UNIVERSIDAD RAFAEL LANDÍVAR

FACULTAD DE INGENIERÍA

VIRTUALIZACIÓN

SECCIÓN 1 VESPERTINA

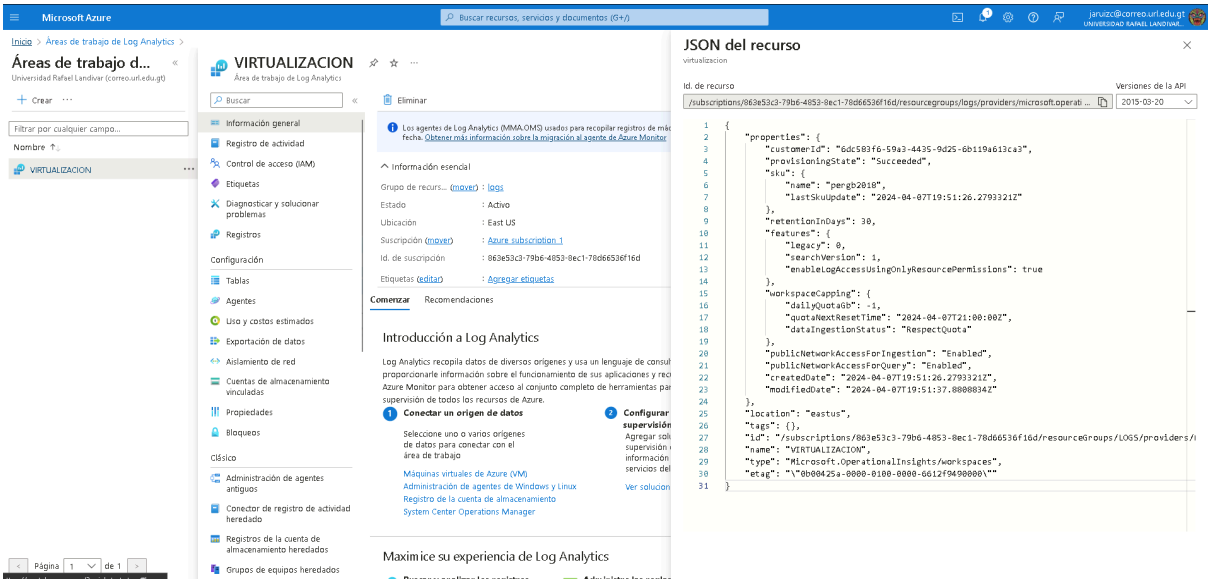
MGTR. JOSSUE LEONEL SAMAYOA PORTILLO

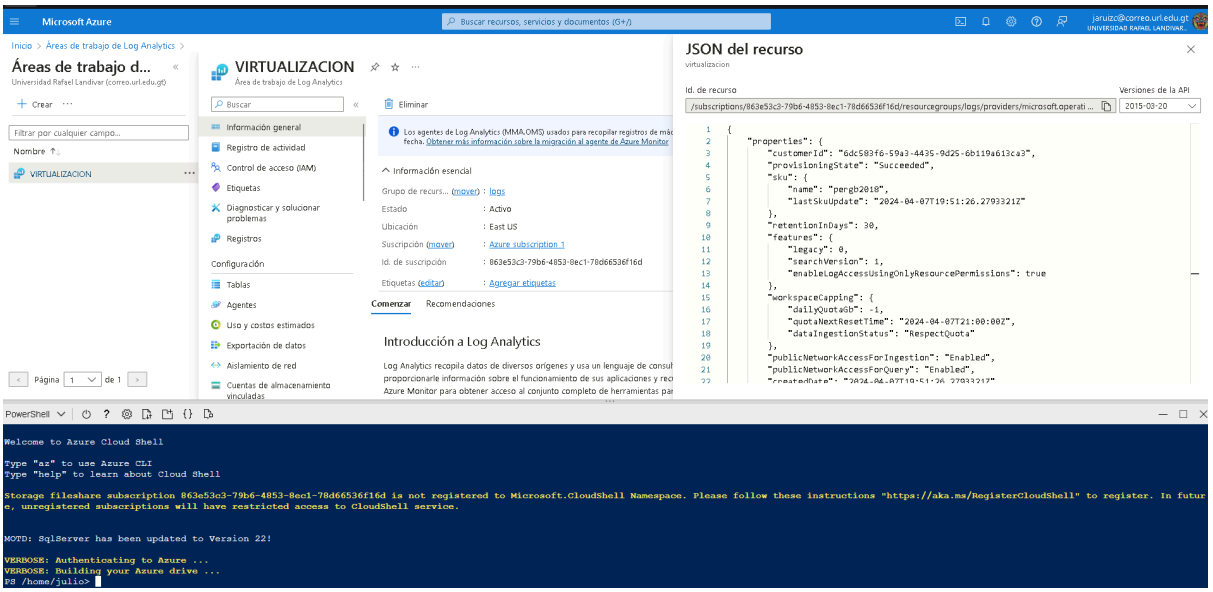
BUILD A LOG ANALYTICS SOLUTION ON AWS

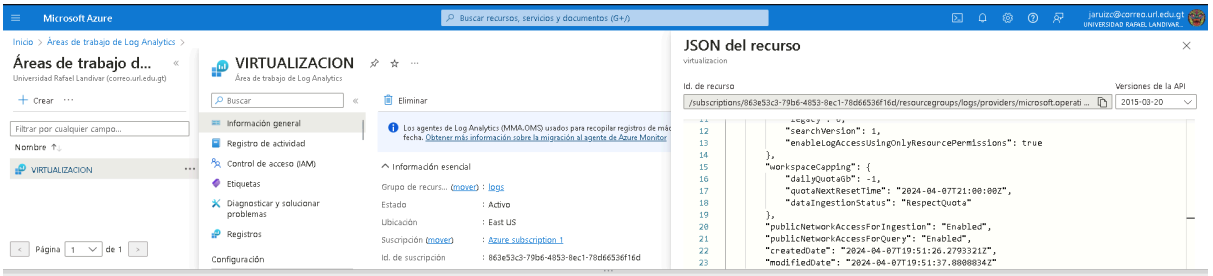
Julio Anthony Engels Ruiz Coto 1284719

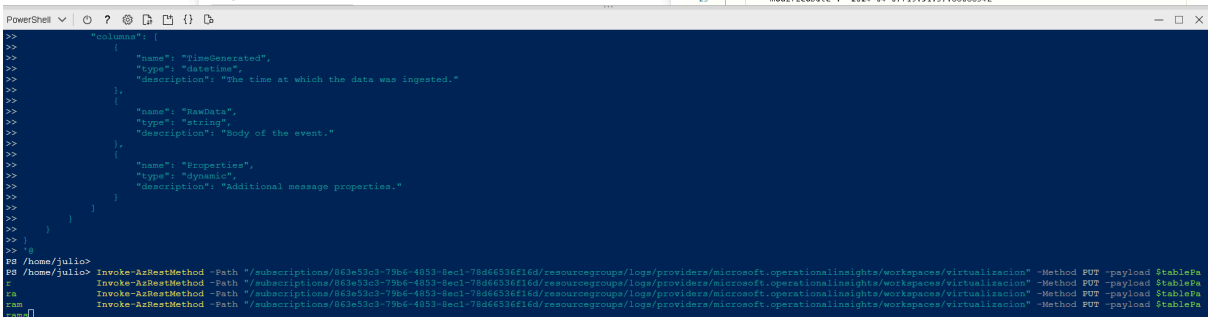
Eddie Alejandro Giron Carranza 1307419

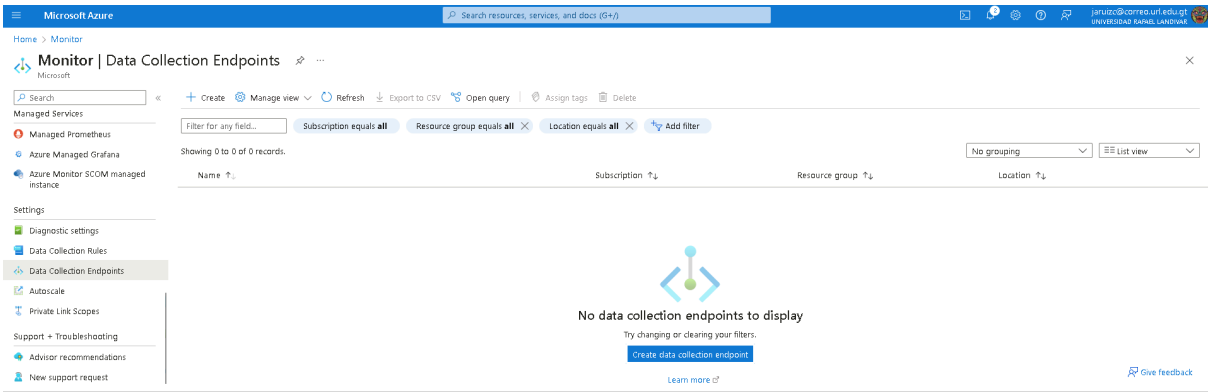
GUATEMALA DE LA ASUNCIÓN, ABRIL 7 DE 2024

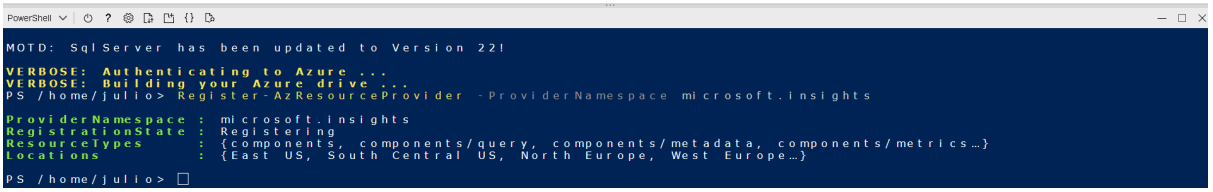

Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
jaruizc@correo.url.edu.gt
UNIVERSIDAD RAFAEL LANDIVAR
Inicio > Áreas de trabajo de Log Analytics >
Áreas de trabajo d...
Universidad Rafael Landivar (correo.url.edu.gt)
Crear
Filtrar por cualquier campo...
Nombre
VIRTUALIZACION
Página 1 de 1
VIRTUALIZACION
Área de trabajo de Log Analytics
Buscar
Información general
Registro de actividad
Control de acceso (IAM)
Etiquetas
Diagnosticar y solucionar problemas
Registros
Configuración
Tablas
Agentes
Uso y costos estimados
Exportación de datos
Aislamiento de red
Cuentas de almacenamiento vinculadas
Propiedades
Bloqueos
Clásico
