Installing and Configuring IBM QRadar with WinCollect for Log Collection

1. Introduction

IBM QRadar is a powerful SIEM (Security Information and Event Management) solution used to centralize and analyze security logs from various systems. This report documents the steps taken to install QRadar Community Edition (CE) on a virtual machine hosted on an Ubuntu machine and to set up WinCollect on a Windows machine to forward logs to QRadar for analysis.

2. Lab Requirements

Hardware

- Ubuntu machine with VMware Workstation installed
- Windows 10/11 or Windows Server machine

Software

- IBM QRadar Community Edition OVA file
- WinCollect Agent Installer

3. Installing QRadar CE on Ubuntu (via VM)

Step 1: Download QRadar CE

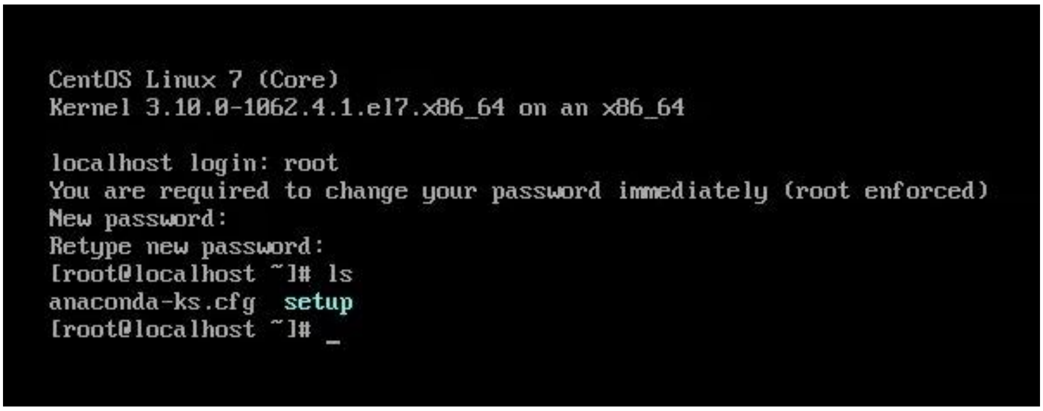
- Navigate to IBM Website
- Download the OVA image for QRadar CE

Step 2: Deploy the OVA

- Import the OVA into VMware
- Allocate the following resources:
  - RAM: 16 GB
  - CPU: 4 cores
  - Disk: 250 GB

Step 3: Initial Setup

- Start the VM and login using:
  - Username: root
  - Password: sword2025



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.4.1.el7.x86_64 on an x86_64

