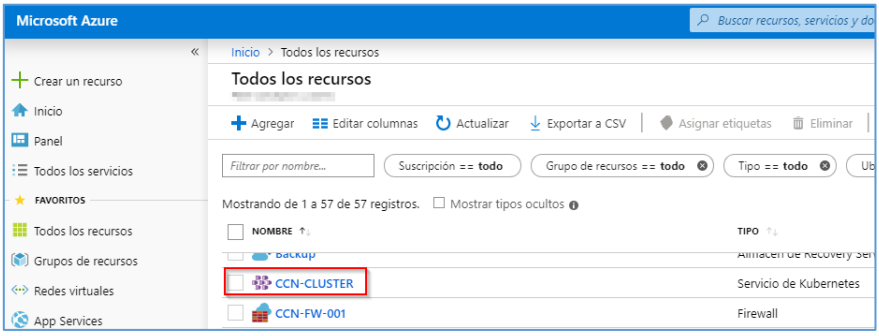
- When the operation took place.
- The state of the operation.
- The values of other properties that could help in the investigation of the operation.

To do this, follow the steps below:

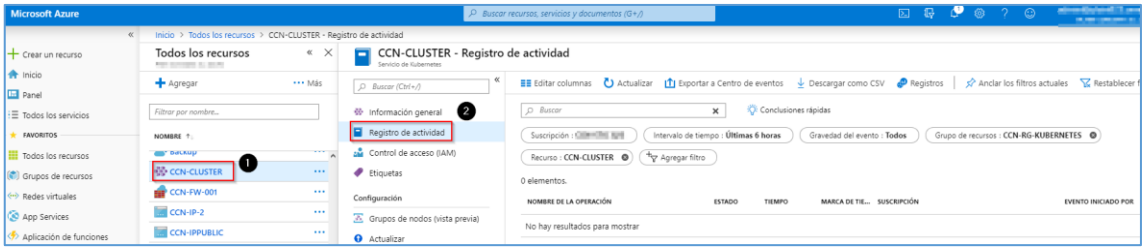
1. From the Azure's portal, click on [all resources].



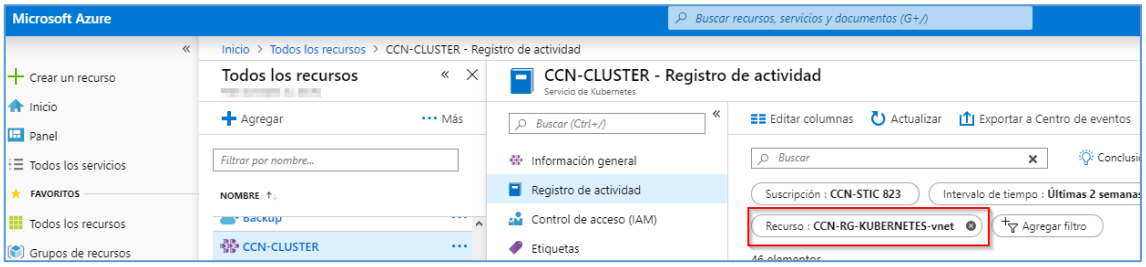
2. The Kubernetes' cluster must be found.



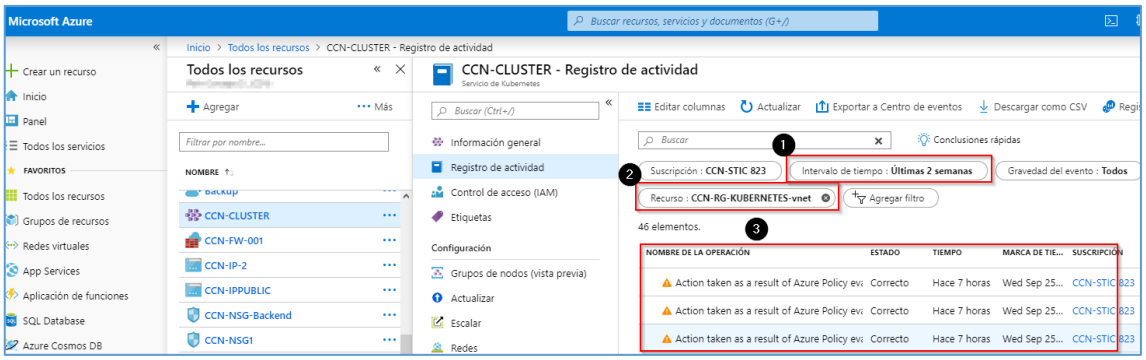
3. From the Kubernetes' cluster, click on [Activity Log].



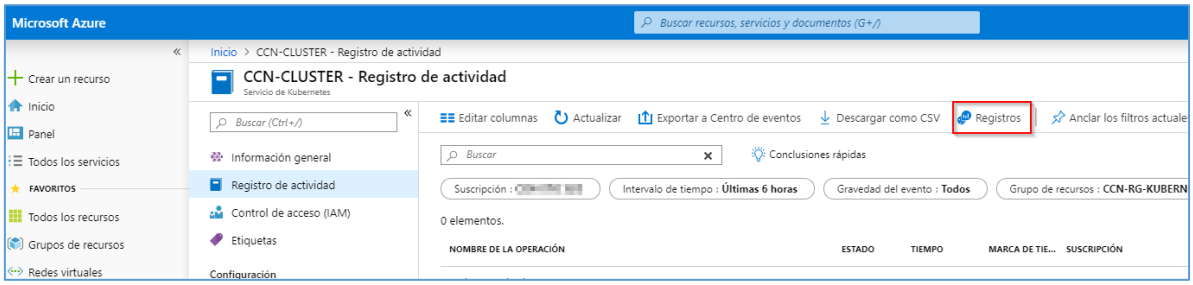
4. From this panel you can filter the logs. For example, in [Resource] select the cluster.



