LAB06: Gain security insights from your Arc-enabled servers using Microsoft Sentinel

Student Lab Manual

Table of Contents

===

Exercise 1 - Configure data collection on Sentinel

Objective

This exercise will walk you through how to enable data collection on Sentinel for Windows security events.

Estimated Time to Complete This Lab

20 minutes

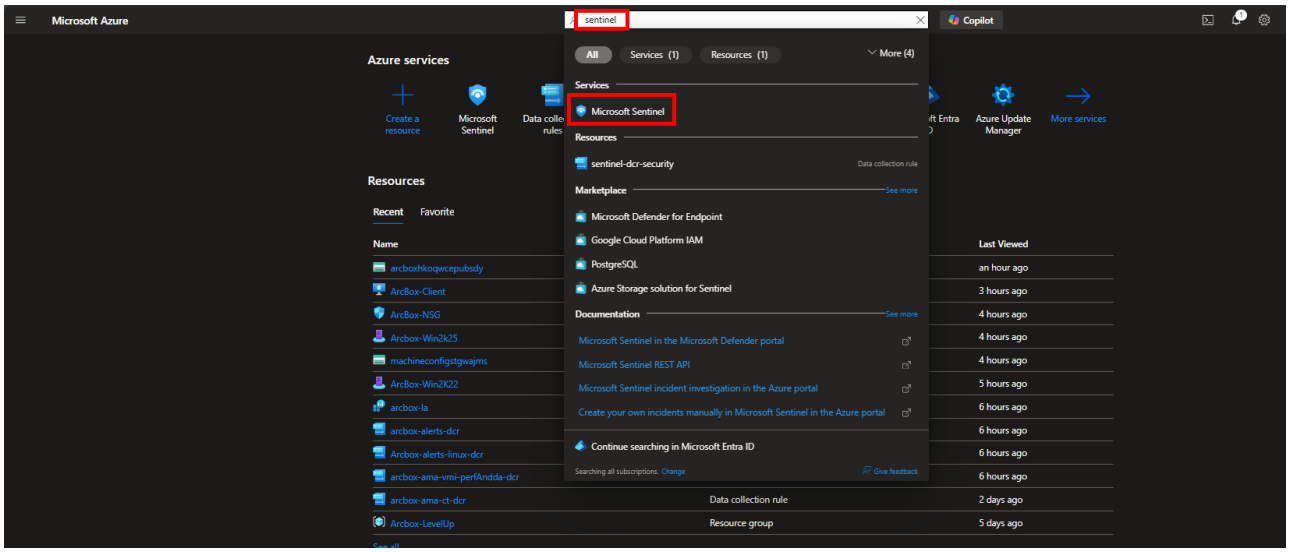
Explanation

In this exercise, you will learn how to enable data collection on Sentinel for Windows security events, simulate failed logins and visualize them in Sentinel.

