CHAPTER 2

Mitigate threats using Microsoft Defender for Cloud

One critical component of any Security Operations Center (SOC) is the quality of the alert that is received from a given data source. The quality of the alert can be measured by the relevance of the information contained in the alert, how that alert reflects into the threat vectors of a cloud workload, and how these indications can help security operation analysts to investigate and respond to that alert. Microsoft Defender for Cloud has different plans that offer threat detections for specific workloads, based on analytics that were created specifically for the threat vector of the workload's type.

To mitigate threats using Microsoft Defender for Cloud you must be able to design, configure, and manage the different types of Microsoft Defender for Cloud plans, manage rules, and understand how to investigate and automate response.

Skills covered in this chapter:

- Design and configure Microsoft Defender for Cloud implementation
- Plan and implement the use of data connectors for ingestion of data in Microsoft Defender for Cloud
- Manage Microsoft Defender for Cloud alert rules
- Configure automation and remediation
- Investigate Microsoft Defender for Cloud alerts and incidents

Skill 2-1: Design and configure Microsoft Defender for Cloud implementation

Before implementing Microsoft Defender for Cloud it is important to understand the different design considerations that will directly affect how you configure the solution based on the scenario's requirements. This section of the chapter covers the skills necessary to design and configure Microsoft Defender for Cloud implementation according to the SC-200 exam outline.

Plan and configure Microsoft Defender for Cloud settings, including selecting target subscriptions and workspace

When planning to use Microsoft Defender for Cloud, you must understand the requirements for the type of plan that you want to implement. If you are planning the implementation of Defender for Servers, Defender for Containers, or Defender for SQL Server on Machines, you also need to consider the requirement to deploy the Log Analytics (LA) Agent to the machines. By doing so, you will need to select the workspace to which the agent will send the information.

Other Microsoft Defender for Cloud plans that are based on other Azure Platform as a Service (PaaS) offerings don't require a workspace configuration in the beginning. This includes plans such as Defender for Key Vault, Defender for App Service, Defender for Resource Manager, Defender for Storage, Defender for Container, Defender for SQL database, Defender for DNS. You will only need to configure a workspace for these Microsoft Defender for Cloud plans if you consider utilizing the *continuous export* capability in Microsoft Defender for Cloud. This feature is often used in the following scenarios:

- When the organization wants to store all alerts that are triggered by all Microsoft Defender for Cloud plans in the workspace because. By default, only VM-based alerts are stored in the workspace.
- When the organization wants to store all security recommendations or regulatory compliance information in the workspace.
- When the organization needs to send the alerts to a security information and event management (SIEM) via Azure Event Hub.

When you first activate Microsoft Defender for Cloud, the auto-provisioning feature is not enabled. However, if you want to ensure that all VMs are automatically configured to receive the LA agent and send the data to the correct workspace, you should enable this option. When auto-provisioning is enabled, and the **Connect Azure VMs To The Default Workspace(s) Created By Security Center** option is selected, Security Center will automatically create and manage a new workspace. Defender for Cloud creates a new resource group and a workspace (called default workspace) in the same geolocation of the VM and connects the agent to that workspace. The naming conventions for the default workspace and resource group are shown below:

- **Workspace** `DefaultWorkspace-[subscription-ID]-[geo]`
- **Resource Group** `DefaultResourceGroup-[geo]`

The fact that a default workspace is created according to the geolocation of the VM is an advantage if your design requirements dictates that you need to ensure that the data sent from the VM is stored in the same region as the VM's location. Table 2-1 shows where the workspace will reside according to the VM's location:

TABLE 2-1 VM and workspace locations

VM Location	Workspace Location
United States and Brazil	United States
Canada	Canada
Europe	Europe
United Kingdom	United Kingdom
East Asia and Southeast Asia	Asia
Korea	Korea
India	India
Japan	Japan
China	China
Australia	Australia

If your organization is already utilizing a Log Analytics workspace and it wants to leverage the same workspace for Defender for Cloud, you should select the **Connect Azure VMs To A Different Workspace** option and specify the workspace, which can be any workspace across all selected subscriptions within the same tenant.

The general best practice for workspace creation is to keep it as minimal as possible, which is not the case when you configure Defender for Cloud to manage the workspaces. When reading a scenario in the SC-200 exam, take into consideration the business requirements as well as the technical requirements. These requirements will lead you to select one of these two options:

- You could use the default workspace, which can create a lot of workspaces according to the regions where the company's VMs reside
- You could take a more centralized approach where all VMs across all subscriptions will have to send data to a single workspace.

IMPORTANT **BEST PRACTICES**

If you plan to use the same workspace for Microsoft Sentinel and Microsoft Defender for Cloud, make sure to read the best practices highlighted in this post: *http://aka.ms/ascbook-lawbp*.

The actual steps to configure auto-provisioning and specify the workspace are provided later in this chapter.

Configure Microsoft Defender for Cloud roles

Security Center uses Role-Cased Access Control (RBAC) based in Azure. By default, there are two roles in Defender for Cloud: **Security Reader** and **Security Admin**. The **Security Reader** role should be assigned to all users that need read access only to the dashboard. For example, Security Operations personnel that needs to monitor, and respond to security alerts, should be assigned the **Security Reader** role. It is important to mention that the assignment of this role is done in the Azure level, under the resource group that Defender for Cloud is monitoring, and using **Access Control (IAM)**, as shown in Figure 2-1.

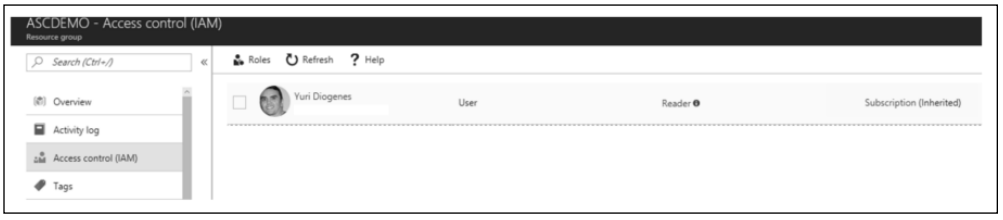

FIGURE 2-1 Access control in Azure

Workload owners usually need to manage a particular cloud workload and its related resources. Besides that, the workload owner is responsible for implementing and maintaining protections in accordance with company security policy. **Security Admin** role should be assigned for users that need to manage Defender for Cloud configuration.

Only subscription **Owners/Contributors** and **Security Admins** can edit a security policy. Only subscription and resource group Owners and Contributors can apply security recommendations for a resource. To enable Microsoft Defender for Cloud, you need **Security Admin** or **Subscription Owner** privilege. To learn more about Role-Based Access Control (RBAC) in Azure, visit *http://aka.ms/azurerbac*.

Custom roles

There will be some scenarios where the organization may want to provide a more granular privilege for some users instead of granting access to the entire **Security Admin** access role. Consider an organization called Contoso that needs to provide privilege to security operation analysts to simply visualize and create alert-suppression rules. In this case, the **Security Admin** role provides more privileges than what is necessary. For scenarios like this, you can create a custom role in Azure and assign write privilege to this operation: `Microsoft.Security/alertsSuppressionRules/write`.

MORE INFO **CREATING CUSTOM ROLES**

To create custom roles, see *http://aka.ms/SC200_CustomRole*.

Another common scenario is when an organization needs to create a custom role to allow users to configure or edit the just-in-time (JIT) VM access. You need a set of privileges to work with JIT; these privileges will vary according to the type of operation that you need to perform or that you want to allow a user to perform. You can be very granular about this permission assignment by using these guidelines:

To configure or edit a JIT policy for a VM, you need to assign these actions to the role:

- On the scope of a subscription or resource group that is associated with the VM: `Microsoft.Security/locations/jitNetworkAccessPolicies/write`.
- On the scope of a subscription or resource group of VM: `Microsoft.Compute/virtualMachines/write`.

