

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

Task 1 - Configure data collection on Sentinel

Exercise 2 - Simulating and viewing security events

Task 1 - Simulating-and viewing security events

====

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

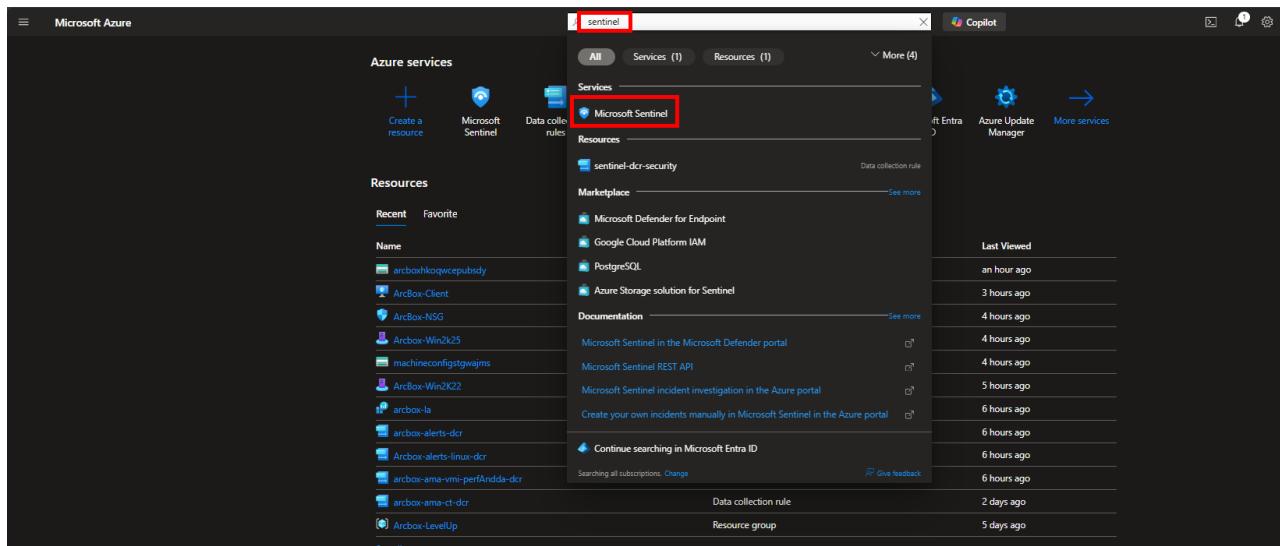
Explanation

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.

The screenshot shows the Microsoft Sentinel Content hub. The left sidebar has 'Content hub' selected and highlighted with a red circle containing the number '1'. The main area shows a search bar with 'windows security events' and a list of solutions. One solution, 'Windows Security Events', is highlighted with a red box and has a red circle with the number '3' next to it, indicating it is selected. To the right, a detailed view of the 'Windows Security Events' solution is shown, including its provider (Microsoft), support (Microsoft), and version (2.0.4). The 'Install' button is highlighted with a red box.

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

The screenshot shows the Microsoft Sentinel Content hub after the 'Windows Security Events' solution has been installed. The 'Content hub' item in the sidebar is still highlighted with a red circle containing '1'. The main area shows the same search results, but now the 'Windows Security Events' solution is listed with a green checkmark icon and the number '1' next to it, indicating it is installed. To the right, the detailed view of the solution includes a 'Manage' button, which is highlighted with a red box.

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

The screenshot shows the Microsoft Sentinel Content hub interface. On the left, there's a sidebar for 'Windows Security Events' with a 'Microsoft Provider' section. In the center, a table lists content items: 1 item (Data connector, 1.0.0), 2 Analytics rule (1.0.1, 1.0.1), 2 Analytics rule (1.0.2, 1.0.1), 2 Analytics rule (1.2.0, 1.0.1). On the right, a larger panel for 'Windows Security Events via AMA' is shown, featuring a status bar with 'Not connected', 'Microsoft Provider', and 'Last Log Received'. Below this is a chart titled 'Data received' showing values from 0 to 4 over dates from August 27 to August 30. At the bottom right of this panel is a button labeled 'Open connector page'.

5. [] Create a new data collection rule.

The screenshot shows the configuration page for the 'Windows Security Events via AMA' connector. It includes sections for 'Instructions' (warning about Azure Arc requirements) and 'Configuration'. Under 'Configuration', there's a 'Create data collection rule' button highlighted with a red border. The 'Related content' sidebar on the left shows 6 Workbooks, 1 Query, and 20 Analytics rules/templates.

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

Create Data Collection Rule
Data collection rule management

Basics **Resources** **Collect** **Review + create**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources.