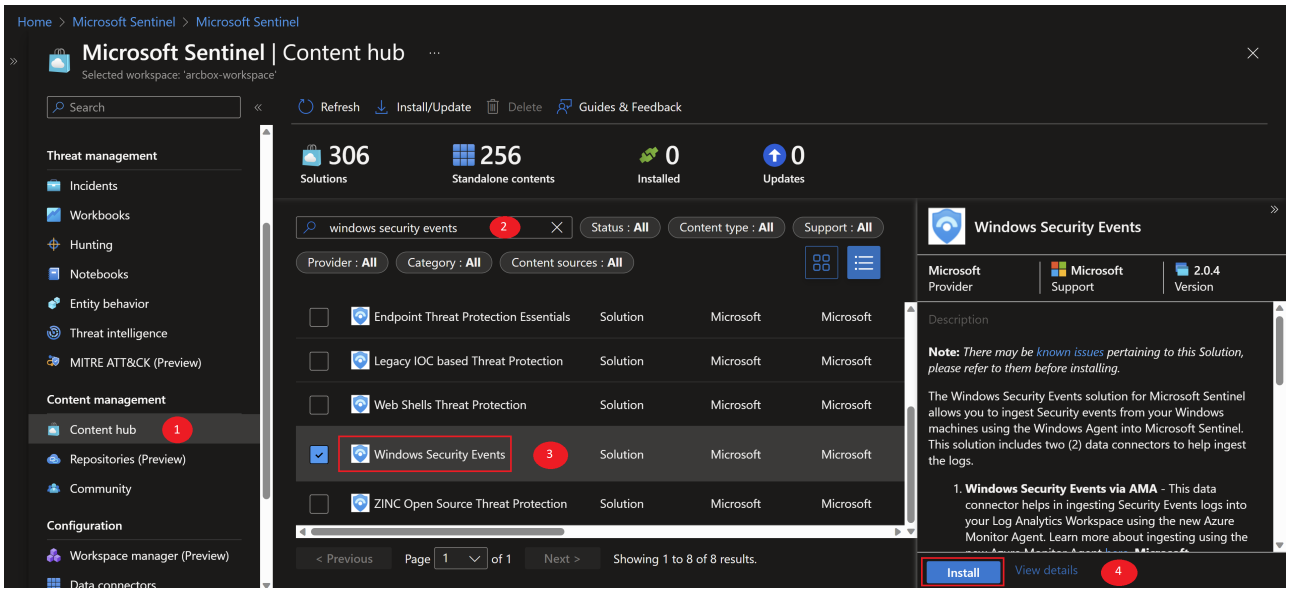
===

Task 1: Configure data collection on Sentinel

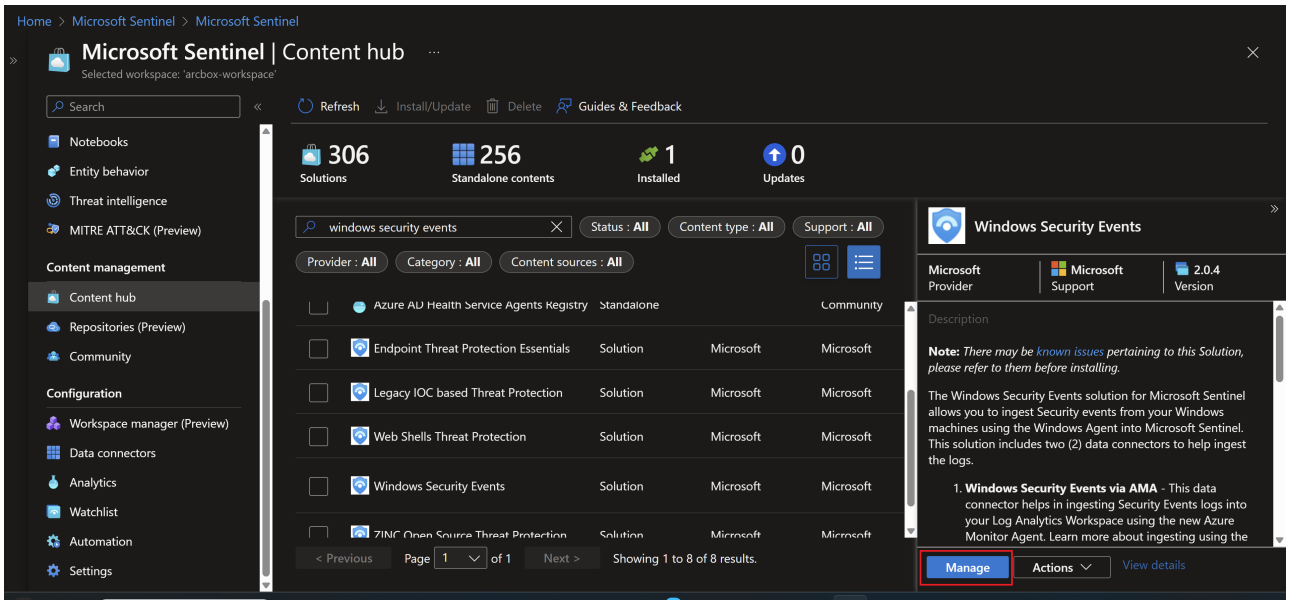
1. [] In the Azure Portal, search for *Sentinel*