To request access to a VM, you need to assign these actions to the user:

- On the scope of a subscription or resource group that is associated with the VM: `Microsoft.Security/locations/jitNetworkAccessPolicies/initiate/action`.
- On the scope of a subscription or resource group that is associated with the VM: `Microsoft.Security/locations/jitNetworkAccessPolicies/*/read`.
- On the scope of a subscription or resource group or VM: `Microsoft.Compute/virtualMachines/read`.
- On the scope of a subscription or resource group or VM: `Microsoft.Network/networkInterfaces/*/read`.

On the scope of a subscription, resource group, or VM that you need to read JIT policies, assign these actions to the user:

- `Microsoft.Security/locations/jitNetworkAccessPolicies/read`
- `Microsoft.Security/locations/jitNetworkAccessPolicies/initiate/action`
- `Microsoft.Security/policies/read`
- `Microsoft.Security/pricings/read`
- `Microsoft.Compute/virtualMachines/read`
- `Microsoft.Network/*/read`

Also, if you need to see the JIT NSG policy from the VM—Networking blade, you need to add the following policies:

- `Microsoft.Network/networkSecurityGroups/read`
- `Microsoft.Network/networkSecurityGroups/defaultSecurityRules/read`
- `Microsoft.Network/networkSecurityGroups/securityRules/read`

While the permissions above can be utilized to apply the principle of least privilege, keep in mind that you will need to merge some permissions if you are accessing via the Azure portal. For example, to configure or edit a JIT policy for a VM, you will need the privileges given and the privileges to read JIT policies.

Configure data retention policies

Microsoft Defender for Servers provides 500 MB per node, per day of free allowance for the data allocated in the Log Analytics workspace against the following subsets of security data types:

- `WindowsEvent`
- `SecurityAlert`
- `SecurityBaseline`
- `SecurityBaselineSummary`
- `SecurityDetection`
- `SecurityEvent`
- `WindowsFirewall`
- `MaliciousIPCommunication`
- `LinuxAuditLog`
- `SysmonEvent`
- `ProtectionStatus`

`Update` and `UpdateSummary` data types can be used when the Update Management solution is not running on the workspace or when solution targeting is enabled.

If the workspace is in the legacy *Per Node* pricing tier, the Microsoft Defender for Servers and Log Analytics allocations are combined and applied jointly to all billable ingested data. When you configure Microsoft Defender for Cloud to utilize a workspace, the data will be stored there is going to be available for 30 days by default. However, you can configure data retention at the workspace level up to 730 days (2 years) for all workspaces unless they are using the legacy *free* tier (for example, when using Microsoft Defender for Cloud without upgrading to Microsoft Defender for Cloud plans).

> ***IMPORTANT*** **AZURE MONITOR PRICING**
>
> **When you choose to extend your data retention for the workspace used by Microsoft Defender for Cloud, extra charges will be applied as per Log Analytics workspace pricing. If the same workspace is shared with Microsoft Sentinel, you get 90 days of data retention included. Visit the Azure Monitor pricing page for more information about the current pricing: *https://azure.microsoft.com/en-us/pricing/details/monitor/*.**

Depending on the scenario that you are addressing, you might need to extend the data retention to more than 30 days. Make sure to always review the business and technical requirements of the scenario for hints about data retention. Once you determine the data retention goal, follow the steps below to configure data retention in Log Analytics workspace:

1. Navigate to the Azure portal by opening *https://portal.azure.com*.
2. In the search bar, type **log ana**, and under **Services**, click **Log Analytics Workspaces**.
3. In the **Log Analytics Workspaces** dashboard, click the workspace for which you want to configure data retention.

4. In the left navigation pane, in the **General** section, click **Usage And Estimated Costs.** The **Usage And Estimated Costs** page appears, as shown in Figure 2-2.

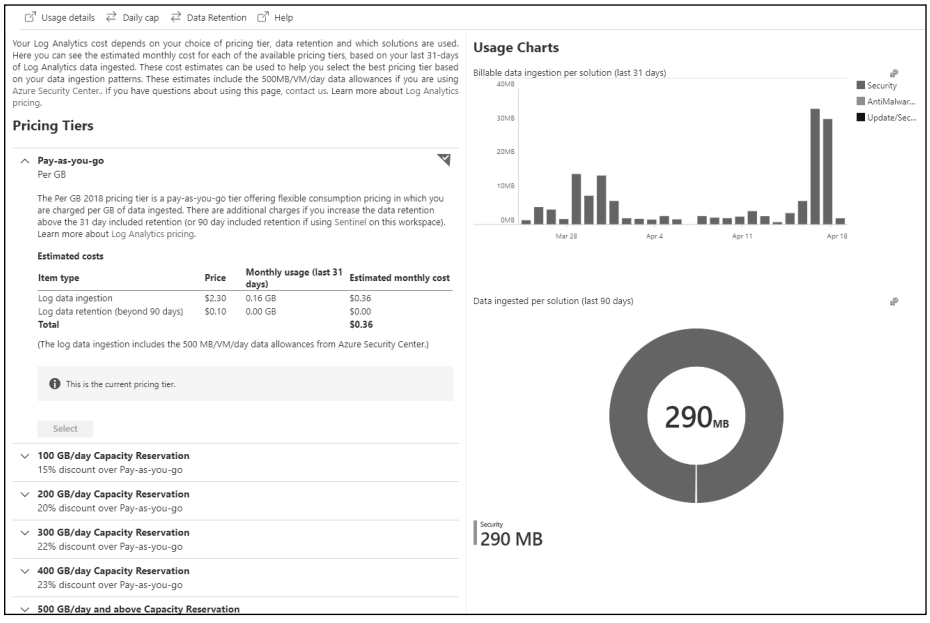

FIGURE 2-2 Log Analytics workspace usage and cost

5. Click the **Data Retention** button, and the **Data Retention** blade appears, as shown in Figure 2-3.

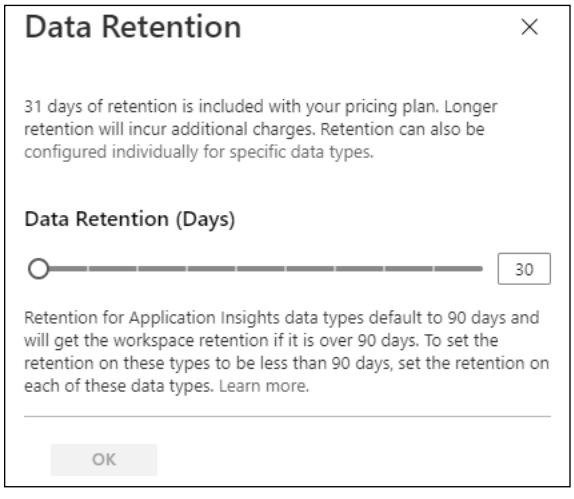

FIGURE 2-3 Configuring data retention for the Log Analytics workspace

6. You can use the **Data Retention (Days)** slider to increase the number of days that you want to retain the data. Once you finish, click the **OK** button to commit the changes.

You can also utilize an Azure Resource Manager (ARM) template to configure data retention by using the `retentionInDays` parameter. The advantage of using an ARM template for this operation is that you can apply in scale, and you can also customize other parameters. For example, if the scenario requires that you set the data retention to 30 days and trigger an immediate purge of older data, you can do that by using the `immediatePurgeDataOn30Days` parameter, which eliminates the grace period. This configuration could also be useful for compliance-related scenarios where immediate data removal is mandatory.

While the extension of the data retention policy for the entire workspace is usually the most common scenario, there are some situations that you might need to change the data retention based on a specific data type. Retention settings for individual data types are available from 4 to 730 days (except for workspaces in the legacy free tier). These settings will override the workspace-level default retention. You will also need to use ARM to change this setting. In the example below, the data retention for the `SecurityEvent` data type is being changed to 550 days:

```
PUT /subscriptions/00000000-0000-0000-0000-00000000000/resourceGroups/
MyResourceGroupName/providers/Microsoft.OperationalInsights/workspaces/MyWorkspaceName/
Tables/SecurityEvent?api-version=2017-04-26-preview
    {
        "properties":
        {
            "retentionInDays": 550
        }
    }
```

EXAM TIP

When evaluating a scenario in the SC-200 exam, look for business requirements that lead to cost savings on data. Changing data retention only in certain data types can be used to reduce overall costs for data retention.

