SPLUNK IMPLEMENTATION FOR SECURITY ANALYSIS

By Oluwaseyi Majekodunmi

INTRODUCTION

This presentation covers my project on implementing Splunk for security analysis. As organizations increasingly face various cyber threats, having robust systems in place for monitoring and analyzing security events is crucial. This project focuses on creating a comprehensive security analysis environment using Splunk, designed to detect and respond to security incidents effectively.

PROJECT OBJECTIVES

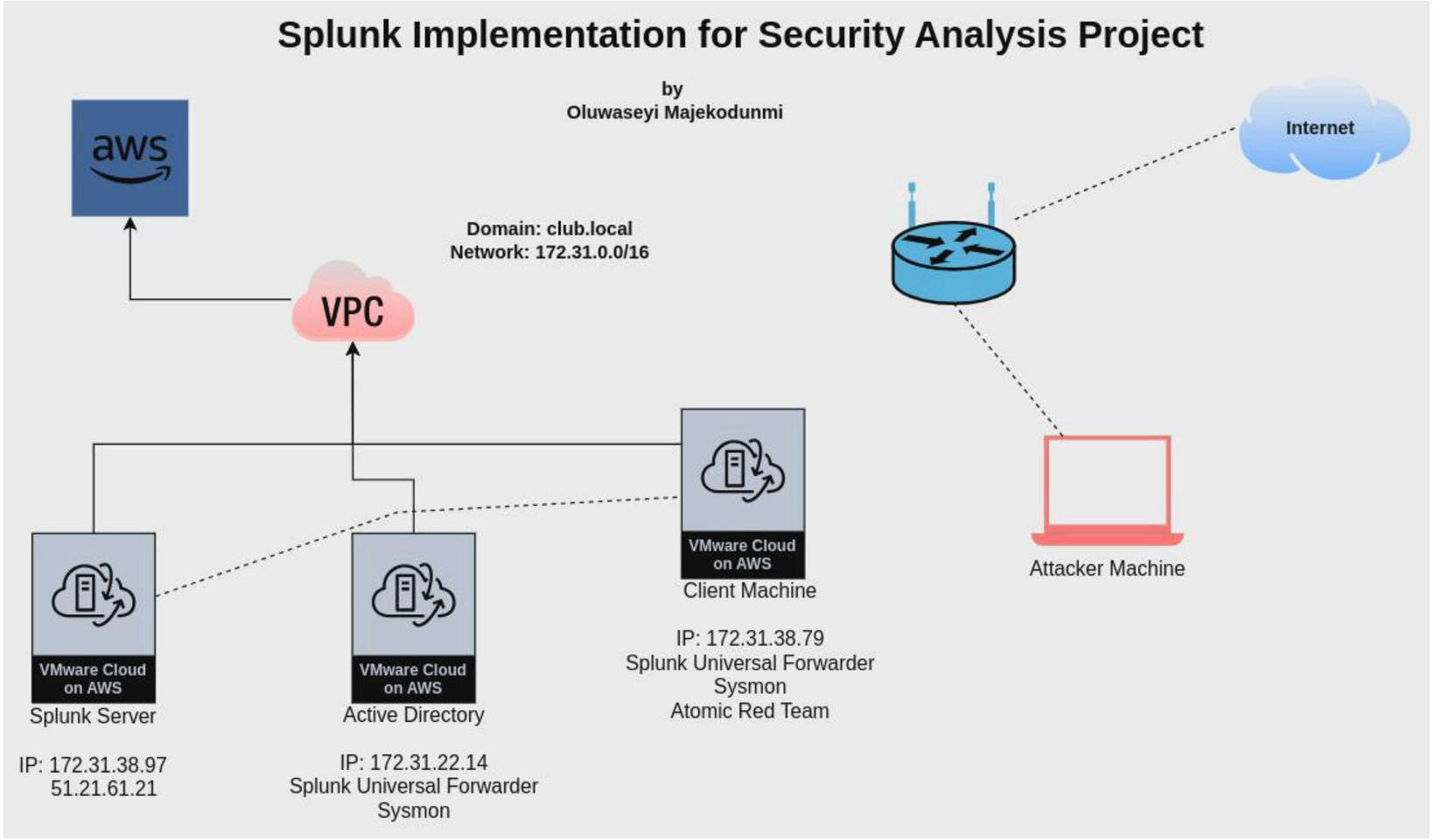
The primary objective of this project is to implement Splunk as a centralized platform for security analysis and threat detection. I aim to establish an environment that integrates Splunk with an Active Directory domain, enabling the simulation of various attacks and the analysis of their impact on client machines within that domain.