Administración de agentes antiguos
Conector de registro de actividad heredado
Registros de la cuenta de almacenamiento heredados
Grupos de equipos heredados
Eliminar
Los agentes de Log Analytics (MMA,OMS) usados para recopilar registros de más
fecha. Obtener más información sobre la migración al agente de Azure Monitor
Información esencial
Grupo de recurs... (mover) : logs
Estado : Activo
Ubicación : East US
Suscripción (mover) : Azure subscription 1
Id. de suscripción : 863e53c3-79b6-4853-8ec1-78d66536f16d
Etiquetas (editar) : Agregar etiquetas
Comenzar
Recomendaciones
Introducción a Log Analytics
Log Analytics recopila datos de diversos orígenes y usa un lenguaje de consul
proporcionarle información sobre el funcionamiento de sus aplicaciones y rec
Azure Monitor para obtener acceso al conjunto completo de herramientas pa
supervisión de todos los recursos de Azure.
1 Conectar un origen de datos
Seleccione uno o varios orígenes de datos para conectar con el área de trabajo
Máquinas virtuales de Azure (VM)
Administración de agentes de Windows y Linux
Registro de la cuenta de almacenamiento
System Center Operations Manager
2 Configurar supervisión
Agregar sol
supervisión
información
servicios del
Ver solucion
Maximice su experiencia de Log Analytics
JSON del recurso
virtualizacion
Id. de recurso
/subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourcegroups/logs/providers/microsoft.operati ...
Versiones de la API
2015-03-20
{
"properties": {
"customerId": "6dc583f6-59a3-4435-9d25-6b119a613ca3",
"provisioningState": "Succeeded",
"sku": {
"name": "pergb2018",
"lastSkuUpdate": "2024-04-07T19:51:26.2793321Z"
},
"retentionInDays": 30,
"features": {
"legacy": 0,
"searchVersion": 1,
"enableLogAccessUsingOnlyResourcePermissions": true
},
"workspaceCapping": {
"dailyQuotaGb": -1,
"quotaNextResetTime": "2024-04-07T21:00:00Z",
"dataIngestionStatus": "RespectQuota"
},
"publicNetworkAccessForIngestion": "Enabled",
"publicNetworkAccessForQuery": "Enabled",
"createdDate": "2024-04-07T19:51:26.2793321Z",
"modifiedDate": "2024-04-07T19:51:37.8808834Z"
},
"location": "eastus",
"tags": {},
"id": "/subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourceGroups/LOGS/providers/
"name": "VIRTUALIZACION",
"type": "Microsoft.OperationalInsights/workspaces",
"etag": "\"0b00425a-0000-0100-0000-6612f0490000\""
}