Assess and recommend cloud workload protection

As enterprises start their journeys to the cloud, they will face many challenges as they adapt their on-premises tools to a cloud-based model. In a cloud environment where there are different workloads to manage, it becomes imperative to have ongoing verification and corrective actions to ensure that the security posture of those workloads is always at the highest possible quality.

Defender for Cloud has a variety of capabilities that can be used in two categories of cloud solutions:

- **Cloud Security Posture Management (CSPM)** This enables organizations to assess their cloud infrastructure to ensure compliance with industry regulations and identify security vulnerabilities in their cloud workloads.

- **Cloud Workload Protection Platform (CWPP)** This enables organizations to assess their cloud workload risks and detect threats against their servers (IaaS), containers, databases (PaaS), and storage. It also allows organizations to identity faulty configurations and remediate those with security best-practice configurations. To use the CWPP capabilities, you need to upgrade to Microsoft Defender for Cloud plans.

With an Azure subscription, you can activate the free tier of Defender for Cloud, which monitors compute, network, storage, and application resources in Azure. It also provides security policy, security assessment, security recommendations, and the ability to connect with other security partner solutions.

Even organizations that are getting started with Infrastructure as a Service (IaaS) in Azure can benefit from this free service because it will improve their security postures. When you upgrade your Defender for Cloud subscription from the free tier to Defender for Servers, the Microsoft Defender for Servers will be automatically enabled. With this plan, the following features will be available:

- Security event collection and advanced search
- Network Map
- Just-in-time VM Access
- Adaptive application controls
- Regulatory compliance reports
- File integrity monitoring
- Network Security Group (NSG) hardening
- Security alerts
- Threat protection for Azure VMs, non-Azure VMs, and PaaS services
- Integration with Microsoft Defender for Endpoint (MDE)
- Integration with Microsoft Cloud App Security (MCAS)
- Multi-cloud support for Amazon Web Services (AWS) and Google Cloud Platform (GCP)
- Vulnerability assessment integration with Qualys and Microsoft Threat Vulnerability Management (TVM)

Another advantage of upgrading to Microsoft Defender for Servers is that it allows you to monitor on-premises resources and VMs hosted by other cloud providers. You achieve this by onboarding your machine using Azure Arc and then installing the Log Analytics agent on the target machine.

Assessment and recommendations

Defender for Cloud will identify resources (compute, network, storage, identity, and application) that need security recommendations and will automatically suggest changes. You can see all recommendations in a single place, which is available under **General** > **Recommendations**. There, you can see security controls, as shown in Figure 2-4.

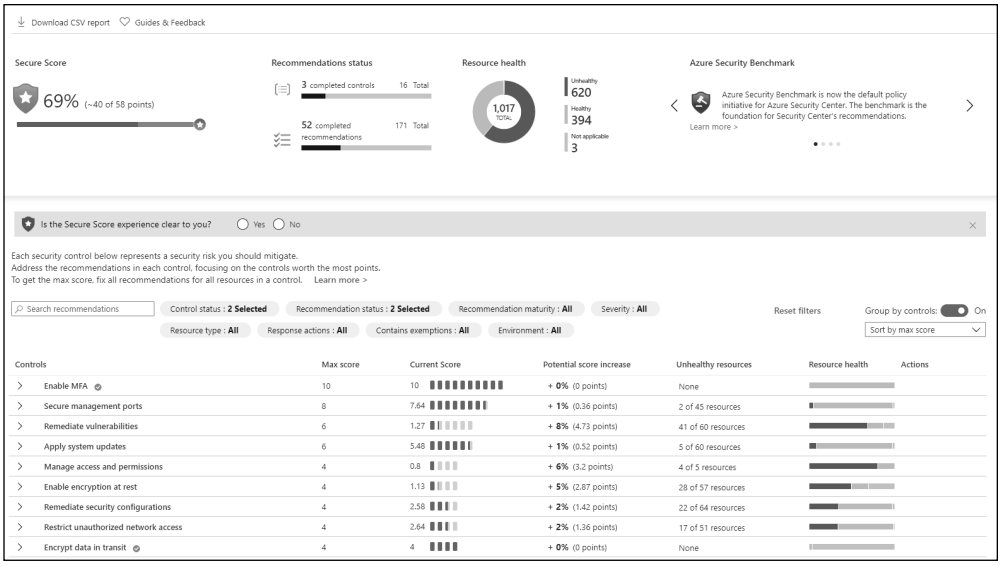

FIGURE 2-4 Security recommendations in Microsoft Defender for Cloud

During this initial assessment, Microsoft Defender for Cloud will also identify which workloads are available in the subscription. Also, it will suggest enabling the different Microsoft Defender for Cloud plans for cloud workload protection. All plans will be part of the Microsoft Defender for Cloud security control, as shown in Figure 2-5.

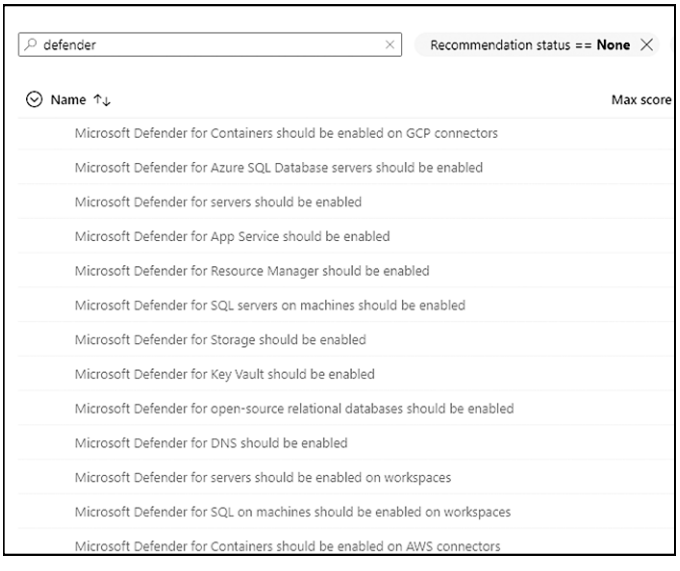

FIGURE 2-5 Enable Microsoft Defender security control

Enabling Microsoft Defender for Cloud Plans

To enable Microsoft Defender for Cloud plans, you can click each recommendation and follow the remediation steps, go to the **Environment settings** option in the left navigation pane, select the subscription, and select the plans you want to utilize. To review the pricing selection, click the **Environment settings** option in the left navigation pane, and under **Management**, click the subscription on which you want to enable Microsoft Defender for Cloud plans. The **Microsoft Defender for Cloud** plans page will appear, as shown in Figure 2-6.

