Inventory of Azure virtual machines

You might want a comprehensive list of virtual machines in your Azure environment when doing the following:

- Managing Azure cloud infrastructure

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Microsoft Azure virtual machine data
- Splunk Add-on for Microsoft Cloud Services

Example

As an administrator, you want to have a high-level view of the number and type of virtual machines running in your Azure infrastructure.

To optimize the search shown below, you should specify an index and a time range.

1. Run the following search:

```
sourcetype= "mscs:resource:virtualMachine"
| fillnull tags={} value="No Tags!"
| fillnull properties.instanceView.extensions{}.name value=""
| stats latest(power_state) BY vm_name, location, properties.storageProfile.imageReference.offer, properties.storageProfile.imageReference.sku, vm_size, tags{}, properties.instanceView.extensions{}.name
| eval mem_capacity=(mem_capacity/1024/1024/1024)
| fields - count
| rename vm_name AS "VM Name" latest(power_state) AS Status vm_size AS Size properties.storageProfile.imageReference.offer AS OS properties.storageProfile.imageReference.sku AS Version mem_capacity AS "Memory GB" location_name AS Location cpu_cores AS CPU tags{} AS Tags properties.instanceView.extensions{}.name AS Extensions
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
### Splunk Search

```splunk
sourcetype="mscs:resource:virtualMachine"
```

**Explanation**

Search only Azure virtual machine data.

### Explanation

| Fill all null tag values with "No Tags!"
| Fill all null extension values with an empty string.
| Locate the most recent value for all relevant fields.
| Calculate the memory capacity for all virtual machines.
| Remove the count field from the results.
| Rename the fields as shown for better readability.

### Result

Sample results for this search are shown in the table below. The status field can be an important item to monitor for cost saving reasons. A status of stopped (not shown below) indicates a VM that had the OS shut down or stopped, but the VM is still allocated and is costing money. Finding those and having the VM deallocated would be useful.
<table>
<thead>
<tr>
<th>VM Name</th>
<th>location</th>
<th>OS</th>
<th>Version</th>
<th>Size</th>
<th>Tags</th>
<th>Extension</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>JaneDoeServer</td>
<td>southcentralus</td>
<td>WindowsServer</td>
<td>2016-Datacenter</td>
<td>Standard_B1s</td>
<td>No Tags!</td>
<td></td>
<td>running</td>
</tr>
<tr>
<td>RYCRYpt0</td>
<td>australiasotheast</td>
<td>CentOS</td>
<td>7.5</td>
<td>Standard_B1s</td>
<td>Owner: RYCRYpt0</td>
<td></td>
<td>starting</td>
</tr>
<tr>
<td>Ry-Win10</td>
<td>australiasotheast</td>
<td>Windows-10</td>
<td>rs5-pro</td>
<td>Standard_D2</td>
<td>Owner: Ryan</td>
<td>Microsoft.IInsights.VMDiagnosticSettings</td>
<td>running</td>
</tr>
<tr>
<td>Ry-Win10</td>
<td>australiasotheast</td>
<td>Windows-10</td>
<td>rs5-pro</td>
<td>Standard_D2</td>
<td>Owner: Ryan</td>
<td>MicrosoftMonitoringAgent</td>
<td>running</td>
</tr>
<tr>
<td>Ry-Win10</td>
<td>australiasotheast</td>
<td>Windows-10</td>
<td>rs5-pro</td>
<td>Standard_D2</td>
<td>Purpose: P5</td>
<td>Microsoft.IInsights.VMDiagnosticSettings</td>
<td>running</td>
</tr>
</tbody>
</table>

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.