5. The search results are displayed.

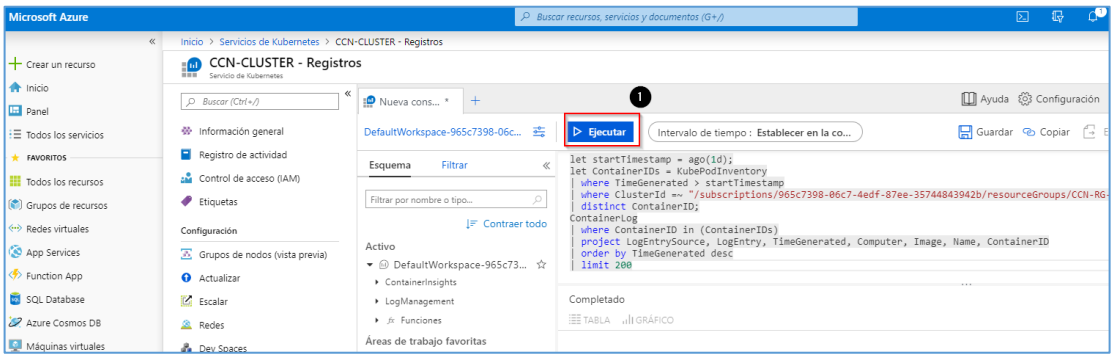


6. In addition, a search can be customized from the Workspace. To do so, click on [log].



7. You can execute the following query to see all users who performed an action on Kubernetes.
8. Copy the content and click on execute.

```
#   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
```



Note: *For more information about the user activity log in Azure. See section [3.1.2.1 User Activity Log] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.3.2 Protection of cryptographic keys

To improve security and compliance of virtual machines, virtual disks must be encrypted in Azure. Disks are encrypted using cryptographic keys that are protected in Azure Key Vault. This can be applied to Kubernetes virtual disks as well as any other *Tenant disk*.

In this first step, an Azure Key Vault must be created to store the cryptographic keys. In Azure Key Vault you can store keys, secrets or passwords that allow the secure deployment in applications and services.

For virtual disk encryption, create an Azure Key Vault storage to store a cryptographic key that is used to encrypt or decrypt the virtual disks.

1. From the PowerShell module create a cryptographic key in Azure Key Vault.

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

The Azure Key Vault containing the cryptographic keys and associated processing resources, such as storage and the virtual machine itself, must be in the same region.

2. An Azure Key Vault instance must be created with New-AzKeyVault and enable Key Vault for use it with the disk encryption.

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

3. You must have access to request the cryptographic keys when the virtual machine boots up to decrypt the virtual disks. To do this, create a cryptographic key in the Key Vault instance with Add-AzureKeyVaultKey.

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

Encryption of a virtual machine

1. The virtual machine must be encrypted with Set-AzVMDiskEncryptionExtension through the Azure Key Vault.

PowerShell Console

```
#   $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
```

Note: *The virtual machine is restarted during the process.*

2. After the encryption process is completed and the virtual machine is restarted, check the status of the encryption with the following PowerShell command Get-AzVmDiskEncryptionStatus.

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

Note: *The same configuration can be applied on Linux servers. To do this, follow the steps in this link:*

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

Note: *For more information on Azure Key Vault see section [3.2.2.2 Encryption] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.4 Continuity of service

3.1.4.1 Continuity plan

As clusters in Azure Kubernetes Service (AKS) are managed, application uptime becomes important.

Kubernetes provides high availability by using several nodes in one availability set. But these multiple nodes do not protect the system from a regional error.

The application can be implemented in several AKS clusters in different regions.

There are two services:

- **Availability by AKS region:** You can choose regions near the users. AKS is continually expanding into new regions.
- **Azure Paired Regions:** For the geographical area, you can choose two regions that are paired with each other. Paired regions coordinate platform updates and prioritize recovery efforts when necessary.

Note: *For more information on the continuity plan, see section [3.1.4 Continuity Plan] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.5 System monitoring

3.1.5.1 Intrusion detection

To maintain the protected environment, suspicious users should be blocked from logging in. You need to create a new authentication policy.

Note: *For more information on Intrusion Detection see section [3.1.6.1 Intrusion Detection] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

3.1.5.2 Metric system

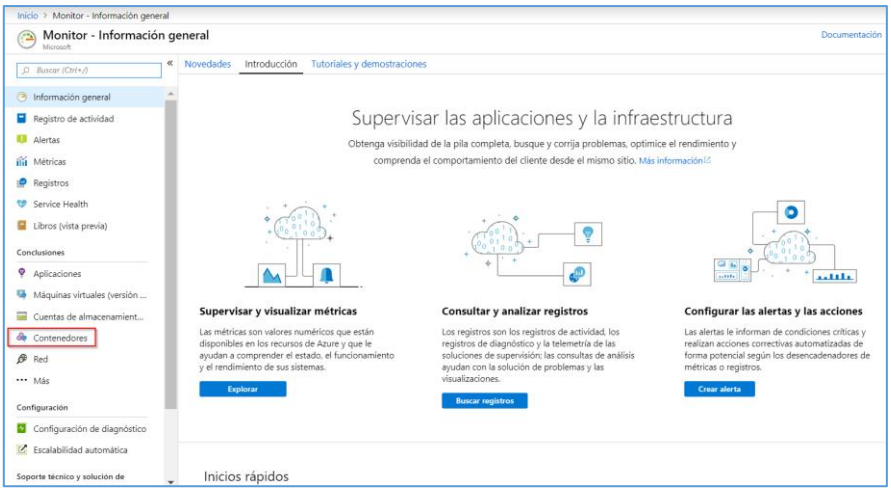
To obtain performance metrics and control of Kubernetes' containers, a new workspace must be created in Log Analytics.