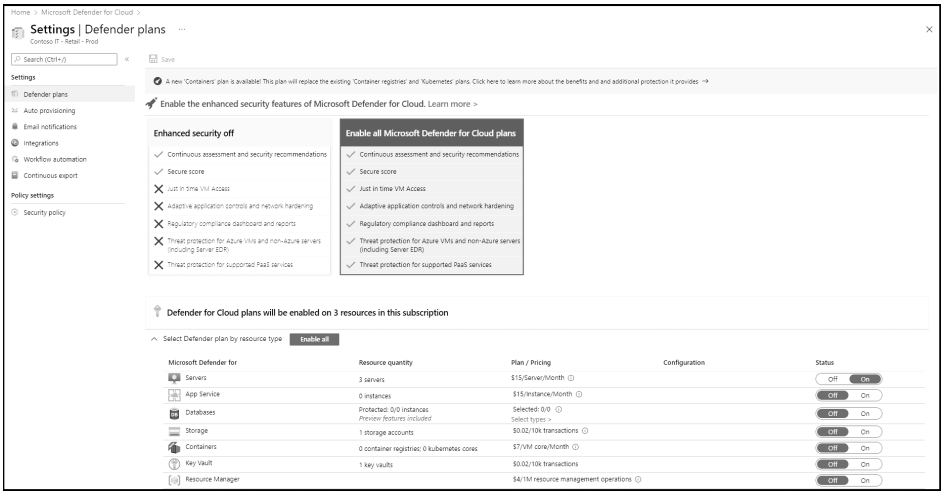

FIGURE 2-6 Pricing page showing the different Microsoft Defender for Cloud plans

On this page, you can change the toggle to **ON** or **OFF**, where **ON** means that the Microsoft Defender for Cloud plan is enabled on the selected subscription. While most of the Microsoft Defender for Cloud plans can only be enabled on the subscription level, there are a couple that can be enabled individually:

- Defender for SQL (Azure SQL Database)
- Defender for Storage (Storage)

In both cases, you can toggle these to the **OFF** setting on this page, and you can go to each Azure SQL database or each Azure Storage account and enable Microsoft Defender for Cloud plans from there. You might do this if the business requirement is to save cost by only enabling Defender for SQL or Defender for Storage on a company's most critical assets, rather than enabling them for the entire subscription.

Make sure to analyze the business requirements that will guide you when deciding whether to disable it at the subscription level and enable it on each resource. If you need to enable Microsoft Defender for Cloud in scale, you can also use ARM Templates or Azure Policy.

Skill 2-2: Plan and implement the use of data connectors for ingestion of data sources in Microsoft Defender for Cloud

When you upgrade from Microsoft Defender for Cloud to Microsoft Defender for Cloud plans, you can start monitoring the security posture of different cloud providers, including Amazon Web Service (AWS) and Google Cloud Platform (GCP). Ingesting data from these platforms is a mandatory step when you need to have visibility across different workloads located in multiple cloud providers. This section covers the skills necessary to plan and implement the use of data connectors for ingestion of data sources in Microsoft Defender for Cloud according to the SC-200 exam outline.

Identify data sources to be ingested for Microsoft Defender for Cloud

Microsoft Defender for Cloud supports the integration of partner security solutions, such as vulnerability assessment by Qualys and Rapid7. It can also integrate with the Microsoft Azure Web Application Firewall on the Azure Application Gateway. The advantage of using this integration varies according to the solution. For vulnerability assessment, the agent can be provisioned using the license you already have for the product (Qualys or Rapid7). Follow these steps to access the **Security Solutions** dashboard:

1. Navigate to the Azure portal by opening *https://portal.azure.com*.
2. In the search bar, type **security,** and under **Services**, click **Microsoft Defender for Cloud**.
3. In Defender for Cloud main dashboard, in the **Management** section, click **Security Solutions**. The **Security Solutions** page appears, as shown in Figure 2-7.

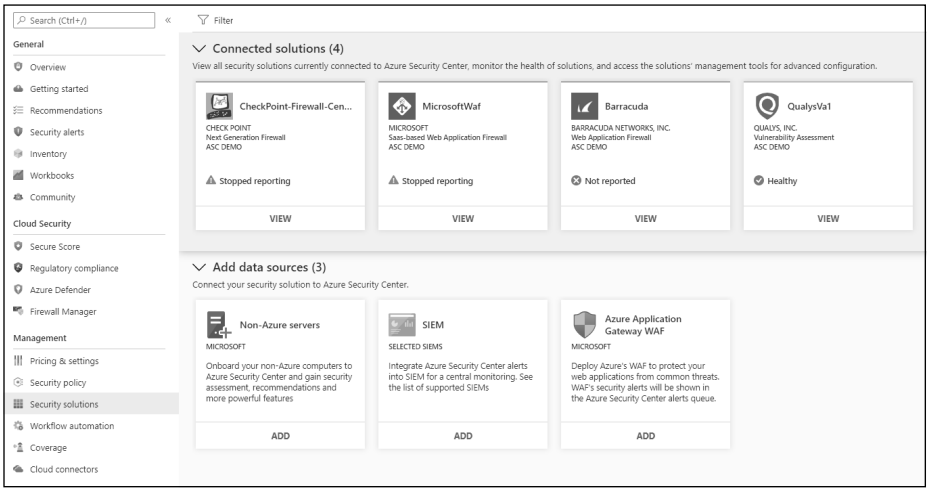

FIGURE 2-7 Security Solutions page with the connected solutions and available data sources

The **Connected Solutions** section is populated according to the solutions that were already deployed. The deployment of the solution will vary according to the vendor. For vulnerability assessment, you will deploy the agent based on the Microsoft Defender for Cloud recommendation indicating that your machine is missing a vulnerability assessment. The **Add Data Source** section of this page allows you to:

- **Onboard a non-Azure machine** In this scenario, you will need to select the workspace in which the Log Analytics (LA) agent will report to, Then you will need to obtain the workspace ID and key, deploy the agent to the server, and configure it to use the workspace ID and key based on your workspace's selection.
- **Connect to a SIEM platform** In this scenario, you need to configure an Azure Event Hub, stream the data from Microsoft Defender for Cloud to this Event Hub, and configure the SIEM to obtain the info from the Event Hub using a SIEM connector. The SIEM connector will vary according to the supported vendor (Splunk, ArcSight, QRadar, or Palo Alto). Keep in mind that you don't need to use an Event Hub if you are connecting Azure Defender with Azure Sentinel. In this case, you just need to use the Microsoft Defender for Cloud connector in Microsoft Sentinel.
- **Azure Web Application Firewall (WAF)** In this scenario, the goal is to surface the Azure WAF logs in the Microsoft Defender for Cloud Security Alerts Dashboard. Note that this integration only works for WAF v1.

Configure automated onboarding for Azure resources and data collection

PaaS-related resources in Azure don't require an agent to work, which means that as long as you have the Microsoft Defender for Cloud plan enabled on the subscription level, the subsequential resources will automatically have Microsoft Defender for Cloud enabled on them. For example, if the technical requirement is to have Defender for Storage enabled on all existing and new storage accounts, you just need to enable Defender for Storage at the subscription level.

As mentioned earlier in this chapter, when dealing with Azure VMs (IaaS scenario), you will need to install the LA Agent. For Azure VMs, this agent can be auto-provisioned based on the auto-provisioning settings that were configured at the subscription level. To change these settings, follow these steps:

1. Open **Azure portal** and sign in with a user who has **Security Admin** privileges.
2. In the left navigation menu, click **Defender for Cloud**.
3. In the Security Center's left navigation menu, under **Management**, click the **Environment settings** option.
4. Click the subscription for which you want to review the auto-provisioning settings.
5. In the **Settings** section on the left, click **Auto Provisioning**. The **Auto Provisioning** settings appear, as shown in Figure 2-8.

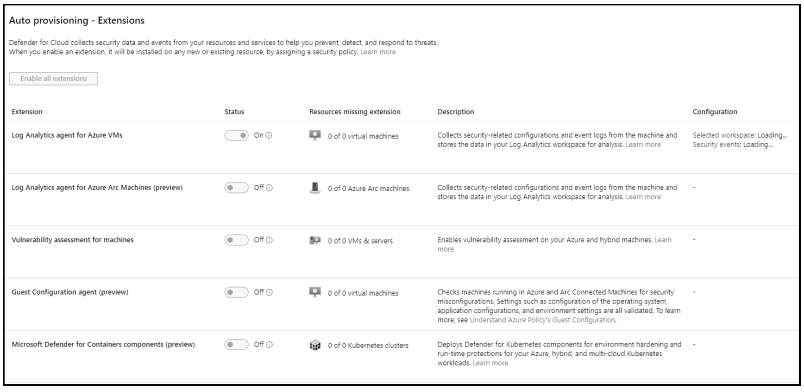

FIGURE 2-8 Auto Provisioning settings in Defender for Cloud

6. In the **Configuration** section for the **Log Analytics Agent For Azure VMs**, click **Edit Configuration**.
7. In the **Extension Deployment Configuration** blade shown in Figure 2-9, the default setting, **Connect Azure VMs To The Default Workspace(s) Created By Security Center**, allows Defender for Cloud to manage the workspace. Use this option if you can select another workspace to be used by Defender for Cloud. This is the preferred option when you have multiple subscriptions and want to centralize the workspace.