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
jaruizc@correo.url.edu.gt
UNIVERSIDAD RAFAEL LANDIVAR
Inicio > Áreas de trabajo de Log Analytics >
Áreas de trabajo d...
Universidad Rafael Landivar (correo.url.edu.gt)
Crear
Filtrar por cualquier campo...
Nombre
VIRTUALIZACION
Página 1 de 1
VIRTUALIZACION
Área de trabajo de Log Analytics
Buscar
Información general
Registro de actividad
Control de acceso (IAM)
Etiquetas
Diagnosticar y solucionar problemas
Registros
Configuración
Tablas
Agentes
Uso y costos estimados
Exportación de datos
Aislamiento de red
Cuentas de almacenamiento vinculadas
Eliminar
Los agentes de Log Analytics (MMA,OMS) usados para recopilar registros de más
fecha. Obtener más información sobre la migración al agente de Azure Monitor
Información esencial
Grupo de recurs... (mover) : logs
Estado : Activo
Ubicación : East US
Suscripción (mover) : Azure subscription 1
Id. de suscripción : 863e53c3-79b6-4853-8ec1-78d66536f16d
Etiquetas (editar) : Agregar etiquetas
Comenzar
Recomendaciones
Introducción a Log Analytics
Log Analytics recopila datos de diversos orígenes y usa un lenguaje de consul
proporcionarle información sobre el funcionamiento de sus aplicaciones y rec
Azure Monitor para obtener acceso al conjunto completo de herramientas pa
JSON del recurso
virtualizacion
Id. de recurso
/subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourcegroups/logs/providers/microsoft.operati ...
Versiones de la API
2015-03-20
{
"properties": {
"customerId": "6dc583f6-59a3-4435-9d25-6b119a613ca3",
"provisioningState": "Succeeded",
"sku": {
"name": "pergb2018",
"lastSkuUpdate": "2024-04-07T19:51:26.2793321Z"
},
"retentionInDays": 30,
"features": {
"legacy": 0,
"searchVersion": 1,
"enableLogAccessUsingOnlyResourcePermissions": true
},
"workspaceCapping": {
"dailyQuotaGb": -1,
"quotaNextResetTime": "2024-04-07T21:00:00Z",
"dataIngestionStatus": "RespectQuota"
},
"publicNetworkAccessForIngestion": "Enabled",
"publicNetworkAccessForQuery": "Enabled",
PowerShell
Welcome to Azure Cloud Shell
Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell
Storage fileshare subscription 863e53c3-79b6-4853-8ec1-78d66536f16d is not registered to Microsoft.CloudShell Namespace. Please follow these instructions "https://aka.ms/RegisterCloudShell" to register. In futur
e, unregistered subscriptions will have restricted access to CloudShell service.
MOTD: SqlServer has been updated to Version 22!
VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/julio>