The ability to monitor performance is based on a Log Analytics agent in containers for Linux, developed specifically for Azure Monitor. This specialized agent collects performance and event data from all the nodes in the cluster, and the agent is automatically implemented and logged in the Log Analytics workspace.

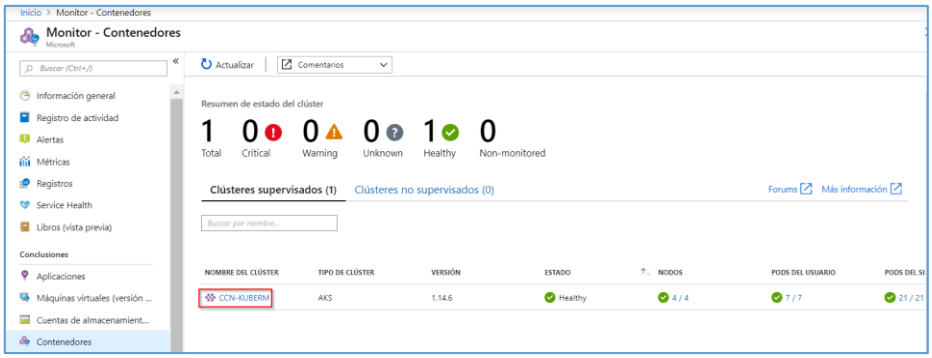
Note: *For more information on log analytics see section [3.1.2.2 Protection of Activity Records] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

To view Kubernetes' metrics follow the steps below:

1. From Azure's portal search engine search for Monitor.
2. Click on [Containers].

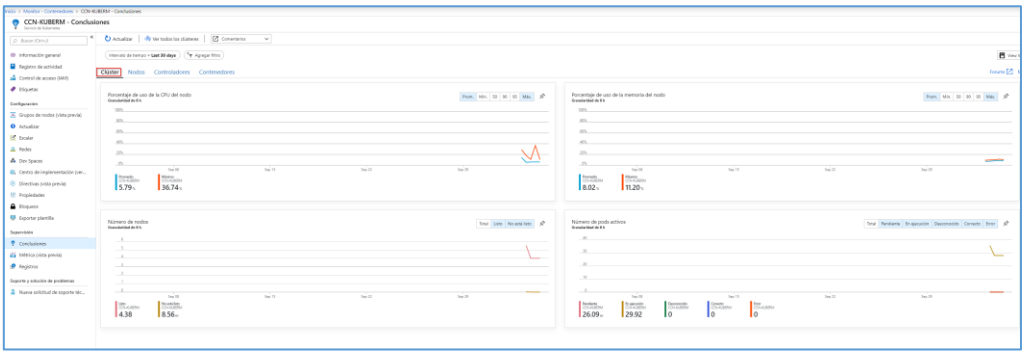


3. All the existing clusters are displayed with an overview of each one, for more information select the cluster to see its monitoring.

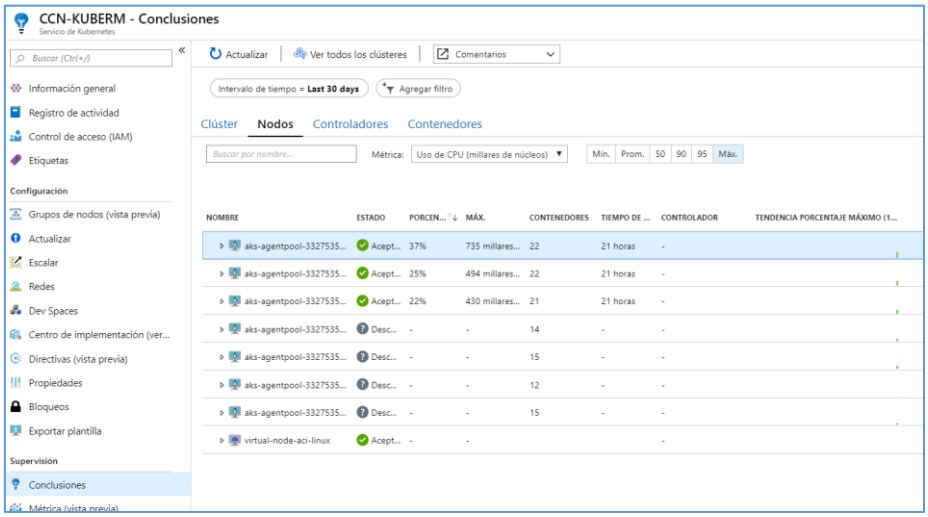


4. Once inside the cluster the metrics are divided into several fields:

   Cluster: General cluster metrics, such as CPU, RAM of the nodes, number of nodes in the cluster and number of active pods.

