Managing Azure cloud infrastructure

To reduce the expenses of buying, owning, and maintaining physical data centers and servers, your organization has converted most of its infrastructure virtual with the help of Azure. This means you have whole new data types to secure and monitor. You have to relearn everything you used to know how to do in order to keep your organization running safely and efficiently. You want to use your Splunk deployment to manage all components of your cloud infrastructure and provide you with necessary information and alerts.

Data required

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- **People:** Cloud administrator
- **Technologies:**
  - Splunk Enterprise or Splunk Cloud Platform
  - Splunk Add-on for Microsoft Cloud Services
  - Microsoft Azure Add-on for Splunk
- **Data:** Azure cloud environment data

How to use Splunk software for this use case

You can run many searches with Splunk software to maintain Azure cloud infrastructure. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Inventory of Azure virtual machines
- Inventory of Azure virtual networks
- List of Azure resource public IP addresses
- List of Azure resource network interface cards
- Inventory of Azure managed disks
- Inventory of unattached Azure managed disks
- Calculating the cost of unattached disks
- Azure security policy review
- Azure resources with no associated tags
- Successful Azure audit operations
- Azure Active Directory audit events
Next steps

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Operational expenses savings due to efficiency actions from observability
- Reduced mean time to problem resolution (MTTR)
- Reduced time for compliance reporting.

You should also review these organizational processes that commonly impact success with this use case:

- Capacity planning and cost tracking. This is important in all IT shops but increases in important when using cloud services.
- Security and compliance

This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Blog: Real-Time operational intelligence for Microsoft Azure
- Blog: Splunking Azure: Event Hubs
- Blog: Splunk Azure: NSG Flow logs
- Conf Talk: Monitor and manage your cloud environment with Azure Monitor and Splunk
- Conf Talk: Gain end-to-end visibility into your Azure cloud environment using Splunk
- Conf Talk: Show and Tell: Prescriptive Use Cases for Azure and Office 365
- Chart: Azure Add-on Landscape (This is a highly recommended resource for understanding the various add-ons for getting data in from Azure)
- App: Microsoft Azure App for Splunk