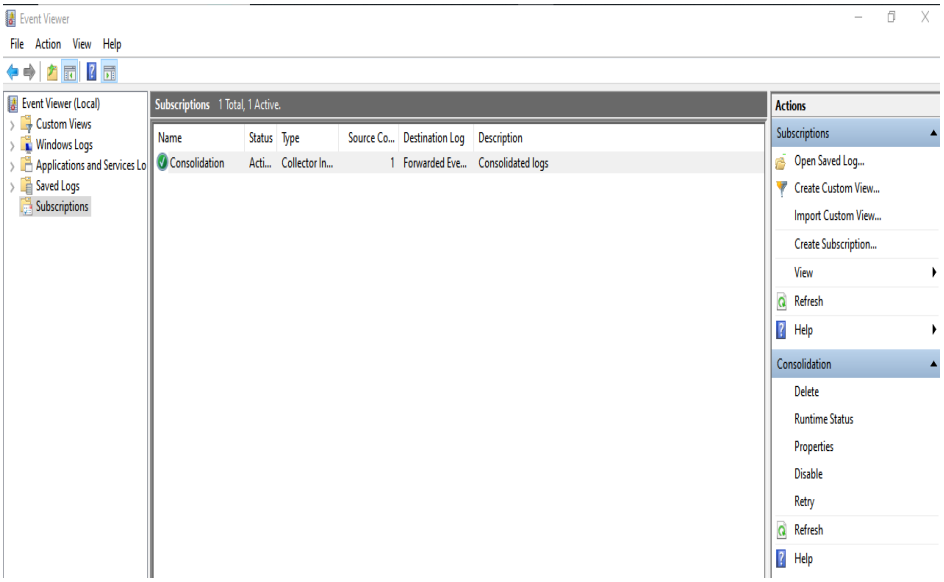
Setting Up a Central Log Repository in Event Viewer

Setting up a central log repository using Event Viewer to consolidate logs from multiple systems can be done using Windows Event Forwarding (WEF).

1.Created a subscription on event viewer named Consolidation



Service Status: Make sure that the Windows Event Collector (WecSvc) service is running on the collector and the Windows Remote Management (WinRM) service is running on the source computers.

In command prompt run these commands:

> winrm quickconfig

> wecutil qc

Automation for analyzing the consolidated logs with Python:

```
import pandas as pd


# Load the logs from a CSV file
logs_df = pd.read_csv('logs.csv')


# Define the levels to filter
```

```
levels_to_filter = ['Warning', 'Error', 'Critical']

# Filter logs based on the defined levels
filtered_logs = logs_df[logs_df['Level'].isin(levels_to_filter)]

# Function to categorize the logs
def categorize_log(level):
    if level == 'Warning':
        return 'Needs Attention'
    elif level == 'Error':
        return 'Requires Immediate Remedy'
    elif level == 'Critical':
        return 'Critical System Issue'
    else:
        return 'Informational'

# Apply the categorization
filtered_logs['Category'] = filtered_logs['Level'].apply(categorize_log)

# Print the filtered and categorized logs
print(filtered_logs)

# Save the filtered and categorized logs to a new CSV file
filtered_logs.to_csv('filtered_logs.csv', index=False)
```