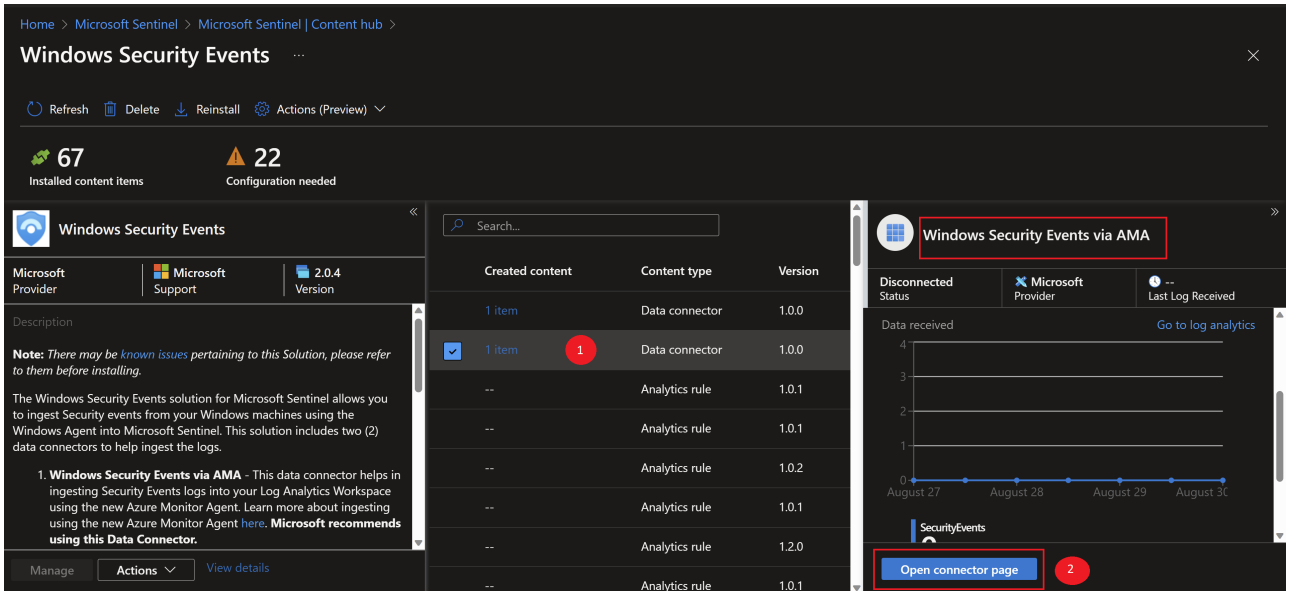
2. [] Click on "Content Hub" and search for "Windows Security Events" and install it.



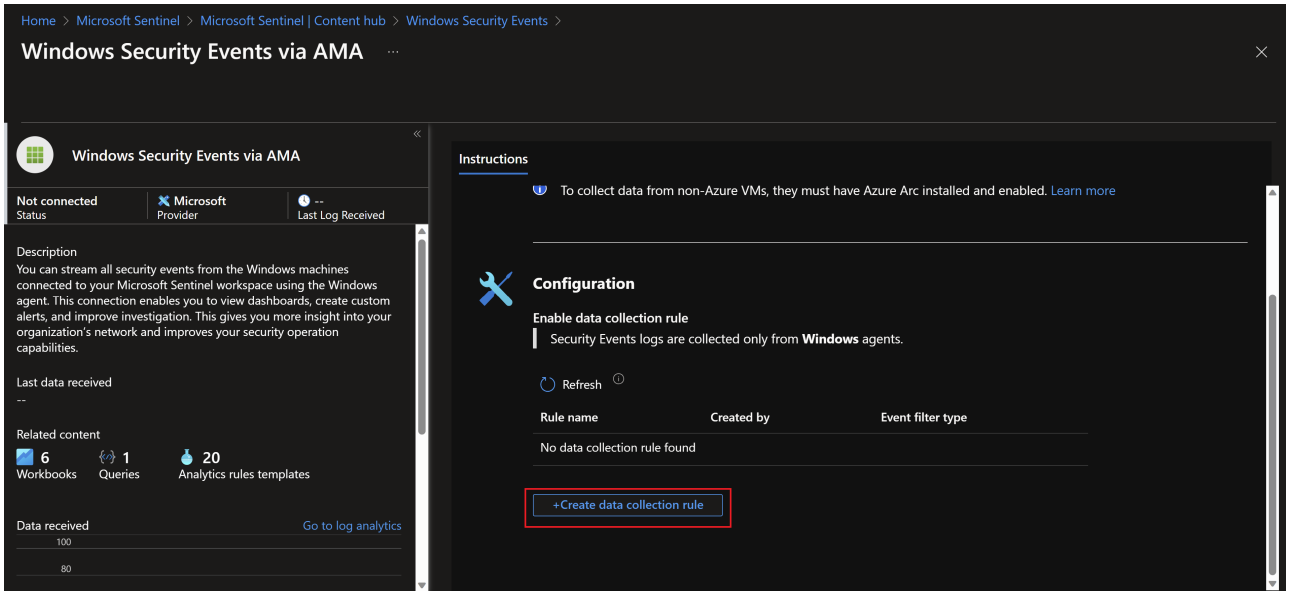
3. [] After installation, click on "Manage" to configure the collector.