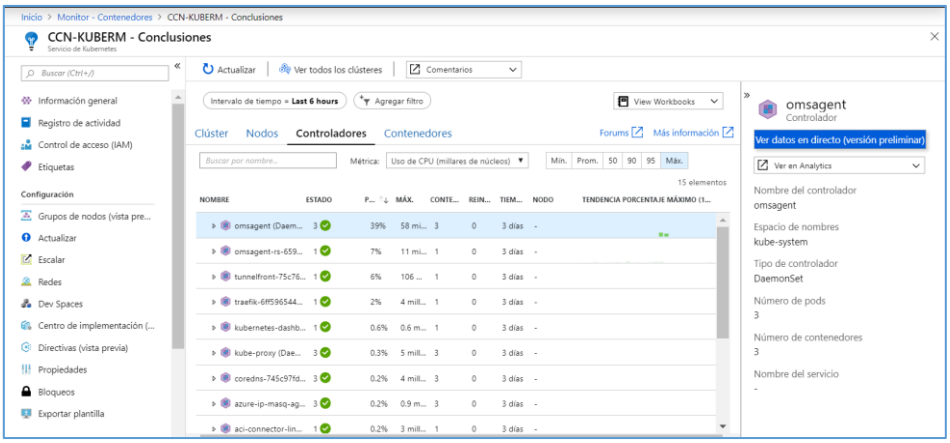


   Nodes: It shows metrics of each node and of the processes that are being executed. To display the processes of a node, you only have to click on the node you want to display.

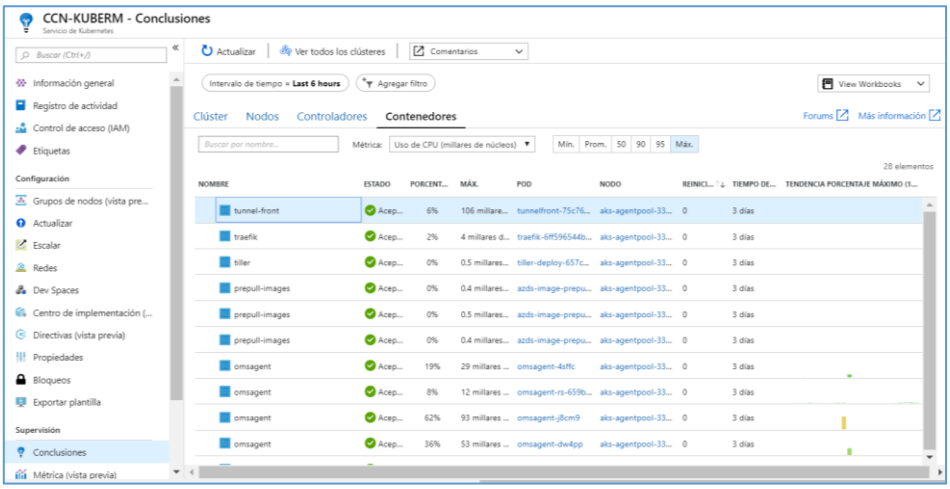


   Controllers: As with the nodes, you can see the metrics of the Kubernetes controllers.

   If you click on the button **View live data,** in case you are executing any operation, the information will be displayed immediately, in real time.



Containers: Shows which containers are executing, which container image they are executing and where the containers are executing.



3.2 PROTECTIVE MEASURES

3.2.1 Protection of communications

3.2.1.1 Network Segregation

With Azure Container Networking Interface (CNI) each pod gets an IP address from the subnet, being able to access it directly. In this way we avoid the translation of network addresses that is performed with classic networks.

This addressing must be unique and requires planification, as there is a possibility of running out of IP addresses as applications grow.

Requirements

- The virtual network of the cluster must allow outgoing connectivity to the Internet.
- You cannot create more than one cluster per subnet.
- Clusters **cannot** use address ranges **169.254.0.0/16, 172.31.0.0/16, 172.30.0.0/16, 192.0.2.0/24**

- The service entity used by the cluster must have network contributor permissions.

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

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

CNI network deployment

When deploying the network, the number of pods to be executed must be taken into account, as well as the number of nodes (maximum) that the cluster can have, since an IP address of the network is assigned to both the nodes and the pods.

The following parameters are required for deployment.

- Virtual Networking
- Subnet
- Kubernetes service address range: Set of IP addresses that Kubernetes assigns to internal services in the cluster.

  You mustn't:
  - Be within the IP address range of the cluster's virtual network.
  - Overlap with any other virtual network.
  - Overlay with no local IP address.
  - Be within the ranges 169.254.0.0/16, 172.30.0.0/16, 172.31.0.0/16 and 192.0.2.0/24

- Kubernetes DNS Service IP Address: The IP address of the cluster's DNS service. This address must be within the address range of the Kubernetes service. Do not use the first IP address in the address range. The first address of the subnet range is used for the address kubernetes.default.svc.cluster.local.
- Docker Bridge Address: The Docker bridge network address represents the default *docker0* bridge network address present in all Docker installations. While *docker0* bridge is not used by AKS clusters or the pods themselves, you must set this address to continue to support scenarios such as *docker build* within the AKS cluster.
  It is required to select a CIDR for the Docker bridge network address because otherwise Docker will pick a subnet automatically which could conflict with other CIDRs. You must pick an address space that does not collide with the rest of the CIDRs on your networks, including the cluster's service CIDR and pod CIDR.