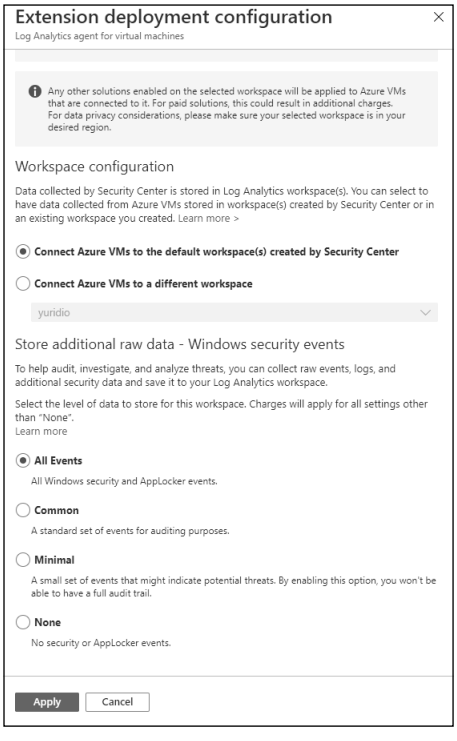

FIGURE 2-9 Options to control the workspace and data collection

NOTE **AUTO-PROVISIONING AGENT ON VMSS AND KUBERNETES**

At the time that this book was written, the Auto-Provisioning agent was not available for VM Scale Set (VMSS) and Azure Kubernetes. To install the agent on those services, you need to configure an Azure Policy to deploy it.

In the **Store Additional Raw Data** section, you can configure the level of data collection granularity for Windows systems. Each setting will determine the type of events that will be collected. If you are using a Group Policy Object (GPO) to configure your servers where the agent will be installed, we recommended that you enable the `Process Creation Event 4688` audit policy and the `CommandLine` field inside event `4688`. Audit Process Creation determines whether the operating system generates audit events when a process is created (starts). Information includes the name of the program or the user who created the process. Following is a summary of what each option collects:

- **All Events** If you select this option, all security events will be stored in your workspace.
- **Common** When you select this option, only a subset of events will be stored in your workspace. Microsoft considers these events—including login and logout events—to provide sufficient detail to represent a reasonable audit trail. Other events, such as Kerberos operations, security group changes, and more, are included based on industry consensus as to what constitutes a full audit trail.
- **Minimal** Choosing this setting results in the storage of fewer events than the **Common** setting, although we aren't sure how many fewer events or what types of events are omitted. Microsoft worked with customers to ensure that this configuration surfaces enough events that successful breaches are detected and that important low-volume events are recorded. However, logout events aren't recorded, so it doesn't support a full user audit trail.
- **None** This option disables security event storage.

To enable data collection for Adaptive Application Controls, Defender for Cloud configures a local AppLocker policy in Audit mode to allow all applications. This will cause AppLocker to generate events that are then collected and stored in your workspace. It is important to note that this policy will not be configured on any machines on which there is already a configured AppLocker policy. To collect Windows Filtering Platform Event ID 5156, you need to enable the Audit Filtering Platform Connection: `Auditpol /set /subcategory:"Filtering Platform Connection" /Success:Enable`.

MORE INFO **WINDOWS EVENT ID**

For details about the event ID that is collected for Windows, see *http://aka.ms/ascdatacollection*.

Connect on-premises computers

As explained previously, VMs that are in Azure will be provisioned automatically, which means that the monitoring agent will be automatically installed. If you need to onboard on-premises computers, you will need to install the agent manually. Follow the steps below to onboard non-Azure computers or VMs:

1. Open **Azure portal** and sign in with a user who has **Security Admin** privileges.
2. In the left navigation menu, click **Defender for Cloud**.
3. In the Defender for Cloud left navigation menu, under **General**, click the **Getting Started** option and click the **Get Started** tab.
4. Under **Add Non-Azure Computers**, click the **Configure** button, as shown in Figure 2-10.

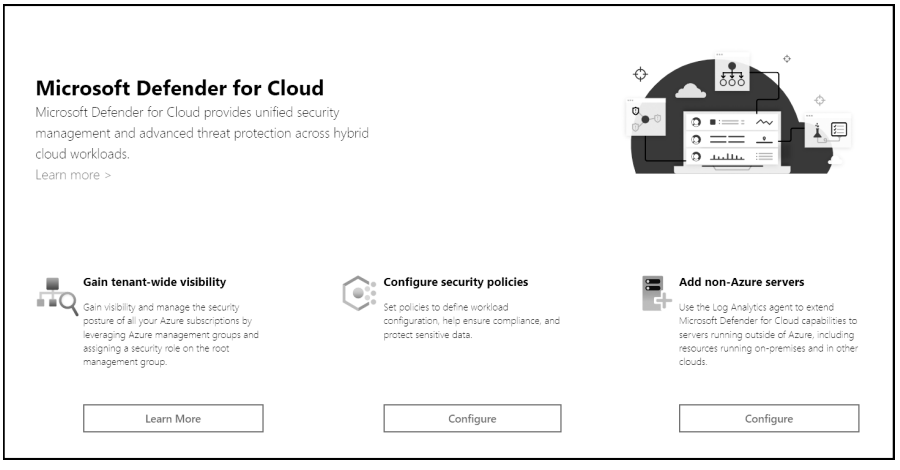

FIGURE 2-10 Option to onboard non-Azure computers

5. In the **Add New Non-Azure Computers** blade, select the workspace in which you want to store the data from these computers, and before onboarding any computer, make sure to click **Upgrade** to upgrade the Workspace to Microsoft Defender for Cloud, as shown in Figure 2-11.

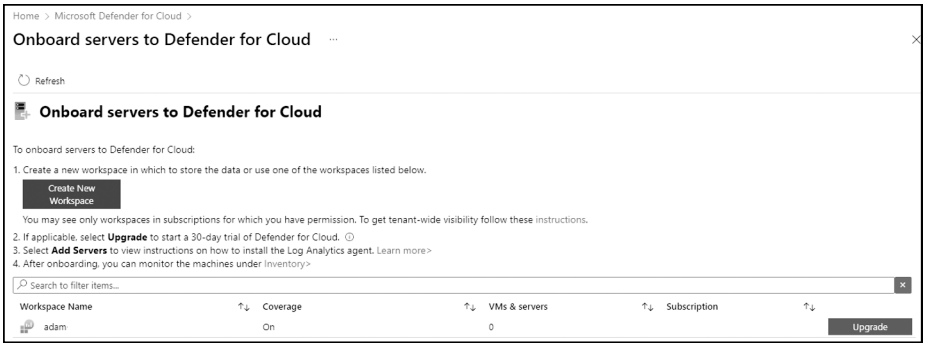

FIGURE 2-11 Upgrading the workspace to Microsoft Defender for Cloud

6. If the **Upgrade** button did not change to **+ Add Servers**, click the **Refresh** button, and you should see the **+ Add Servers** button, as shown in Figure 2-12. Click **Add Servers** to proceed.