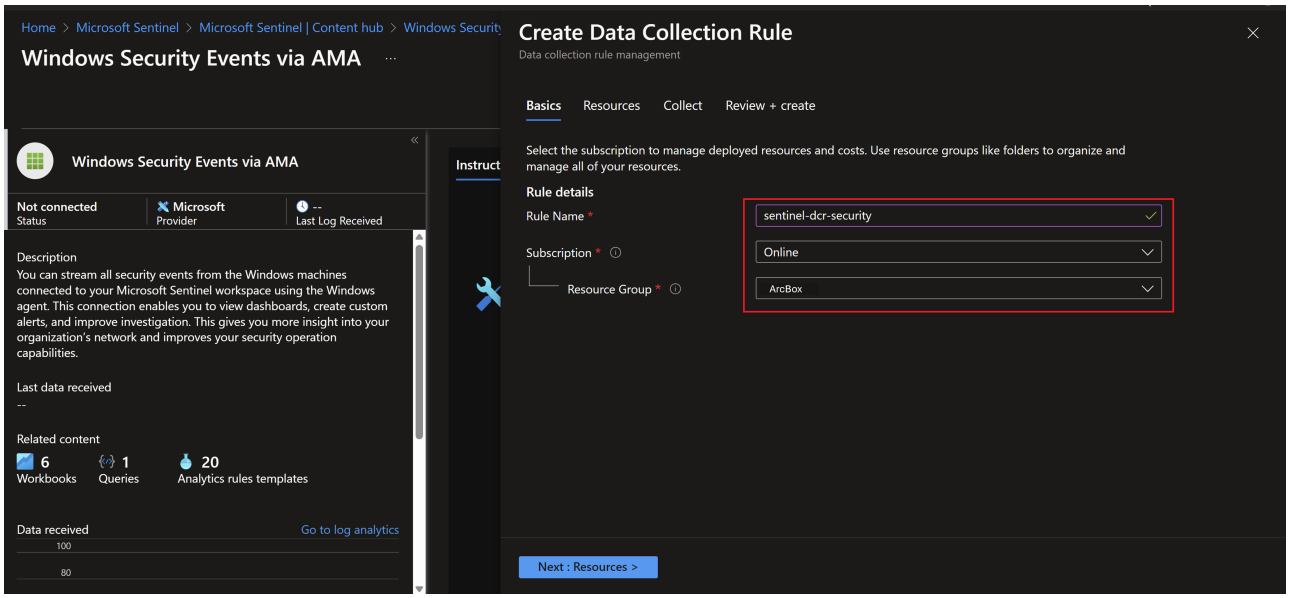
4. [] Select the data connector and make sure you've selected the *Windows Security Events via AMA* and click "open connector page".



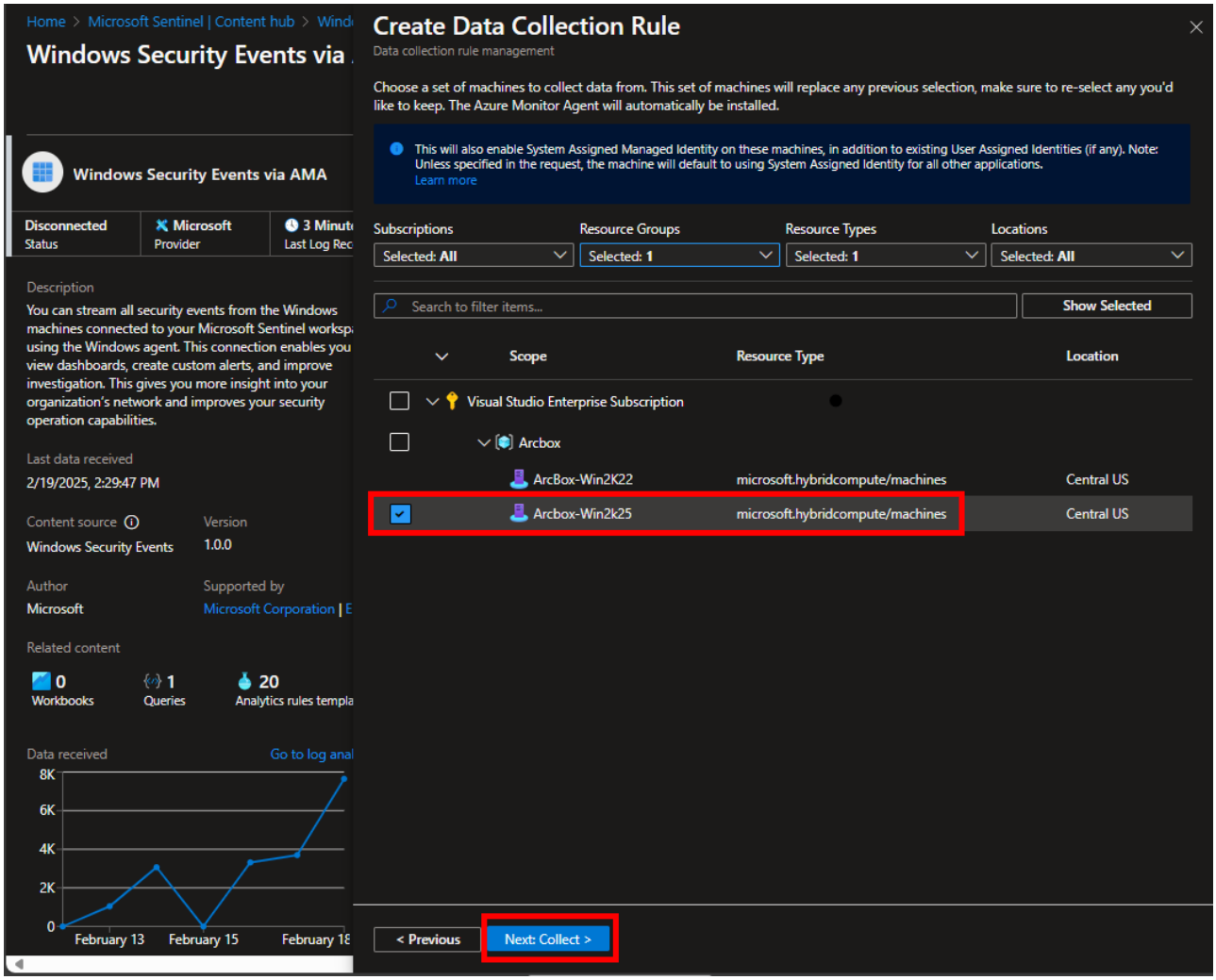
5. [] Create a new data collection rule.