localhost login: root
You are required to change your password immediately (root enforced)
New password:
Retype new password:
[root@localhost ~]# ls
anaconda-ks.cfg  setup
[root@localhost ~]# _
```

- Run the configuration script:
- /opt/qradar/support/all_servers.sh
- Access the QRadar web interface at https://<192.168.1.11>
- Login with:
  - Username: admin
  - Password: sword2025
  - Entering new password
  - Sword2025@

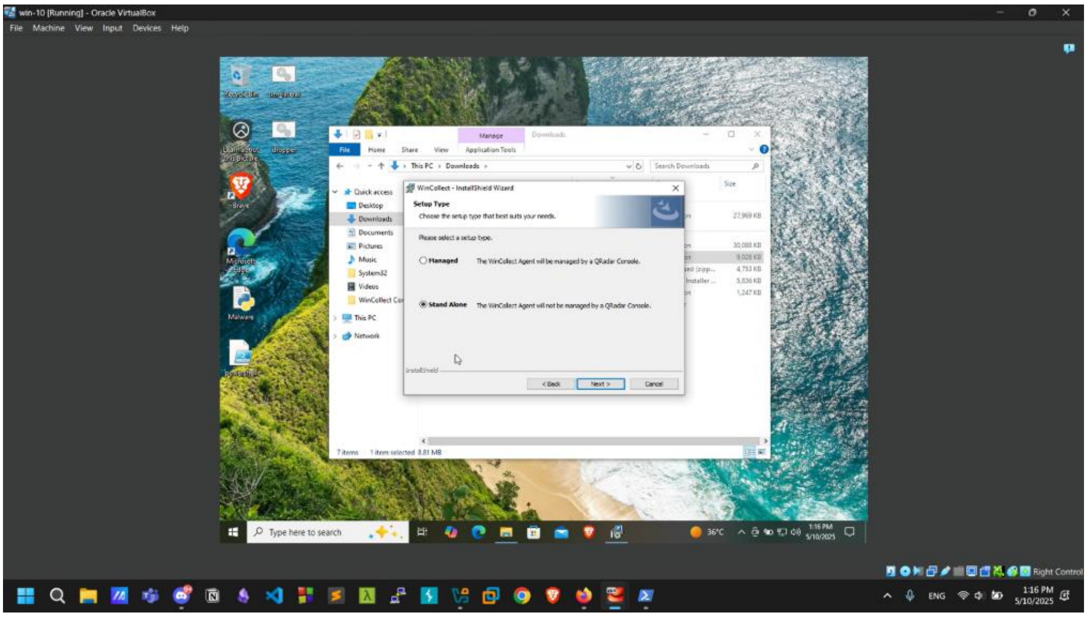
4. Installing WinCollect and Wincollect Stand alone Patch installer on Windows

Step 1: Download the WinCollect Agent and The patch installer

- From the QRadar GUI: Admin > WinCollect > Download Agent
- Alternatively, download from IBM Fix Central (requires IBM ID)

Step 2: Install WinCollect

- Run the installer on the Windows machine
- Choose installation type:
  - Managed (for direct configuration from QRadar)
  - Stand-alone (for manual configuration)



WinCollect - InstallShield Wizard

Setup Type

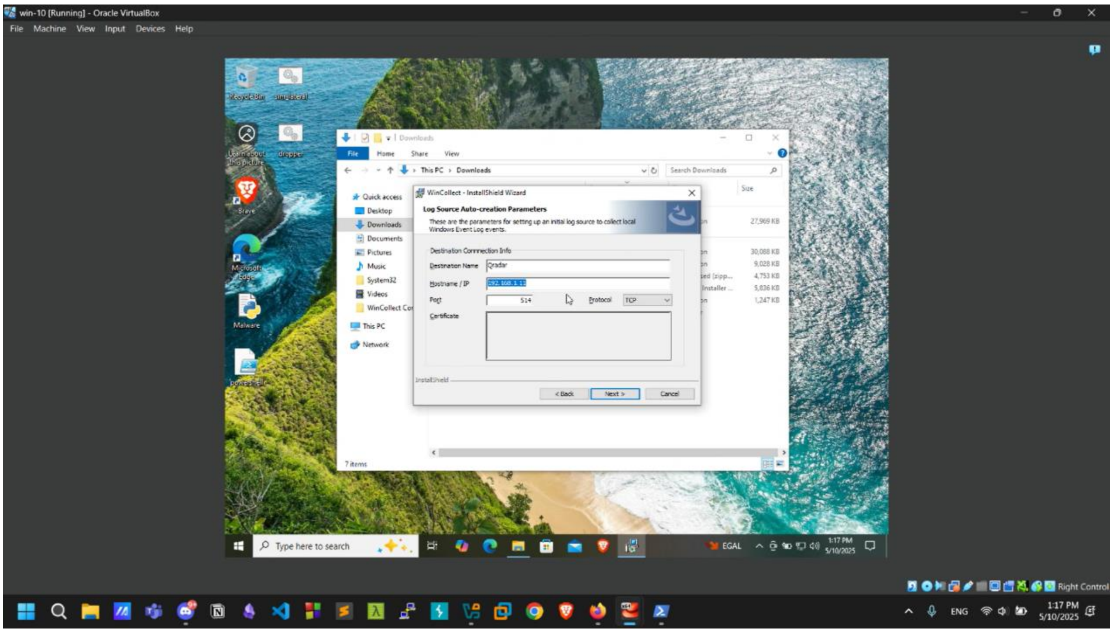
Choose the setup type that best suits your needs.

Please select a setup type.

○ **Managed** The WinCollect Agent will be managed by a QRadar Console.

● **Stand Alone** The WinCollect Agent will not be managed by a QRadar Console.

- Input the QRadar IP address when prompted



WinCollect - InstallShield Wizard

Log Source Auto-creation Parameters

These are the parameters for setting up an initial log source to collect local Windows Event Log events.

Destination Connection Info

Destination Name: Qradar

Hostname / IP: 192.168.1.11

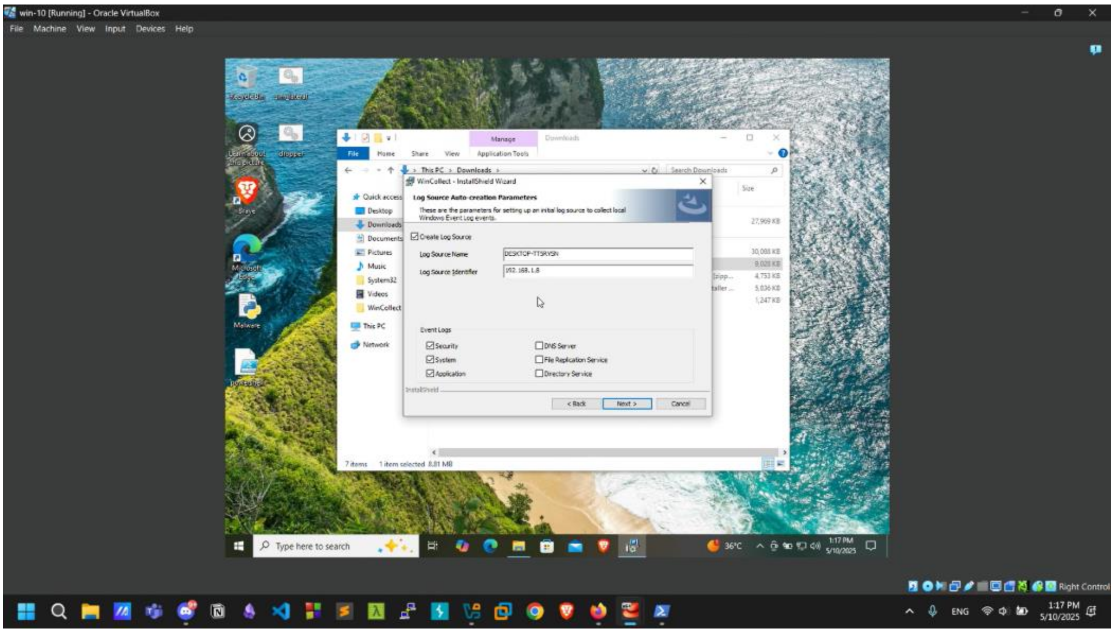
Port: 514