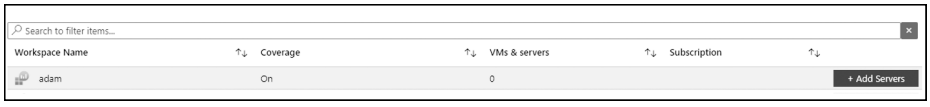

FIGURE 2-12 Adding servers to the workspace

7. Once you click the **+ Add Servers** button, the **Agents Management** page appears, as shown in Figure 2-13.

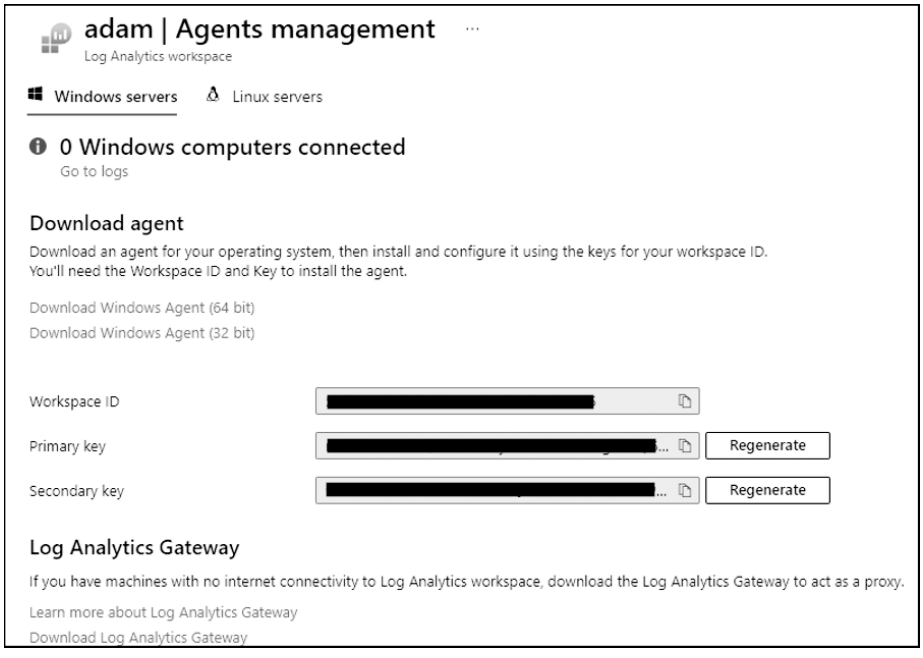

FIGURE 2-13 Agents Management

8. On this page, click the appropriate Windows agent (64-bit or 32-bit version). If you are installing the agent on a Linux operating system, click the **Linux Servers** tab and follow the instructions from there. Make sure to copy the **Workspace ID** and **Primary Key** values to the clipboard; you will need those values when installing the agent on the target system.

9. When you finish downloading it, you can close the Defender for Cloud dashboard (close your browser) and copy the agent installation file to a shared network location where the client can access it.

For this example, the agent installation will be done on an on-premises Windows Server 2016 computer, though the same set of procedures apply to a non-Azure VM located in a different cloud provider. Log in on the target system and follow the steps below to perform the installation:

1. Double-click in the `MMASetup-AMD64.exe` file, and if the **Open File—Security Warning** dialog appears, click **Run**.
2. If the **User Access Control** dialog appears, click **Yes**.
3. On the **Welcome To The Microsoft Monitoring Agent Setup Wizard** page, click **Next**.
4. Read the **Microsoft License Terms** and click **I Agree**.
5. In the **Destination Folder** page, leave the default selection and click **Next**. The **Agent Setup Options** page appears, as shown in Figure 2-14.

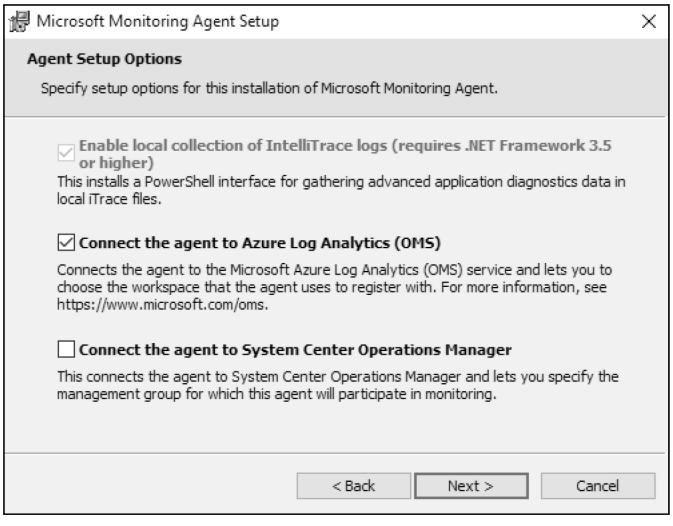

FIGURE 2-14 Selecting the target service

6. Select **Connect The Agent To Azure Log Analytics (OMS)**, as shown in Figure 2-14, and click **Next**. The **Azure Log Analytics** page appears, as shown in Figure 2-15.
7. On this page, you need to enter the **Workspace ID** and **Workspace Key** that were obtained in step 8 of the previous procedure. Notice that the primary key should be entered in the **Workspace Key** field. If this computer is behind a proxy server, you need to click the **Advanced** button and provide the Proxy URL and authentication if needed. Once you finish filling in these options, click **Next**.

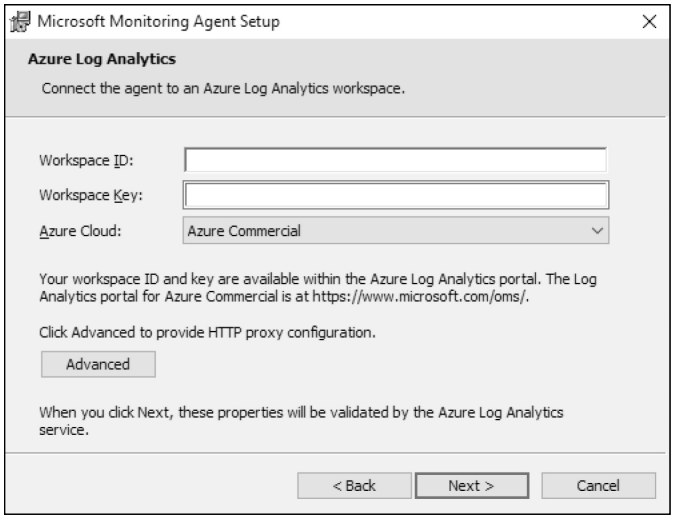

FIGURE 2-15 Providing the workspace ID and primary key

8. On the **Microsoft Update** page, select **Use Microsoft Update For Updates (Recommended)** and click **Next**.
9. On the **Ready To Install** page, review the summary field and click **Install**.
10. The **Installing The Microsoft Monitoring Agent** page appears, and the installation proceeds.
11. Once the installation is finished, the **Microsoft Monitoring Agent Configuration Completed Successfully** page appears. Click **Finish**.

You can also perform this installation using the command-line interface (CLI). Use the following code:

```
MMASetup-AMD64.exe /Q:A /R:N /C:"setup.exe /qn ADD_OPINSIGHTS_WORKSPACE=1 OPINSIGHTS_
WORKSPACE_AZURE_CLOUD_TYPE=0 OPINSIGHTS_WORKSPACE_ID=<yourworkspaceID> OPINSIGHTS_
WORKSPACE_KEY=<yourworkspaceprimarykey> AcceptEndUserLicenseAgreement=1"
```

Most of the parameters that you saw in the agent installation are self-explanatory. The only one that isn't immediately obvious is the `OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE` parameter, which is the cloud environment specification. The default is `0`, which represents the Azure commercial cloud. You should only use `1` if you are installing the agent in an Azure government cloud.

It can take some time for this new non-Azure computer to appear in Defender for Cloud. If you want to validate the connectivity between this computer and the workspace, you can use the `TestCloudConnection` tool. On the target computer, open the command prompt and navigate to the `\Program Files\Microsoft Monitoring Agent\Agent` *folder*. From there, execute the `TestCloudConnection.exe` command, and if the connectivity is working properly, you should see all tests followed by this message: `Connectivity test passed for all hosts for workspace id <workspace id>`.