Los agentes de Log Analytics (MMA.OMS) usados para recopilar registros de máq
fecha. Obtener más información sobre la migración al agente de Azure Monitor

Grupo de recurs... (mover) : logs
Estado : Activo
Ubicación : East US
Suscripción (mover) : Azure subscription 1
Id. de suscripción : 863e53c3-79b6-4853-8ec1-78d66536f16d

Id. de recurso: /subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourcegroups/logs/providers/microsoft.operati ...

Versiones de la API: 2015-03-20

```
            "legacy": 0,
            "searchVersion": 1,
            "enableLogAccessUsingOnlyResourcePermissions": true
        },
        "workspaceCapping": {
            "dailyQuotaGb": -1,
            "quotaNextResetTime": "2024-04-07T21:00:00Z",
            "dataIngestionStatus": "RespectQuota"
        },
        "publicNetworkAccessForIngestion": "Enabled",
        "publicNetworkAccessForQuery": "Enabled",
        "createdDate": "2024-04-07T19:51:26.2793321Z",
        "modifiedDate": "2024-04-07T19:51:37.8808834Z"
```

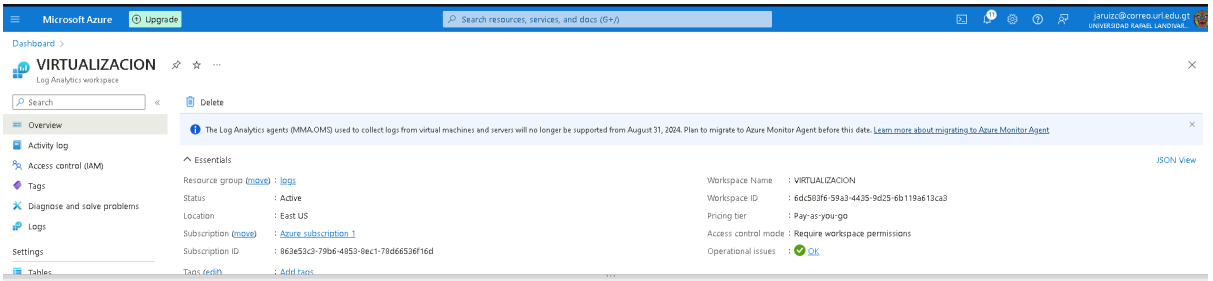
```
>>             "columns": [
>>                 {
>>                     "name": "TimeGenerated",
>>                     "type": "datetime",
>>                     "description": "The time at which the data was ingested."
>>                 },
>>                 {
>>                     "name": "RawData",
>>                     "type": "string",
>>                     "description": "Body of the event."
>>                 },
>>                 {
>>                     "name": "Properties",
>>                     "type": "dynamic",
>>                     "description": "Additional message properties."
>>                 }
>>             ]
>>         }
>>     }
>> }
>> '@
PS /home/julio>
PS /home/julio> Invoke-AzRestMethod -Path "/subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourcegroups/logs/providers/microsoft.operationalinsights/workspaces/virtualizacion" -Method PUT -payload $tablePa
r               Invoke-AzRestMethod -Path "/subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourcegroups/logs/providers/microsoft.operationalinsights/workspaces/virtualizacion" -Method PUT -payload $tablePa
ra              Invoke-AzRestMethod -Path "/subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourcegroups/logs/providers/microsoft.operationalinsights/workspaces/virtualizacion" -Method PUT -payload $tablePa
ram             Invoke-AzRestMethod -Path "/subscriptions/863e53c3-79b6-4853-8ec1-78d66536f16d/resourcegroups/logs/providers/microsoft.operationalinsights/workspaces/virtualizacion" -Method PUT -payload $tablePa
rams
```