ARCHITECTURE OVERVIEW

The architecture of this project consists of several key components that work together to facilitate security analysis. The following diagram (see next page) illustrates how these components are connected and interact within the environment. Below are brief descriptions of each component and their roles:

- **Active Directory Server:** This server is responsible for managing user authentication and permissions within the domain.
- **Client Machine:** The target for simulated attacks, from which logs and event data are collected for analysis.
- **Splunk Server:** The core of the analysis environment. Splunk collects, indexes, and analyzes data generated from the client machine to provide valuable insights into security events.

Splunk Implementation for Security Analysis Project



IMPLEMENTATION DETAILS

This section outlines the key steps involved in setting up the security analysis environment:

- **Install and Configure Splunk:** I began by installing Splunk on a dedicated server to handle incoming data. After installation, I configured Splunk to process logs from various sources and set up indexers and forwarders to manage data ingestion efficiently.
- **Setting Up Active Directory:** Next, I configured Active Directory on a Windows Server. This setup involved installing the Active Directory Domain Services (AD DS) role, creating a domain, and managing user accounts and permissions within the domain. Active Directory is essential for managing authentication and centralizing domain control across the client and Splunk servers.

- **Universal Forwarder Installation:** The Splunk Universal Forwarder was installed on both the Active Directory server and the client machine. The Universal Forwarder collects logs from these machines and forwards them to the Splunk server for indexing and analysis, ensuring that no critical event data is missed during the simulation of attacks.
- **Sysmon Setup:** I also installed Sysmon on both the Active Directory server and the client machine. Sysmon provides detailed event logs for system activity, such as process creations, network connections, and file modifications, which are crucial for detecting potential attack patterns and behaviors during simulations.
- **Data Collection:** With the Universal Forwarder and Sysmon in place, I configured the environment to collect event logs, system activity, and security-related data from both the Active Directory server and the client machine. This ensures that Splunk receives real-time data for indexing and further analysis.

- **Splunk Configuration:** Finally, I configured Splunk to receive and index the data from both sources (Active Directory and client machine). This involved setting up data inputs, creating indexes, and writing searches to monitor specific events such as login attempts, process creations, and network activity.

By following these steps, I created a robust environment capable of simulating and analyzing attacks in real-time using Splunk's advanced security analysis features.

ATTACK SIMULATION

In this project, various types of attacks were simulated, including:

- **Brute Force Attack on RDP:** I conducted a brute force attack on Remote Desktop Protocol (RDP) using Hydra. This involved attempting multiple login combinations to test the strength of the authentication mechanism and assess the potential vulnerabilities in the system.
- **Atomic Red Team Simulations:** I set up Atomic Red Team on the client machine to simulate several attacks based on the MITRE framework. This allowed me to test various attack techniques and tactics commonly used by adversaries, providing a comprehensive assessment of the security environment.

By employing these methods, I aim to gain insights into how well the Splunk implementation can detect and respond to different types of attacks.

DATA ANALYSIS

Once the attacks are simulated and data is collected, Splunk's powerful processing capabilities come into play.

- **Real-Time Data Indexing:** Splunk allows me to index incoming data in real time, making it searchable almost instantly.
- **Example Queries:** I created specific queries to filter and analyze the data collected from the client machine. For instance, I searched for login attempts that failed multiple times, which could indicate a brute-force attack.

RESULTS AND FINDINGS

Through my simulations and analysis, I gained valuable insights into the security vulnerabilities of my environment. The findings include:

- Notable trends in attack patterns and how quickly they can be detected by Splunk.
- Recommendations for improving security measures based on the analysis of attack simulations.

CONCLUSION

In conclusion, the implementation of Splunk for security analysis offers a powerful solution for organizations looking to enhance their security posture. By establishing a dedicated environment for monitoring and analyzing various attack simulations, I can better understand potential threats and improve response strategies. Future work could include expanding the types of attacks simulated and integrating additional security tools to further strengthen my analysis capabilities.