Connect AWS cloud resources

For Azure Defender to connect with AWS, the target AWS account must have AWS Security Hub enabled on it. AWS Security Hub has a cost associated to it, which varies according to the number of accounts and regions where it is enabled.

Once the AWS connector is operational, you will start seeing security recommendations for AWS appearing in the Security Center Recommendations Dashboard. However, before configuring the AWS connector, you will need to: do the following:

1. Access to an AWS account
2. To activate Defender for Containers plan, you will need the following:
   - At least one Amazon EKS cluster with permission to access to the EKS K8s API server.
3. To activate Defender for servers plan, you will need the following:
   - Microsoft Defender for servers enabled on your subscription
   - An active AWS account, with EC2 instances.
   - Azure Arc for servers installed on your EC2 instances.

With those steps in place, you are ready to configure the Cloud Connector. If you also want to onboard servers that are in AWS, you will need to ensure that the following three tasks are done before configuring the cloud connector in Azure Defender:

1. Install the AWS Systems Manager on your Servers (EC2 instance) that reside in AWS. For instructions, see *http://aka.ms/ascbookaws*.
2. Configure this Server (EC2 Instance) to use Azure Arc. For instructions, see *http://aka.ms/ascbookarc*.
3. In Azure, make sure to create a service principal that will be used for Azure Arc. To configure that service principal, follow the steps from this article: *http://aka.ms/ascbookspn*.

Now that all prerequisites are fulfilled, you can follow the steps below to start the configuration of the AWS connector in Defender for Cloud:

1. Open **Azure portal** and sign in with a user who has ownership privileges in the subscription.
2. In the left navigation menu, click **Defender for Cloud**.

3. In the Security Center's left navigation menu, under **Management**, click the **Environment settings** option, click **Add environment** button, click **Amazon Web Services** option. The **Add account** page appears, as shown in Figure 2-16:

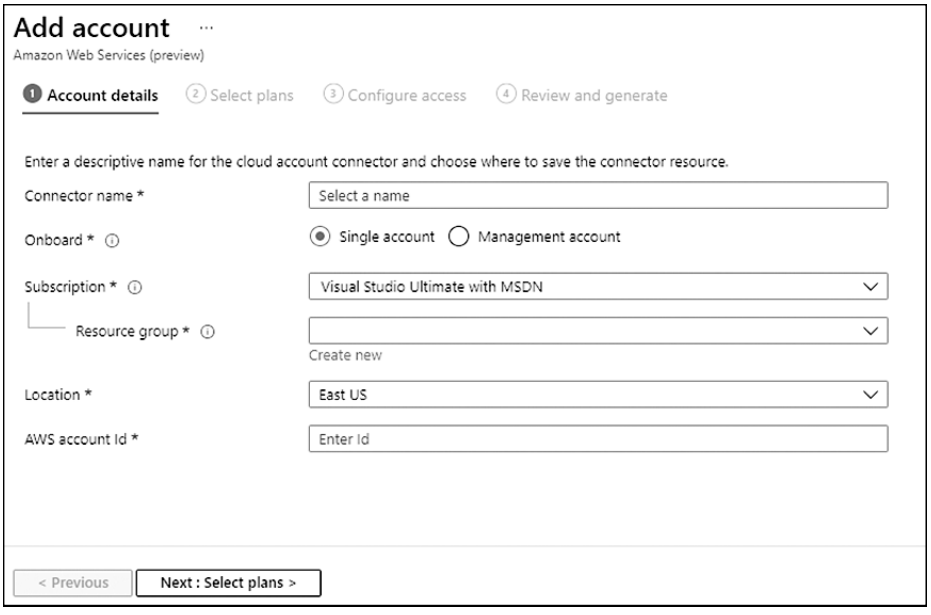

FIGURE 2-16 Connect AWS Account

4. In the **Account details** type the connector name in **Display name** field.
5. In the **Onboard** section select the type of account, in this case select **Single account**, select the appropriate **Subscription** from the drop down menu, the **Resource group**, the **Location** and **AWS account id**. Click **Next: select plans** button to continue. Figure 2-17 shows an example of the next page in this wizard.

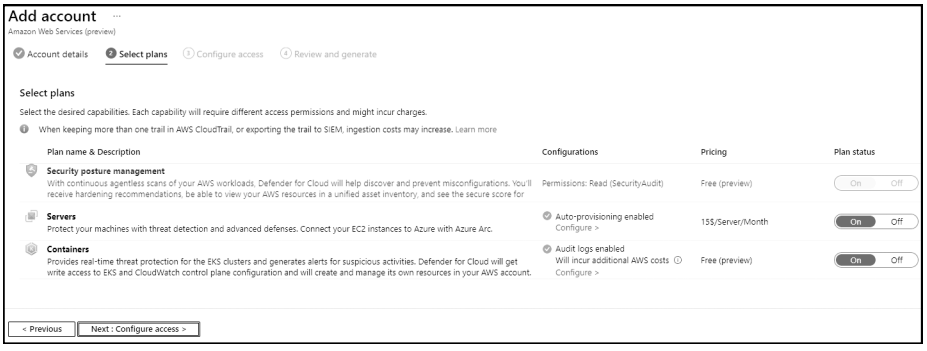

FIGURE 2-17 Options to enable different Defender for Cloud plans in the connector

6. In the **Select plans** page, you will have the option to enable Defender for Servers and Defender for Containers plans. For this example, leave only **Security posture management** selected and click **Next:Configure access** button. You may receive a pop up message emphasizing that you should enable Defender for Servers for full protection, click **Deny** button to continue.
7. Follow the steps shown in the screen, see example from Figure 2-18, to download the template and run in AWS.

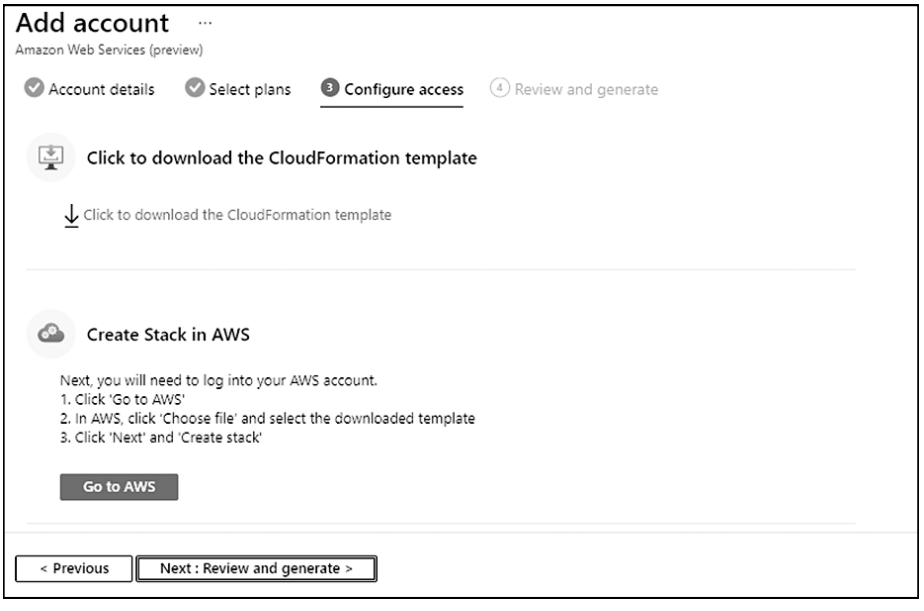

FIGURE 2-18 Final steps to prepare the AWS environment

After some time, you will be able to see recommendations for your AWS account. In the search box, you can type **AWS**, and you will see all AWS-related recommendations, as shown in Figure 2-19.