Limitations

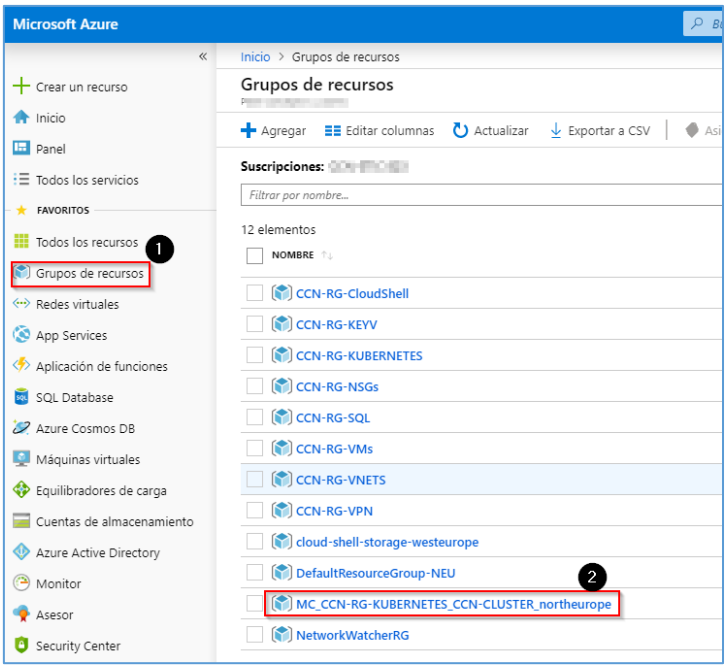
Azure Resource	Limit
Virtual Network	The size can be up to /8, limited to 65536 IP addresses.
Subnet	It must be large enough to accommodate nodes, pods and all Kubernetes and Azure resources that can be provisioned on the cluster, within the limits of the Virtual Network.
Kubernetes address range	This range must not be used by any network element in this virtual network or connected to it. The CIDR of the service address must be less than /12.
Kubernetes DNS service IP address	IP address of the Kubernetes service address range to be used in cluster service detection. Do not use the first IP address in the address range, such as .1. The first address of the subnet range is used for the address *kubernetes.default.svc.cluster.local*.
Docker's bridge address	The Docker bridge network address represents the default *docker0* bridge network address present in all Docker installations. While *docker0* bridge is not used by AKS clusters or the pods themselves, you must set this address to continue to support scenarios such as *docker build* within the AKS cluster.

3.2.1.2 Secure perimeter

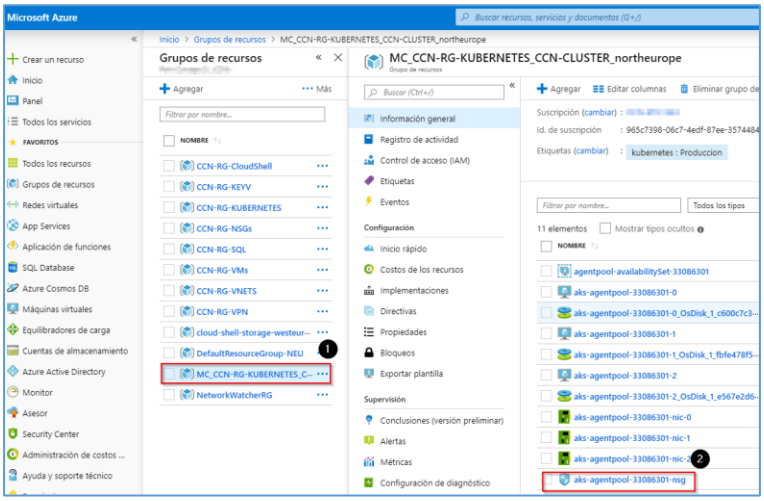
AKS clusters have unlimited outbound Internet access. This level of network access allows the nodes and services it executes to access external resources as needed. As a recommendation, outbound traffic should be restricted, access to a limited number of ports and addresses is necessary to keep the cluster in good condition.

Then perform the following steps.

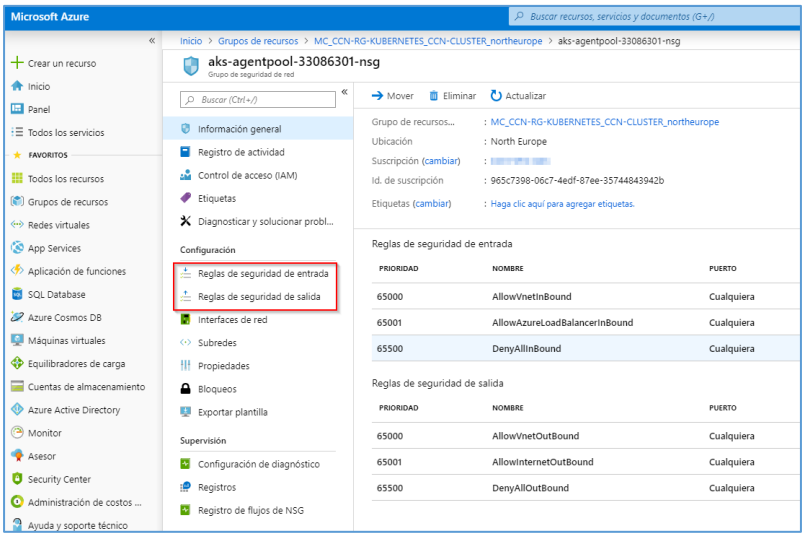
1. Click on [resource group] in the Azure's portal.