Protocol: TCP

Certificate:

Step 3: Configure Event Log Sources

- Choose which logs to forward:
  - Security
  - System
  - Application



WinCollect - InstallShield Wizard

Log Source Auto-creation Parameters

These are the parameters for setting up an inital log source to collect local Windows Event Log events.

☑ Create Log Source

Log Source Name: DESKTOP-TTSRYSN

Log Source Identifier: 192.168.1.8

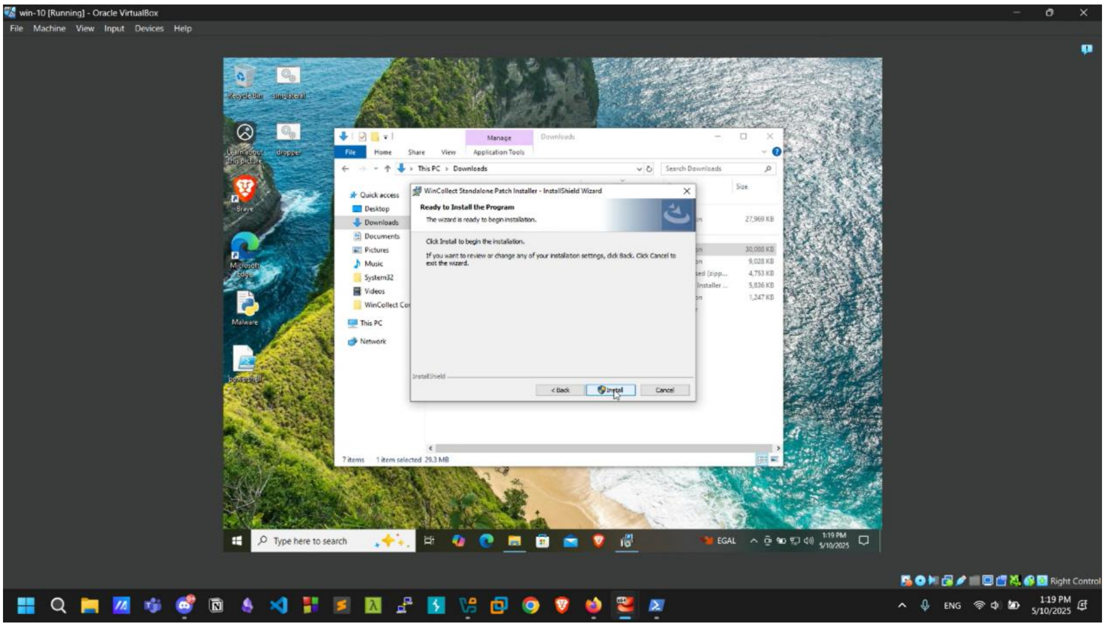
Event Logs

☑ Security ☐ DNS Server

☑ System ☐ File Replication Service

☑ Application ☐ Directory Service

- Save configuration and complete installation



WinCollect Standalone Patch Installer - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

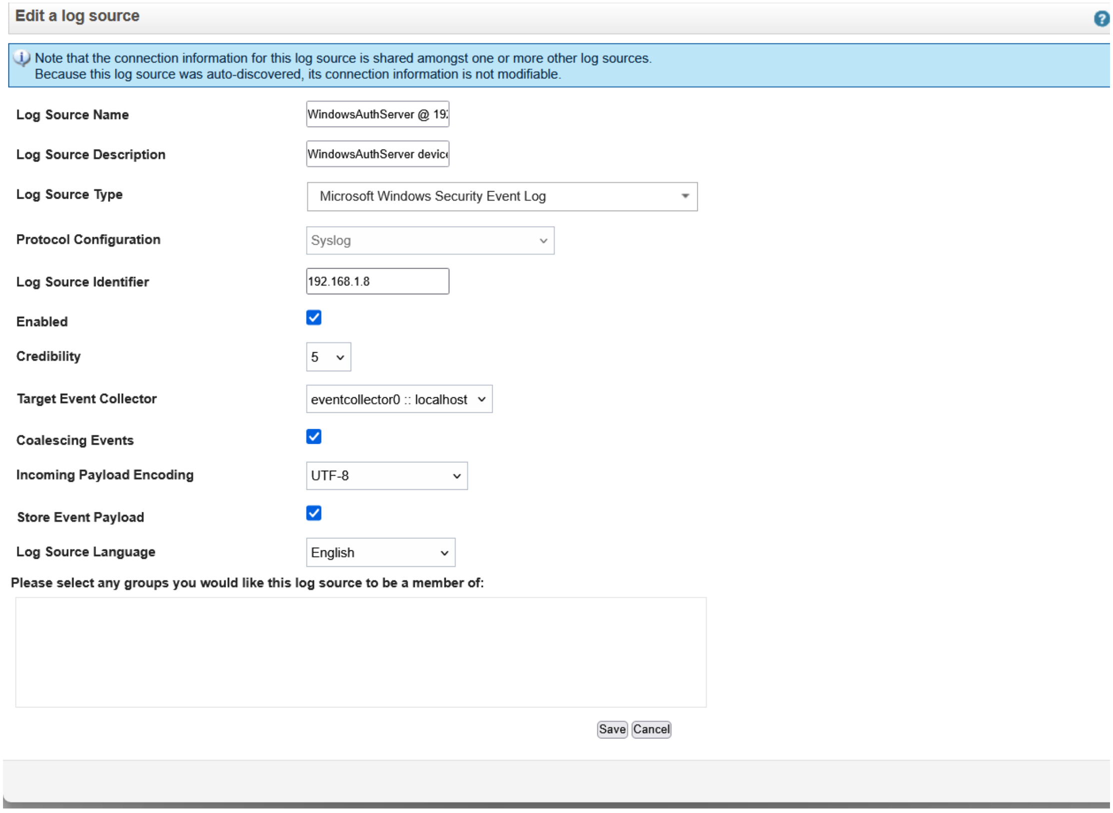
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

5. Configuring QRadar to Receive Logs

Step 1: Add a New Log Source

- Navigate to Admin > Log Sources > Add
- Enter the following:
  - Log Source Type: WinCollect
  - Protocol: Syslog
  - Log Source Identifier: Hostname or IP of the Windows machine
- Enable Auto Detection if desired
- Save the new log source



Edit a log source

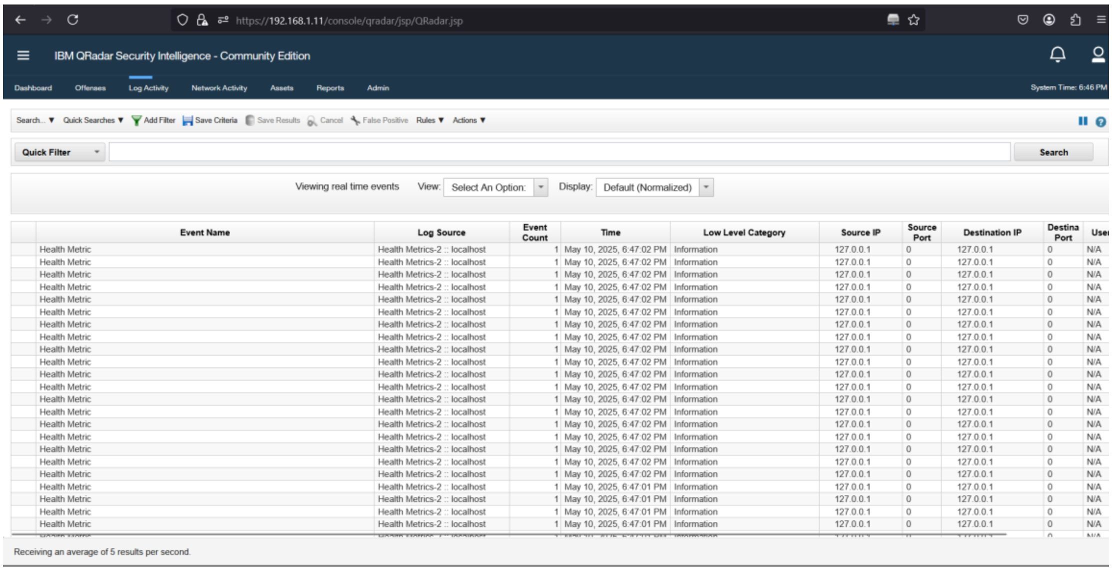
Note that the connection information for this log source is shared amongst one or more other log sources.
Because this log source was auto-discovered, its connection information is not modifiable.

Log Source Name	WindowsAuthServer @ 19
Log Source Description	WindowsAuthServer devic
Log Source Type	Microsoft Windows Security Event Log
Protocol Configuration	Syslog
Log Source Identifier	192.168.1.8
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: localhost