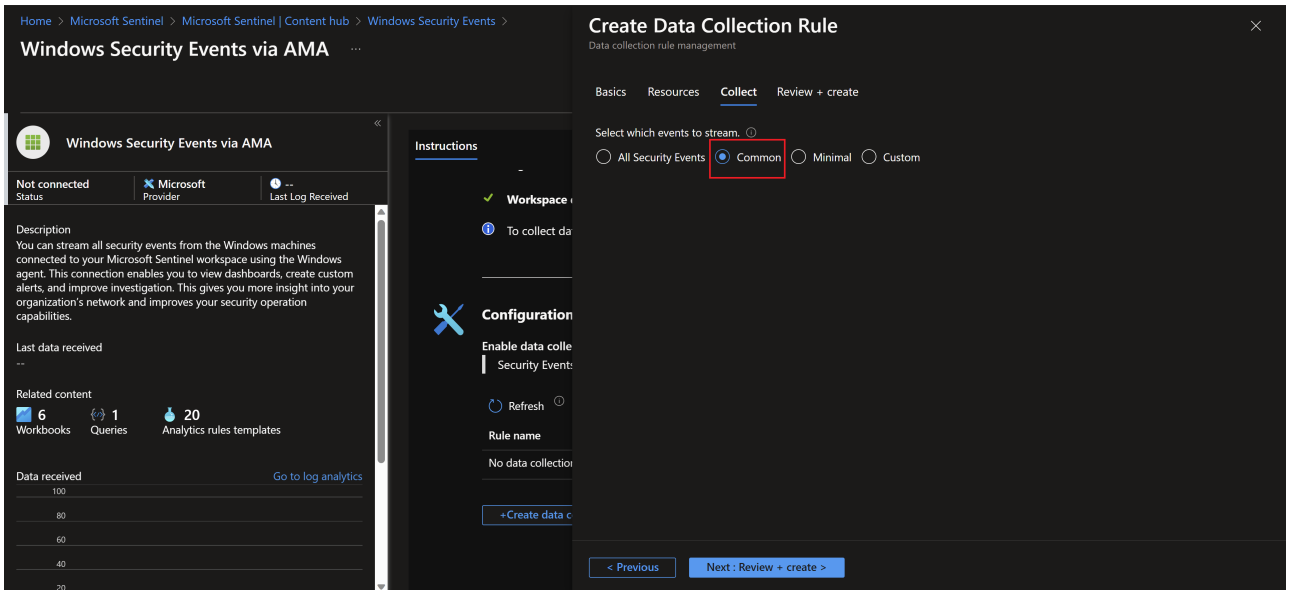
6. [] Provide a name for the data collection rule and select the same resource group where you've deployed this level-up lab.