Rule details

Rule Name * sentinel-dcr-security

Subscription * Online

Resource Group * ArcBox

Last data received --

Description You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Related content 6 Workbooks, 1 Queries, 20 Analytics rules templates

Data received 100 Go to log analytics

Next : Resources >

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

Create Data Collection Rule
Data collection rule management

Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other applications.
[Learn more](#)

Subscriptions	Resource Groups	Resource Types	Locations
Selected: All	Selected: 1	Selected: 1	Selected: All

Search to filter items... Show Selected

Scope	Resource Type	Location
Visual Studio Enterprise Subscription	microsoft.hybridcompute/machines	Central US
Arcbox		
Arbox-Win2k22	microsoft.hybridcompute/machines	Central US
<input checked="" type="checkbox"/> Arbox-Win2k25	microsoft.hybridcompute/machines	Central US

Last data received 2/19/2025, 2:29:47 PM

Content source 1 Version 1.0.0

Author Microsoft Supported by Microsoft Corporation | E

Related content 0 Workbooks, 1 Queries, 20 Analytics rules templates

Data received 8K Go to log anal

8K
6K
4K
2K
0 February 13 February 15 February 18

< Previous Next: Collect >

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

The screenshot shows the 'Create Data Collection Rule' wizard in Microsoft Sentinel. The current step is 'Collect'. In the 'Instructions' section, it says 'Select which events to stream.' with an info icon. Below are four radio button options: 'All Security Events', 'Common' (which is selected and highlighted with a red box), 'Minimal', and 'Custom'. The 'Configuration' section includes a 'Refresh' button, a 'Rule name' input field (set to 'No data collection'), and a '+Create data collection rule' button. At the bottom are navigation buttons: '< Previous' and 'Next : Review + create >'.

The screenshot shows the 'Windows Security Events via AMA' configuration page. The 'Event filter type' dropdown for the rule 'senintel-dcr-security' is highlighted with a red box. Other columns in the table include 'Rule name' (senintel-dcr-security), 'Created by' (Sentinel), and 'Event filter type' (Common). The rest of the page displays the Windows Security Events workspace details, including a description, status, and related content like workbooks, queries, and analytics rules templates.