Coalescing Events	☑
Incoming Payload Encoding	UTF-8
Store Event Payload	☑
Log Source Language	English

Please select any groups you would like this log source to be a member of:

Step 2: Ensure Syslog Port is Accessible

- Verify that ports UDP/514 and TCP/514 are open on the QRadar host
- Ensure firewalls do not block incoming log traffic



Viewing real time events View: Select An Option: Display: Default (Normalized)

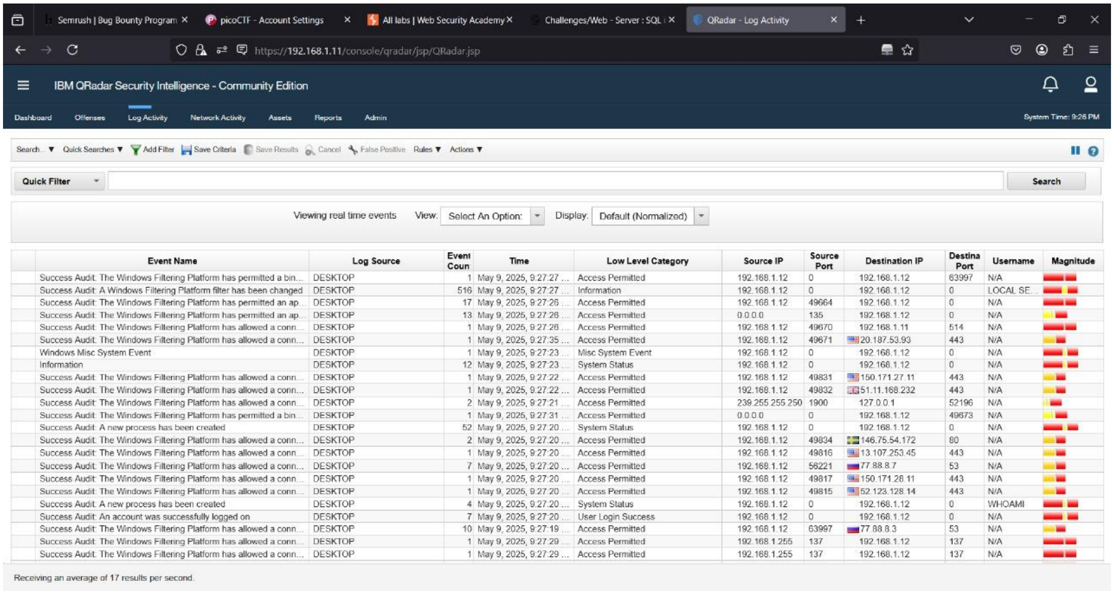
Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Use
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:02 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:01 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:01 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:01 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: localhost	1	May 10, 2025, 6:47:01 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A

Receiving an average of 5 results per second.

6. Verifying Log Collection

Step 1: Generate Logs on Windows

- Open Event Viewer
- Trigger events (e.g., login attempts to generate Event IDs like 4624 or 4625)



Viewing real time events View: Select An Option: Display: Default (Normalized)

Event Name	Log Source	Event Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
Success Audit: The Windows Filtering Platform has permitted a bin...	DESKTOP	1	May 9, 2025, 9:27:27 ...	Access Permitted	192.168.1.12	0	192.168.1.12	63997	N/A	
Success Audit: A Windows Filtering Platform filter has been changed	DESKTOP	516	May 9, 2025, 9:27:27 ...	Information	192.168.1.12	0	192.168.1.12	0	LOCAL SE...	