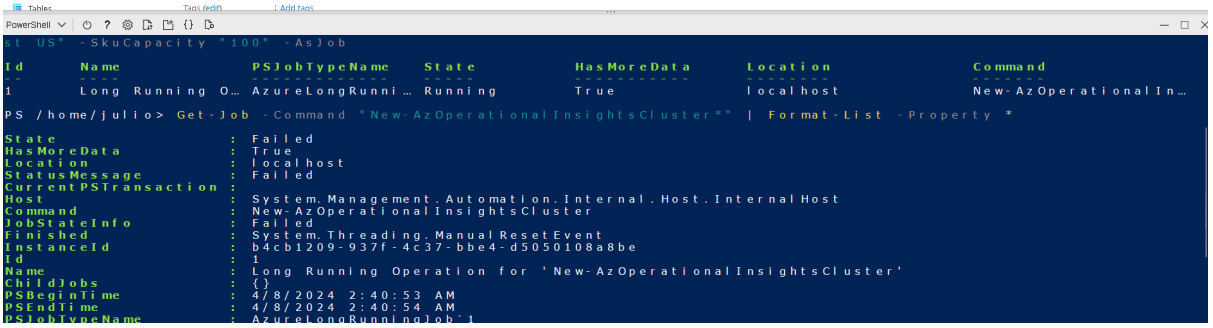
Showing 0 to 0 of 0 records.

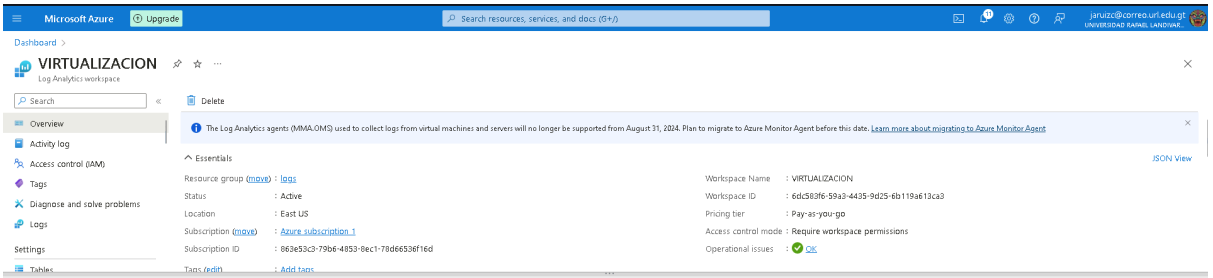
No data collection endpoints to display

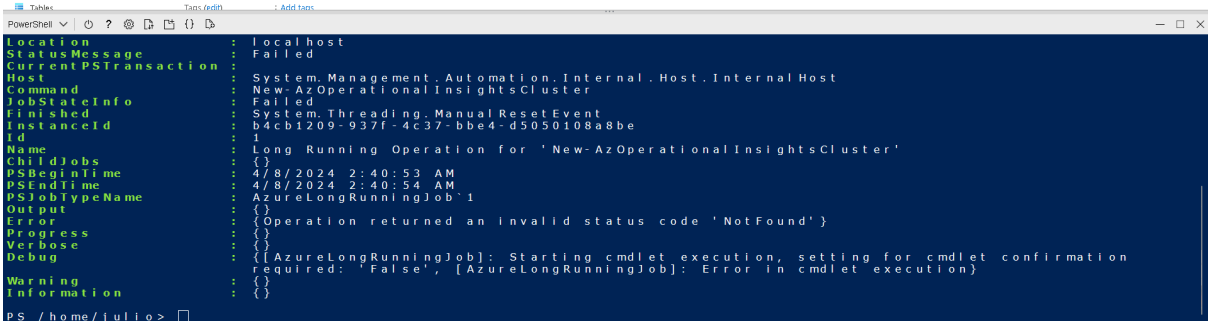
Try changing or clearing your filters.

```
MOTD: SqlServer has been updated to Version 22!

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/julio> Register-AzResourceProvider -ProviderNamespace microsoft.insights

ProviderNamespace : microsoft.insights
RegistrationState : Registering
ResourceTypes     : {components, components/query, components/metadata, components/metrics…}
Locations         : {East US, South Central US, North Europe, West Europe…}

PS /home/julio>
```