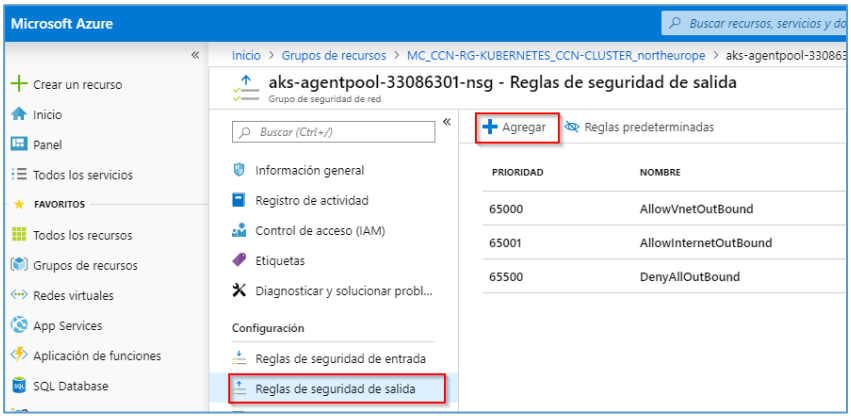
2. Click on the Kubernetes network security resources group.



3. Click on [Secure Exit rules].



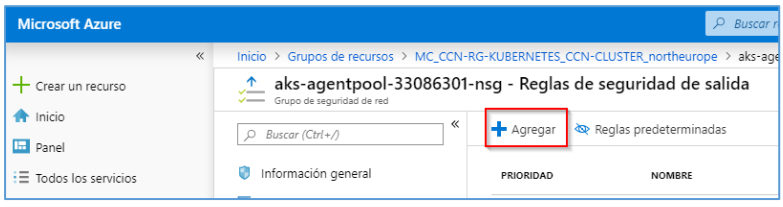
4. Click on [add].



Note: *Azure creates the rules 65000, 65501 and 65500 by default in each network security group*.

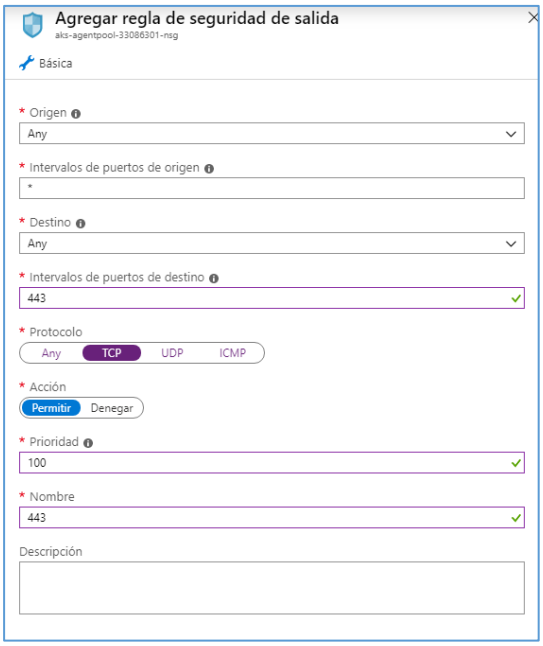
Then add the recommended output ports for Kubernetes.

5. Click on [add].

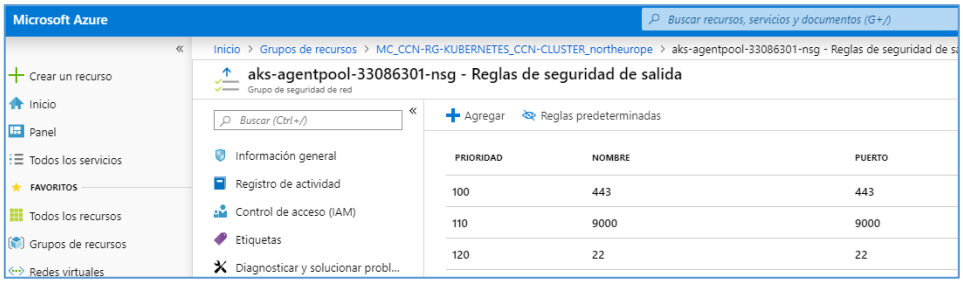


6. Add the following ports.

- TCP port 443
- TCP 9000 port and TCP 22 port for the pod at the front of the tunnel to communicate with the tunnel end on the API server.



At the end, the new rules will appear.



Note: *For more information on NSG rules see section [3.2.1.2 Secure Perimeter] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*