Success Audit: The Windows Filtering Platform has permitted an ap...	DESKTOP	17	May 9, 2025, 9:27:26 ...	Access Permitted	192.168.1.12	49664	192.168.1.12	0	N/A	
Success Audit: The Windows Filtering Platform has permitted an ap...	DESKTOP	13	May 9, 2025, 9:27:26 ...	Access Permitted	0.0.0.0	135	192.168.1.12	0	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:26 ...	Access Permitted	192.168.1.12	49670	192.168.1.11	514	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:35 ...	Access Permitted	192.168.1.12	49671	20.187.53.93	443	N/A	
Windows Misc System Event	DESKTOP	1	May 9, 2025, 9:27:23 ...	Misc System Event	192.168.1.12	0	192.168.1.12	0	N/A	
Information	DESKTOP	12	May 9, 2025, 9:27:23 ...	System Status	192.168.1.12	0	192.168.1.12	0	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:22 ...	Access Permitted	192.168.1.12	49831	150.171.27.11	443	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:22 ...	Access Permitted	192.168.1.12	49832	51.11.168.232	443	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	2	May 9, 2025, 9:27:21 ...	Access Permitted	239.255.255.250	1900	127.0.0.1	52196	N/A	
Success Audit: The Windows Filtering Platform has permitted a bin...	DESKTOP	1	May 9, 2025, 9:27:31 ...	Access Permitted	0.0.0.0	0	192.168.1.12	49673	N/A	
Success Audit: A new process has been created	DESKTOP	52	May 9, 2025, 9:27:20 ...	System Status	192.168.1.12	0	192.168.1.12	0	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	2	May 9, 2025, 9:27:20 ...	Access Permitted	192.168.1.12	49834	146.75.54.172	80	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:20 ...	