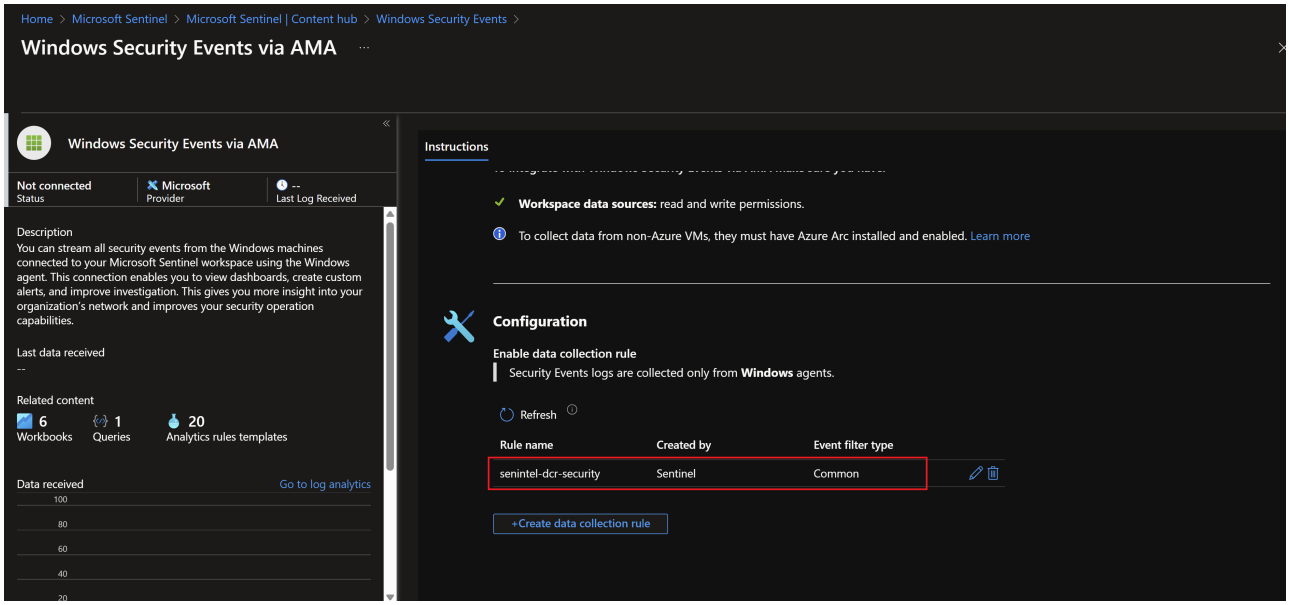


7. [] Select one or multiple Windows Arc-enabled machines.



8. [] Select the "Common" event type and create the data collection rule.





Task 1 has been completed

===

Exercise 2 - Simulating and viewing security events

Objective

This exercise will walk you through how to view Windows security events in Sentinel.

Estimated Time to Complete This Lab

20 minutes

Explanation

In this exercise, you will learn how to leverage Sentinel to view failed logins using Windows security events data collection.