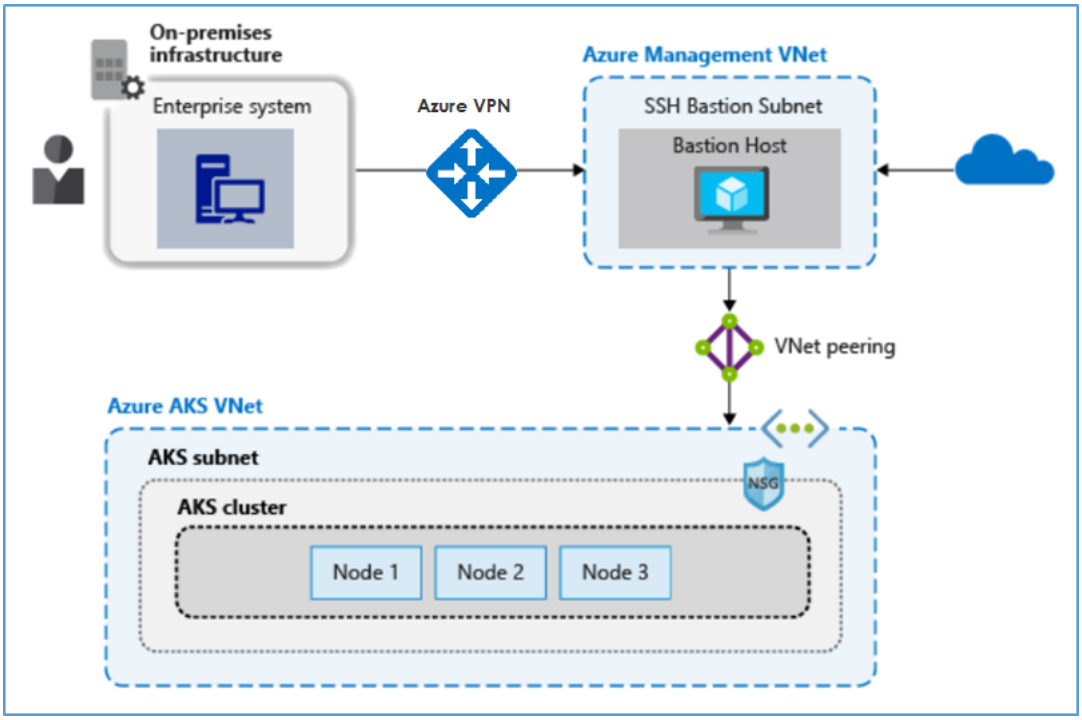
Application Gateway

For connection to kubernetes clusters it is recommended to not expose the connectivity of AKS nodes. To do this, it is recommended to create an application gateway from an administration network.

Most operations in AKS can be performed with Azure's management tools or using the Kubernetes API server.

The nodes would be connected to a private network and to connect to them or to perform maintenance tasks must be done from a jump host in a management network.

Here is a graph of the architecture:



At the same time, in order to connect to the administration network, it is advisable to create a **VPN** connection and control the access with network security groups (NSG).

Perform the following steps to configure the gateway (once the AKS cluster and the management network have been created):

1. Create the VPN with the management network.
2. Protect communications with a network security group.
3. Perform a peering between the administration network and the node network.

Note: *For more information on congifuring a network, see section [3.2.1.1 Network Segregation] of the [CCN-STIC-884A - Azure Secure Configuration Guide].*

Note: *For more information on network security groups, see section [3.2.1.2 Secure Perimeter] of the [CCN-STIC-884A - Azure Secure Configuration Guide].*

Note: *For more information on creating a VPN, see section [3.2.1.3 Protecting Privacy] in the [CCN-STIC-884A - Azure Secure Configuration Guide].*

Network Policies

By default, all the pods in an AKS cluster can send and receive traffic without limitations. To improve security, you can define rules that control the flow of traffic.

You can see the network policies in action by creating and expanding a policy that defines the traffic flow for:

- Deny all the traffic to the pod.
- Allow the traffic based on pod tags
- Allow the traffic by name space

It is recommended to follow the instructions on this link:

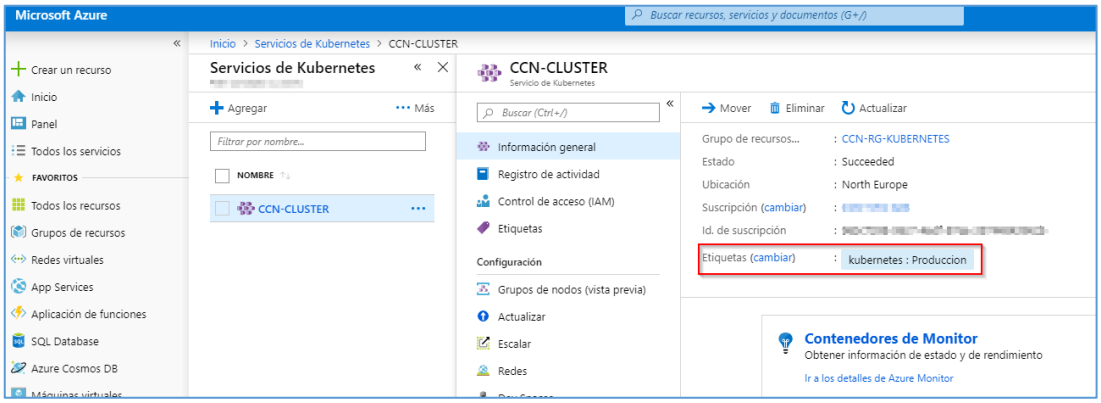
https://docs.microsoft.com/es-es/azure/aks/use-network-policies

3.2.2 Protection of information

3.2.2.1 Rating of information

Applying labels to Azure's resources facilitates the organization of Kubernetes' services. Each label consists of a name and a pair of values.

Labels allow you to retrieve related resources that are in different resource groups. This approach can be useful if you need to organize resources for management.



Note: *For more information on labels, see section [3.2.2.1 Qualification of Information] of the [CCN-STIC-884A - Azure Secure Configuration Guide].*

3.2.2.2 Backup

Azure Backup organizes the backups of the machines and manages the configuration of the restoration procedures. It also has two ways of backing up data for operational recovery.

The Azure Backup service executes in the cloud and maintains recovery points, enforces policy compliance, and allows to manage the application and the data protection.