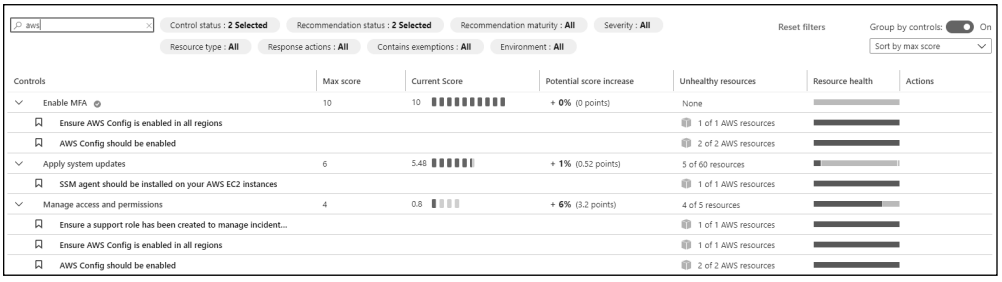

FIGURE 2-19 AWS-related recommendations

At this point, your Azure Arc machines will be discovered, but you still need to install the Log Analytics agent on those machines. There is a specific recommendation for that, as shown in Figure 2-20.

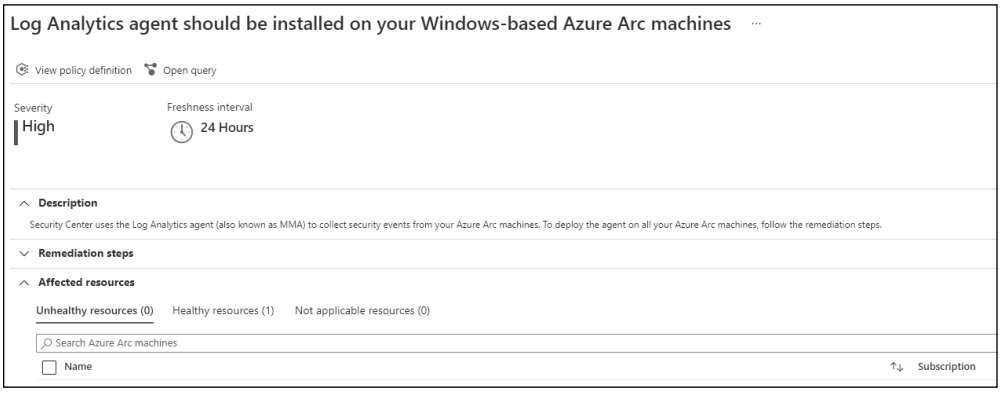

FIGURE 2-20 Recommendation to install the Log Analytics agent on the Azure Arc machine

You can leverage the **Quick Fix** feature to deploy the agent to this Azure Arc machine quickly. You just need to select the server and click the **Remediate** button. As mentioned in the freshness interval description, it might take 24 hours for this remediation to take effect.

Connect GCP cloud resources

When connecting your GCP accounts to specific Azure subscriptions, you need to take into consideration the Google Cloud resource hierarchy. Based on this hierarchy, you can

- Connect your GCP accounts to ASC at the organization level
- Connect multiple organizations to one Azure subscription
- Connect multiple organizations to multiple Azure subscriptions

> ***IMPORTANT*** **ALL PROJECTS ADDED**
>
> **When you connect an organization, all projects within that organization are added to Microsoft Defender for Cloud.**

Follow the steps below to start the configuration of the GCP connector in Microsoft Defender for Cloud:

1. Open **Azure portal** and sign in with a user who has ownership privileges in the subscription.
2. In the left navigation menu, click **Defender for Cloud**.
3. In the Security Center's left navigation menu, under **Management**, click the **Environment settings** option, click **Add environment** button, click Google Cloud Platform option and the **Create GCP connector** appears as shown in Figure 2-21.

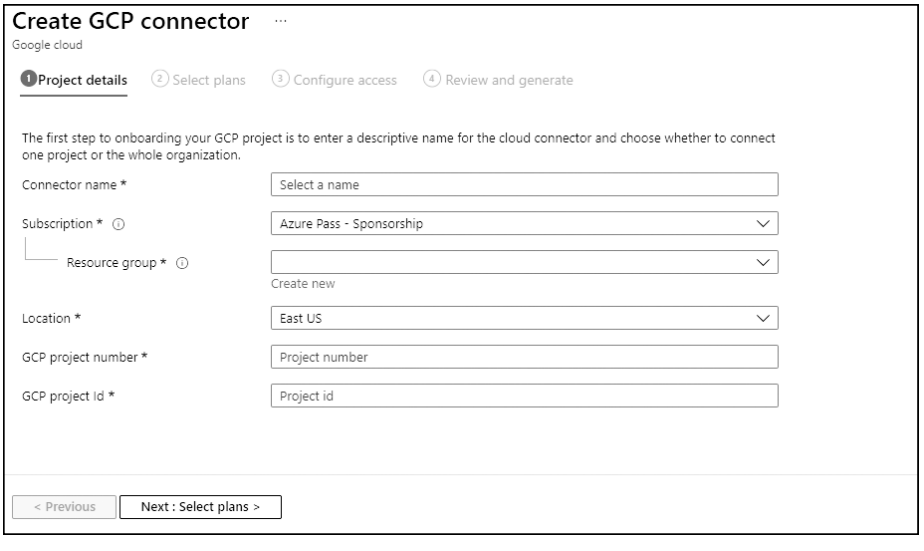

FIGURE 2-21 Connect GCP Account

4. In the **Connector name**, type the name for the connector.
5. Select the appropriate **Subscription** in the drop down list and the appropriate **Resource group**.

6. Select the appropriate **Location** in the drop down list and in the **GCP project Id** type the identification number for the Google Project. Click **Next: Select plans** button to continue.
7. In the **Select plans**, the experience is similar to AWS, leave the default selection and click **Next: configure access** to continue.
8. In the **Configure access**, click Copy button, click **GCP Cloud Shell button**, paste the script and run. Once if finish to run, navigate back to the wizard, click **Next: Review and generate** button and conclude the configuration by clicking **Create** button.

The security recommendations for your GCP resources will appear in the Defender for Cloud Recommendations Dashboard and in the regulatory compliance dashboard between 5 and 10 minutes after the onboard process is completed. To view only the GCP recommendations, you can also change the **Environment** filter in the security Recommendations Dashboard to filter for **GCP** only, as shown in Figure 2-22.

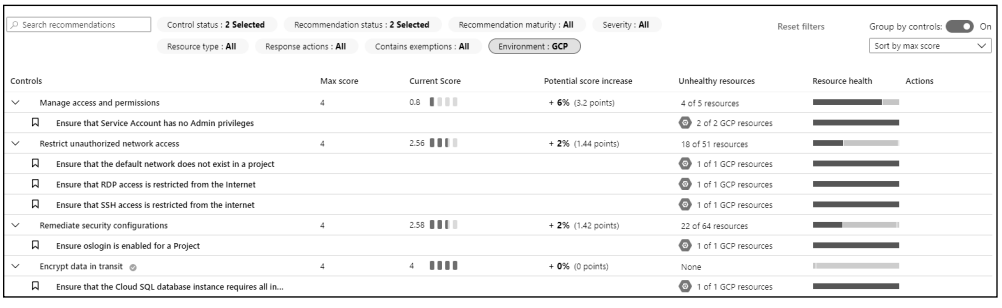

FIGURE 2-22 GCP recommendations

EXAM TIP

When studying for the SC-200 exam, make sure you know the exact order of operations that must be done in AWS and GCP before going to Microsoft Defender for Cloud to configure the connectors.

Skill 2-3: Manage Microsoft Defender for Cloud alert rules

For the Security Operations Center (SOC) to be effective, it needs to have high-level, quality data to be analyzed. For some workloads, the ingestion of raw data is desirable. However, over time, SOC Analysts became too busy rationalizing the raw data to identify indications of compromise. When using Microsoft Defender for Cloud, you will take advantage of a high-level, quality alert that already provides the needed information about an attack and how to respond to it. This section of the chapter covers the skills necessary to manage Microsoft Defender for Cloud alert rules according to the Exam SC-200 outline.