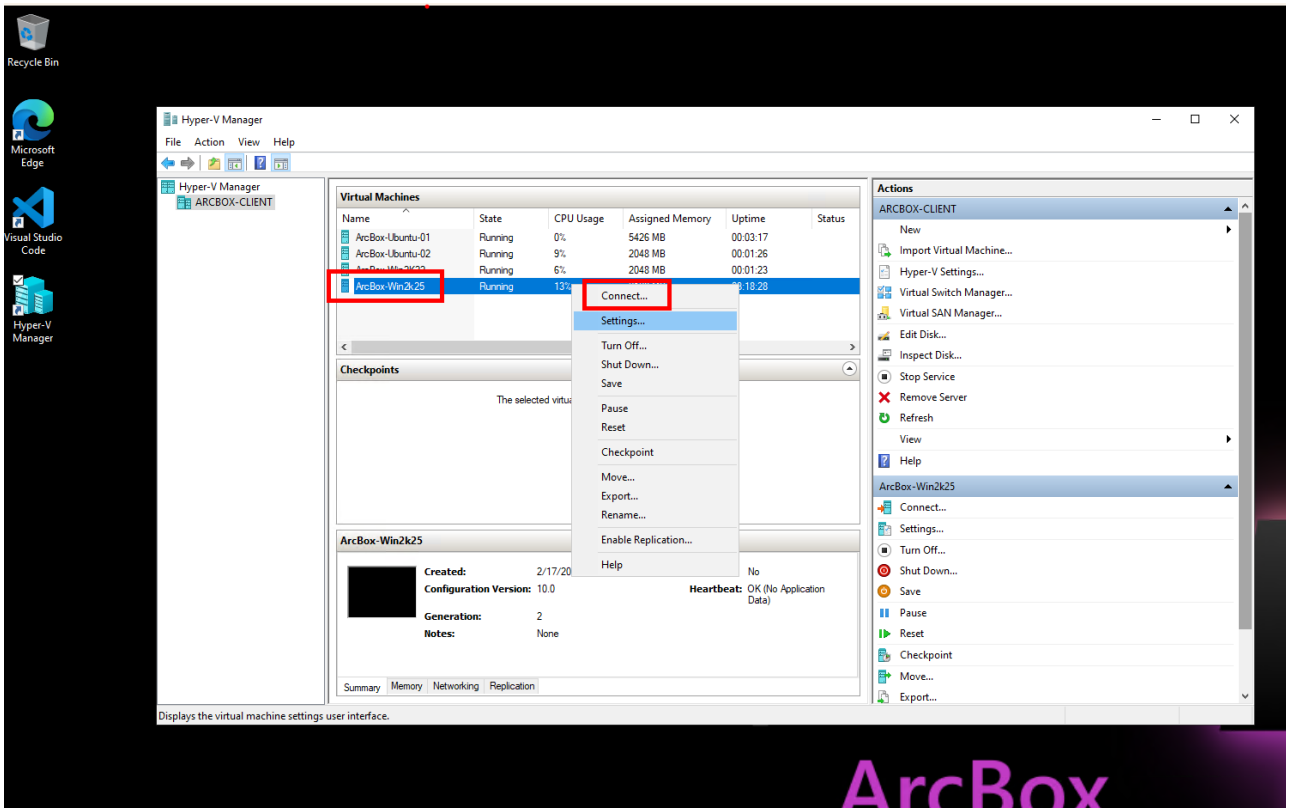
===

Task 1: Simulating-and viewing security events

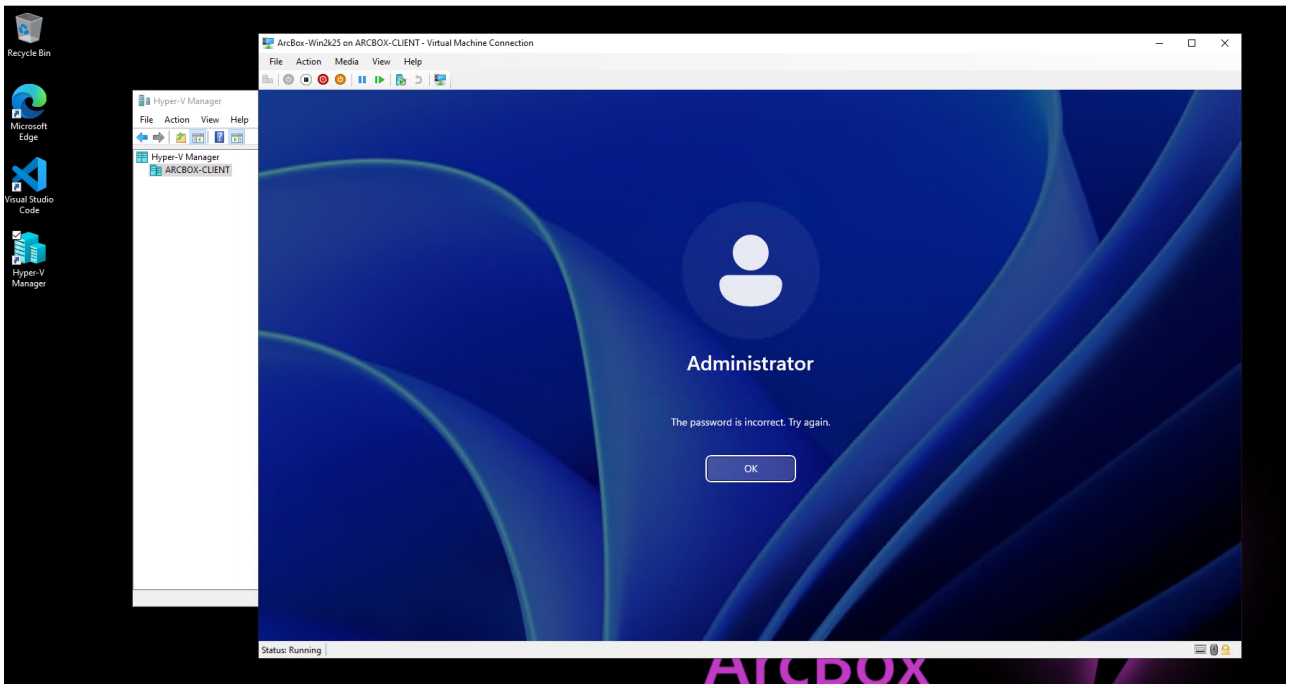
1. [] After configuring Sentinel, now we need to simulate some failed login attempts on one or more Windows Arc-enabled machines.

2. [] Connect to *ArcBox-Client* VM, and open the *Hyper-v manager*.