Note: *For more information on Azure Backup, see section [3.2.2.3 Backup] of the [CCN-STIC-884A - Azure Secure Configuration Guide].*

4. GLOSSARY AND ABBREVIATIONS

4.1 GLOSSARY AND ABBREVIATIONS

The following describes several security terms, acronyms and abbreviations used in this guide:

Term	Definition
Cluster	These are physical or virtual resources, and storage resources used by Kubernetes where pods are deployed, managed and replicated. Kubernetes can be used in

	different systems such as: Windows Azure, Debian, Ubuntu, RedaHat, among others.
Pods	They are the smallest unit comprising one or more Docker containers operating under one unit. In many cases a Pod consists of a single container, but its ability to hold several containers in close proximity to each other is a very powerful feature of Kubernetes.
Replication Controllers	They manage the life cycle of the pod, ensuring that the number of automatic replicas of the pod are executing, creating and destroying the pods, as required.
Services	The services allow access to the containers with a unique DNS name and stable IP addresses.
FQDN	An FQDN (fully qualified domain name) is a name that includes the name of the server and the domain name associated to that computer.
Labels	They are fundamental and are used to organize and select a group of objects in pairs of the type key:value. They help to get the lists of the servers where the traffic should go.

5. SUMMARY TABLE OF SECURITY MEASURES

The following is a summary table of configurations to be applied for the protection of the service, where the organization will be able to evaluate which measures of the proposals are fulfilled.

<table>
<tr><th>ENS Control</th><th colspan="3">Configuration</th><th>Status</th></tr>
<tr><td>op</td><td colspan="4">Operational Framework</td></tr>
<tr><td>op.acc</td><td colspan="4">Access Control</td></tr>
<tr><td rowspan="3">op.acc.1</td><td colspan="4">Identification</td></tr>
<tr><td colspan="3" rowspan="2">For the correct management of AKS, Azure Active directory accounts and groups have been configured.

Section [3.1.1 Identification] the of [CCN-STIC-884A - Azure Secure Configuration Guide] guide has been consulted.</td><td>It applies:

☐ Yes ☐ No</td><td>It complies:

☐ Yes ☐ No</td></tr>
<tr><td>Evidence collected:

☐ Yes ☐ No</td><td>Comments:</td></tr>
<tr><td>op.acc.2</td><td colspan="4">Entry Requirements</td></tr>
</table>

	The access requirement has been configured according to sections 3.1.2.4 "Local access" and "3.1.2.5	**It applies:** ☐ Yes ☐ No	**It applies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
op.acc.3	**Segregation of functions and tasks**		
	Roles have been designed, created and applied to user groups. At least the Administrator and user roles for cluster, storage and networking should be applied.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**

op.acc.5	**Authentication mechanism**		
	Multi-Factor Authentication (MFA) has been enabled on the Tenant.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
op.acc.5	**Authentication mechanism**		
	A Multi-Factor Authentication policy has been created for administrators.	**It applies:** ☐ Yes ☐ No	**It complies** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
op.acc.6	**Local access**		
	Conditional access has been configured. Taking into account a source IP address/devices among others.	**It applies:** ☐ Yes ☐ No	**It applies:** ☐ Yes ☐ No

		Evidence collected: ☐ Yes ☐ No	**Comments:**
op.acc.6	**Remote Access**		
	The conditional access policy was enabled by delimiting geographical areas and IPS ranges for remote accesses.	**It applies:** ☐ Yes ☐ No	**It applies:** ☐ Yes ☐ No
		It applies: ☐ Yes ☐ No	**Comments:**
op.exp	**Exploitation**		
op.exp. 8	**Recording user activity**		
	It has been verified that the Audit log is activated and capturing events.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**

op.exp. 10	**Protection of activity logs**		
	The user activity log has been enabled. *See section [3.1.2.1 User Activity Log] of the [CCN-STIC-884A - Azure Secure Configuration Guide] guide.*	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op-exp.11	**Protection of cryptographic keys**		
	The Key Vault has been configured, limiting access to administrative users only. Following the instructions of the guide CCN-STIC-884A Safe configuration for Azure, section. 3.2.2.2 Encryption	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.cont.2	**Continuity plan**		
	Azure Site Recovery has been configured replicating the virtual machines and database in order to create a recovery plan.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐

No

		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.cont.3	**Periodic testing**		
	For the virtual machines a failover has been performed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evience collected: ☐ Yes ☐ No	**Comments:**
Op.mon.1	**Intrusion detection**		
	Azure monitor and *Azure Security Center* have been configured following the recommendations of the guide *CCN-STIC-884A Secure Configuration for Azure, section. [3.1.6 System Monitoring]*	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Op.mon.2	**Metric system**		

	Azure monitor has been configured applying the popular logs and Network Watcher display.	**It applies:** ☐ Yes ☐ No	**It applies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.com.1	**Secure perimeter**		
	The NSG / Azure Firewall deployment has been configured applying the recommended rules for Kubernetes.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.com.1	**Secure perimeter**		
	The application gateway has been configured.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No

		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.com.2	**Protection of confidentiality**		
	High availability VPN services connected to the management vnet have been deployed.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.com.3	**Protection of authenticity and integrity**		
	To cover this measure it is necessary to apply the services of: ***Azure Security Center*** ***Azure Multi-Factor Authentication*** ***Azure DDoS Protection***	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**

Mp.com.4	**Network Segregation**		
	The recommendations in section 3.2.1.1 have been configured.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.info.2	**Rating of information**		
	Azure labels have been configured in the installed services.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.info.3	**Encryption**		
	Encryption has been configured for the nodes in the cluster.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No

		☐ ☐	☐
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.info.9	**Backup**		
	A backup plan has been configured for the nodes in the Kubernetes cluster.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No
		Evidence collected: ☐ Yes ☐ No	**Comments:**
Mp.s.8	**Protection against denial of service**		
	DDOS have been configured and enabled on all the VNETs.	**It applies:** ☐ Yes ☐ No	**It complies:** ☐ Yes ☐ No