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

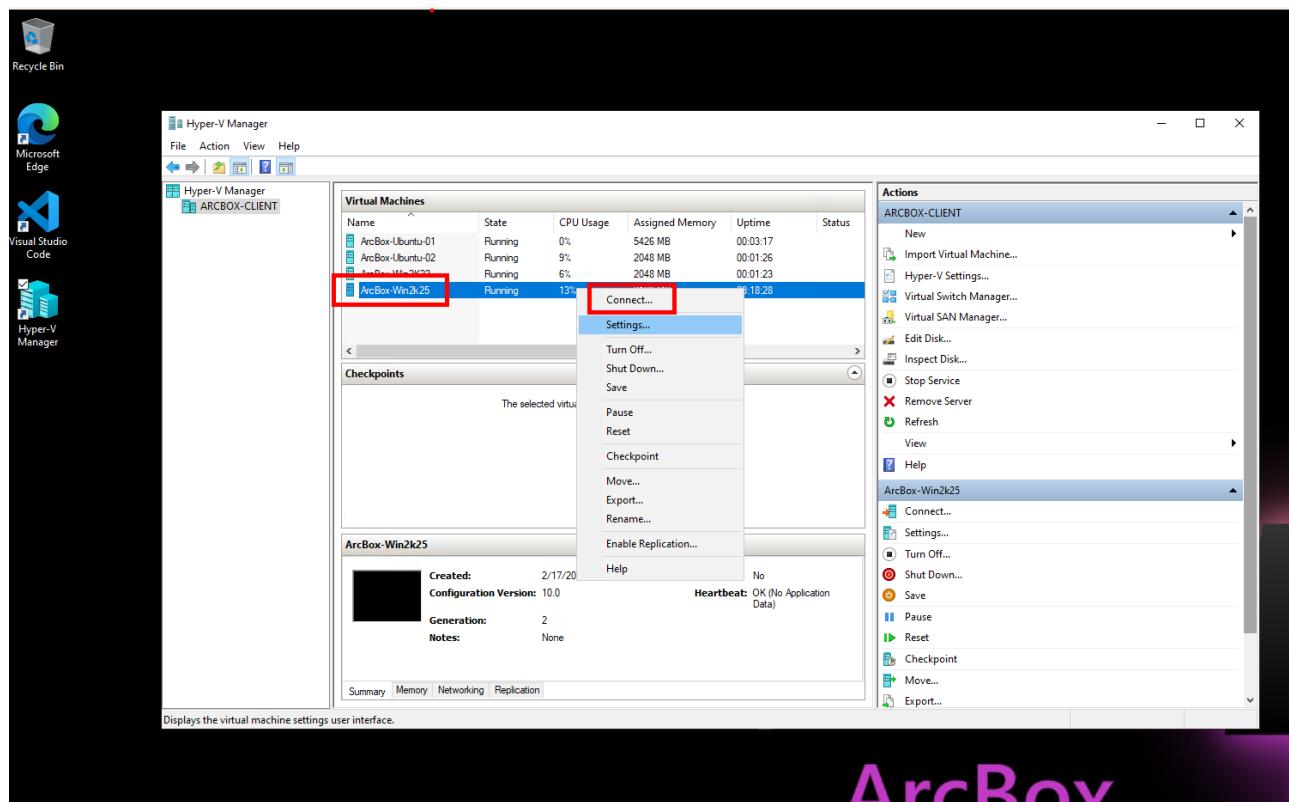
Explanation

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

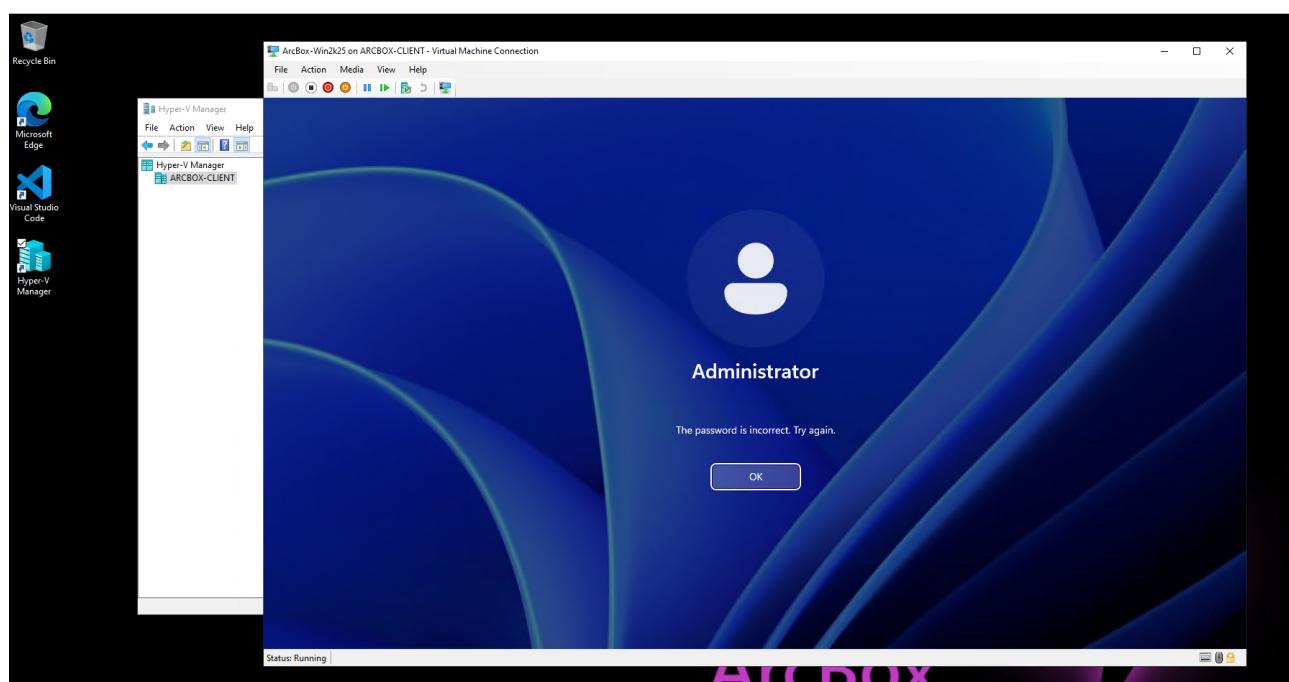
====

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.

The screenshot shows the Microsoft Sentinel Workbooks interface. On the left, there's a sidebar with categories like General, Threat management, Content management, and Configuration. Under Threat management, 'Workbooks' is selected, indicated by a red circle with the number '1'. In the main area, there are sections for 'My workbooks' and 'Templates'. The 'Identity & Access' template is highlighted with a red circle and has a red circle with '2' above it. To the right, there's a detailed view of the 'Identity & Access' template, including its description, required data types (SecurityEvent), content source (Windows Security Events), version (1.1.0), author (Microsoft), and supported by (Microsoft Corporation). A red circle with '3' is at the bottom right of this panel.

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

The screenshot shows the Microsoft Sentinel Identity & Access workbook. It has two main sections: 'User activities' on the left and 'Machine activities' on the right. The 'User activities' section shows a table with columns: Name, Type, Activity Count, and Trend. One row for 'administrator' is highlighted with a red box, showing an activity count of 4. The 'Machine activities' section shows a table with columns: Name, Type, Activity Count, and Trend. It lists several machines, with 'ArcBox-Client' having the highest activity count of 5282. A red box highlights the 'administrator' row in the User activities table.

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**