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
jaruizc@correo.url.edu.gt
UNIVERSIDAD RAFAEL LANDIVAR...
Dashboard
VIRTUALIZACION
Log Analytics workspace
Search
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Settings
Tables
The Log Analytics agents (MMA/OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to Azure Monitor Agent
Essentials
JSON View
Resource group (move) : logs
Status : Active
Location : East US
Subscription (move) : Azure subscription 1
Subscription ID : 863e53c3-79b6-4853-8ec1-78d66536f16d
Tags (edit) : Add tags
Workspace Name : VIRTUALIZACION
Workspace ID : 6dc583f6-59a3-4435-9d25-6b119a613ca3
Pricing tier : Pay-as-you-go
Access control mode : Require workspace permissions
Operational issues : OK


PowerShell
st US" -SkuCapacity "100" -AsJob
Id Name PSJobTypeName State HasMoreData Location Command
1 Long Running O... AzureLongRunni... Running True localhost New-AzOperationalIn...
PS /home/julio> Get-Job -Command "New-AzOperationalInsightsCluster*" | Format-List -Property *
State : Failed
HasMoreData : True
Location : localhost
StatusMessage : Failed
CurrentPSTransaction :
Host : System.Management.Automation.Internal.Host.InternalHost
Command : New-AzOperationalInsightsCluster
JobStateInfo : Failed
Finished : System.Threading.ManualResetEvent
InstanceId : b4cb1209-937f-4c37-bbe4-d5050108a8be
Id : 1
Name : Long Running Operation for 'New-AzOperationalInsightsCluster'
ChildJobs : {}
PSBeginTime : 4/8/2024 2:40:53 AM
PSEndTime : 4/8/2024 2:40:54 AM
PSJobTypeName : AzureLongRunningJob`1


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
jaruizc@correo.url.edu.gt
UNIVERSIDAD RAFAEL LANDIVAR...
Dashboard
VIRTUALIZACION
Log Analytics workspace
Search
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Settings
Tables
The Log Analytics agents (MMA/OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. Learn more about migrating to Azure Monitor Agent
Essentials
JSON View
Resource group (move) : logs
Status : Active
Location : East US
Subscription (move) : Azure subscription 1
Subscription ID : 863e53c3-79b6-4853-8ec1-78d66536f16d
Tags (edit) : Add tags
Workspace Name : VIRTUALIZACION
Workspace ID : 6dc583f6-59a3-4435-9d25-6b119a613ca3
Pricing tier : Pay-as-you-go
Access control mode : Require workspace permissions
Operational issues : OK


PowerShell
Location : localhost
StatusMessage : Failed
CurrentPSTransaction :
Host : System.Management.Automation.Internal.Host.InternalHost
Command : New-AzOperationalInsightsCluster
JobStateInfo : Failed
Finished : System.Threading.ManualResetEvent
InstanceId : b4cb1209-937f-4c37-bbe4-d5050108a8be
Id : 1
Name : Long Running Operation for 'New-AzOperationalInsightsCluster'
ChildJobs : {}
PSBeginTime : 4/8/2024 2:40:53 AM
PSEndTime : 4/8/2024 2:40:54 AM
PSJobTypeName : AzureLongRunningJob`1
Output : {}
Error : {Operation returned an invalid status code 'NotFound'}
Progress : {}
Verbose : {}
Debug : {[AzureLongRunningJob]: Starting cmdlet execution, setting for cmdlet confirmation required: 'False', [AzureLongRunningJob]: Error in cmdlet execution}
Warning : {}
Information : {}
PS /home/julio>