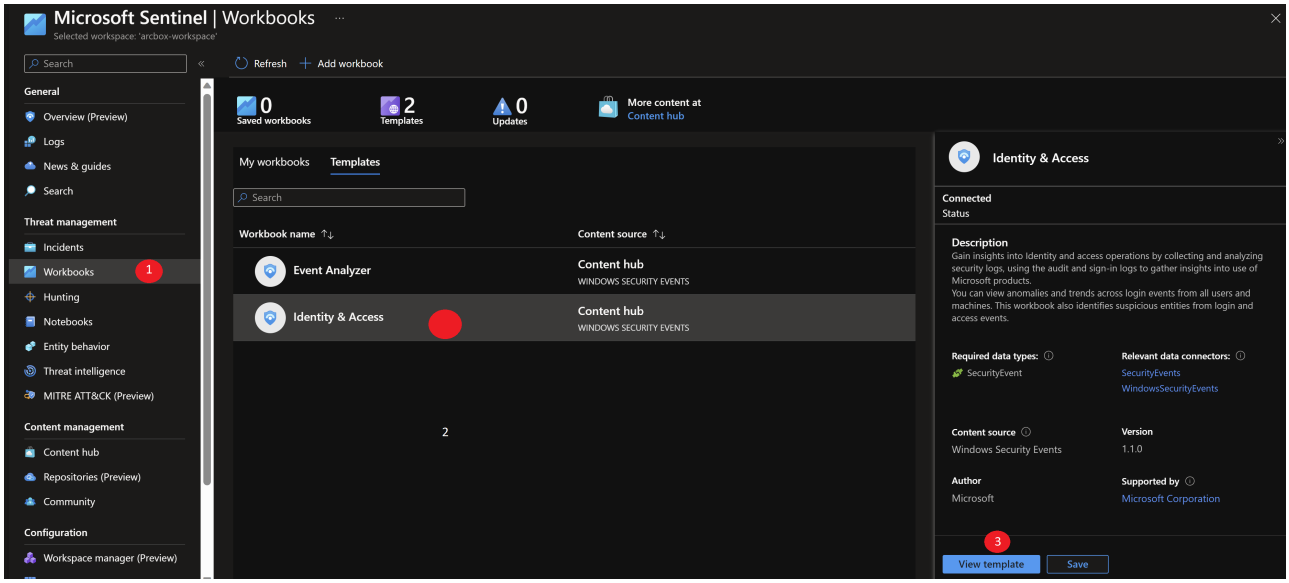
3. [] Right-click one of the Windows machines and connect to it.



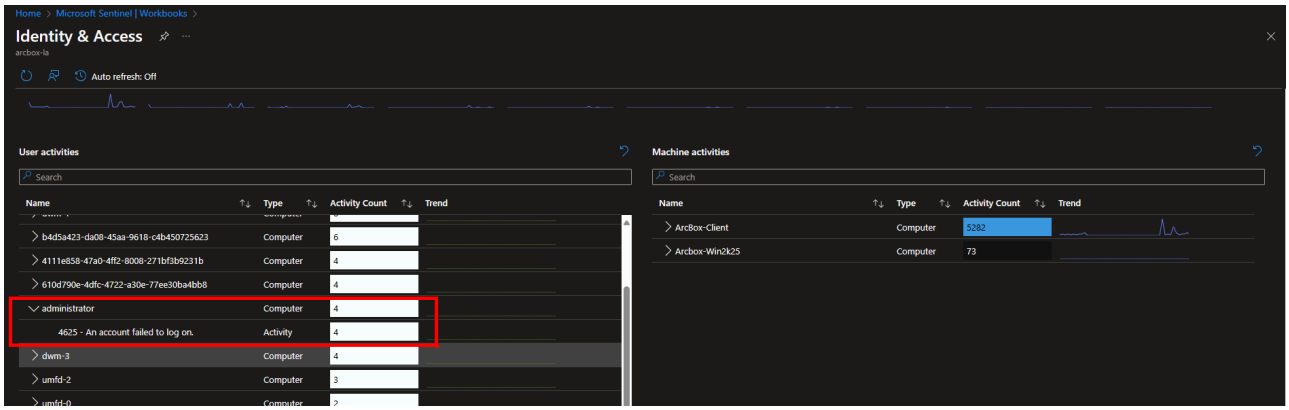
4. [] Simulate some failed login attempts by trying to login multiple times using an incorrect password.



5. [] After waiting for about 10-15 minutes for data to start getting ingested into the log analytics workspace, navigate to "Workbooks" and select the "Identity & Access" workbook.



6. [] Once data is being ingested, you will start seeing the failed login attempts in the workbook.



Task 1 has been completed

===

Congratulations, you have completed all tasks in this lab

Click **Next** for the next lab or **Go back to the main table of content**