Access Permitted	192.168.1.12	49816	13.107.253.45	443	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	7	May 9, 2025, 9:27:20 ...	Access Permitted	192.168.1.12	56221	77.88.8.7	53	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:20 ...	Access Permitted	192.168.1.12	49817	150.171.28.11	443	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:20 ...	Access Permitted	192.168.1.12	49815	52.123.128.14	443	N/A	
Success Audit: A new process has been created	DESKTOP	4	May 9, 2025, 9:27:20 ...	System Status	192.168.1.12	0	192.168.1.12	0	WHOAMI	
Success Audit: An account was successfully logged on	DESKTOP	7	May 9, 2025, 9:27:20 ...	User Login Success	192.168.1.12	0	192.168.1.12	0	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	10	May 9, 2025, 9:27:19 ...	Access Permitted	192.168.1.12	63997	77.88.8.3	53	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:29 ...	Access Permitted	192.168.1.255	137	192.168.1.12	137	N/A	
Success Audit: The Windows Filtering Platform has allowed a conn...	DESKTOP	1	May 9, 2025, 9:27:29 ...	Access Permitted	192.168.1.255	137	192.168.1.12	137	N/A	

Receiving an average of 17 results per second.

Step 2: Check QRadar Log Activity

- Go to Log Activity
- Filter by the Windows machine IP or hostname
- Confirm log entries are being received and parsed correctly

7. Conclusion

In this lab, we successfully set up IBM QRadar CE in a virtual environment on an Ubuntu machine and configured a Windows host with WinCollect to send event logs to QRadar. This setup enables real-time log collection and analysis, an essential step in building a security monitoring infrastructure.