ATTACHMENTS

splunk>enterprise Apps ▾ Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Receive data

Forwarding and receiving » Receive data

New Receiv

Showing 1-1 of 1 item

filter

25 per

Listen on this port ⇕
9997

splunk>enterprise Apps ▾

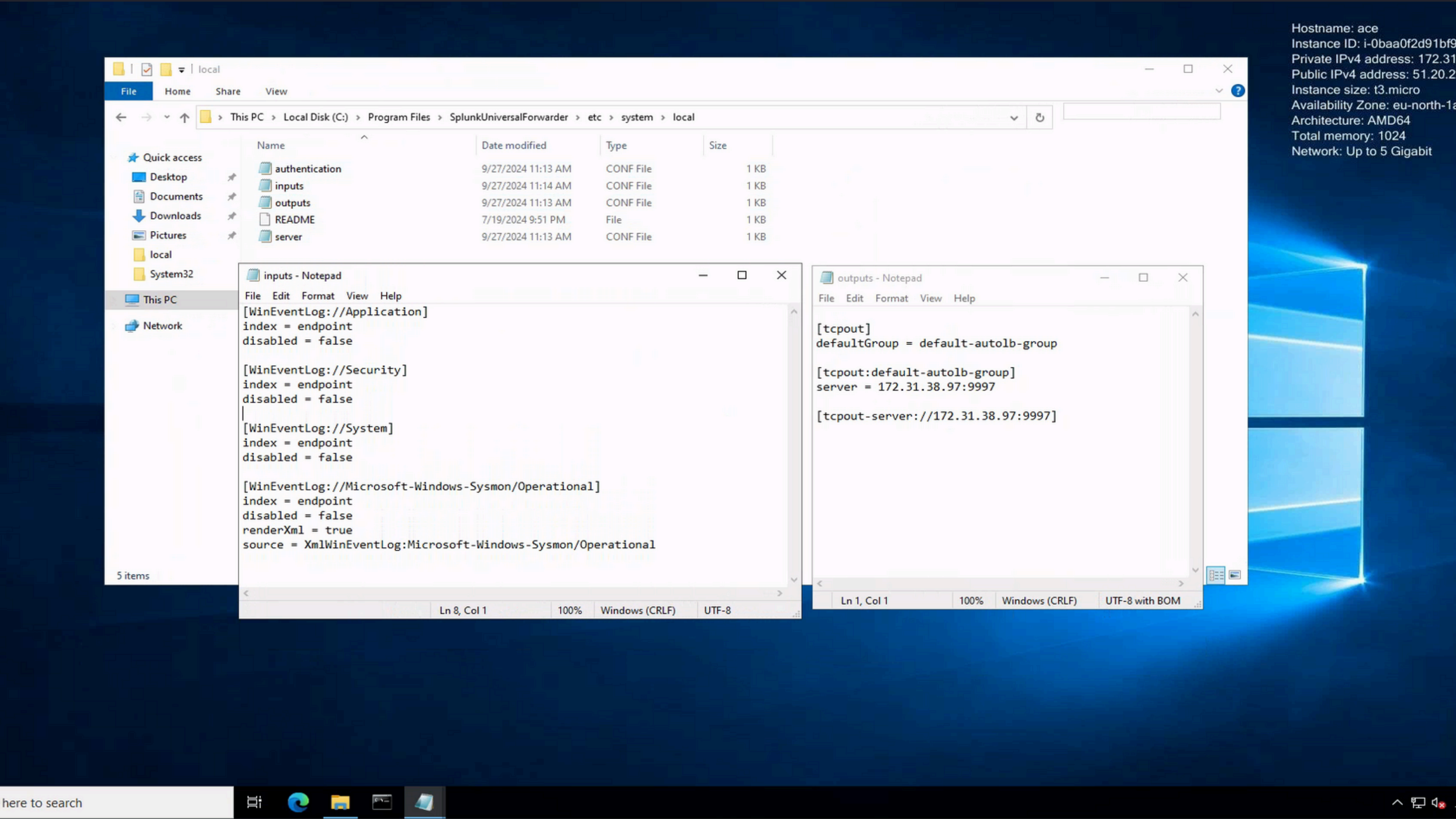
Indexes

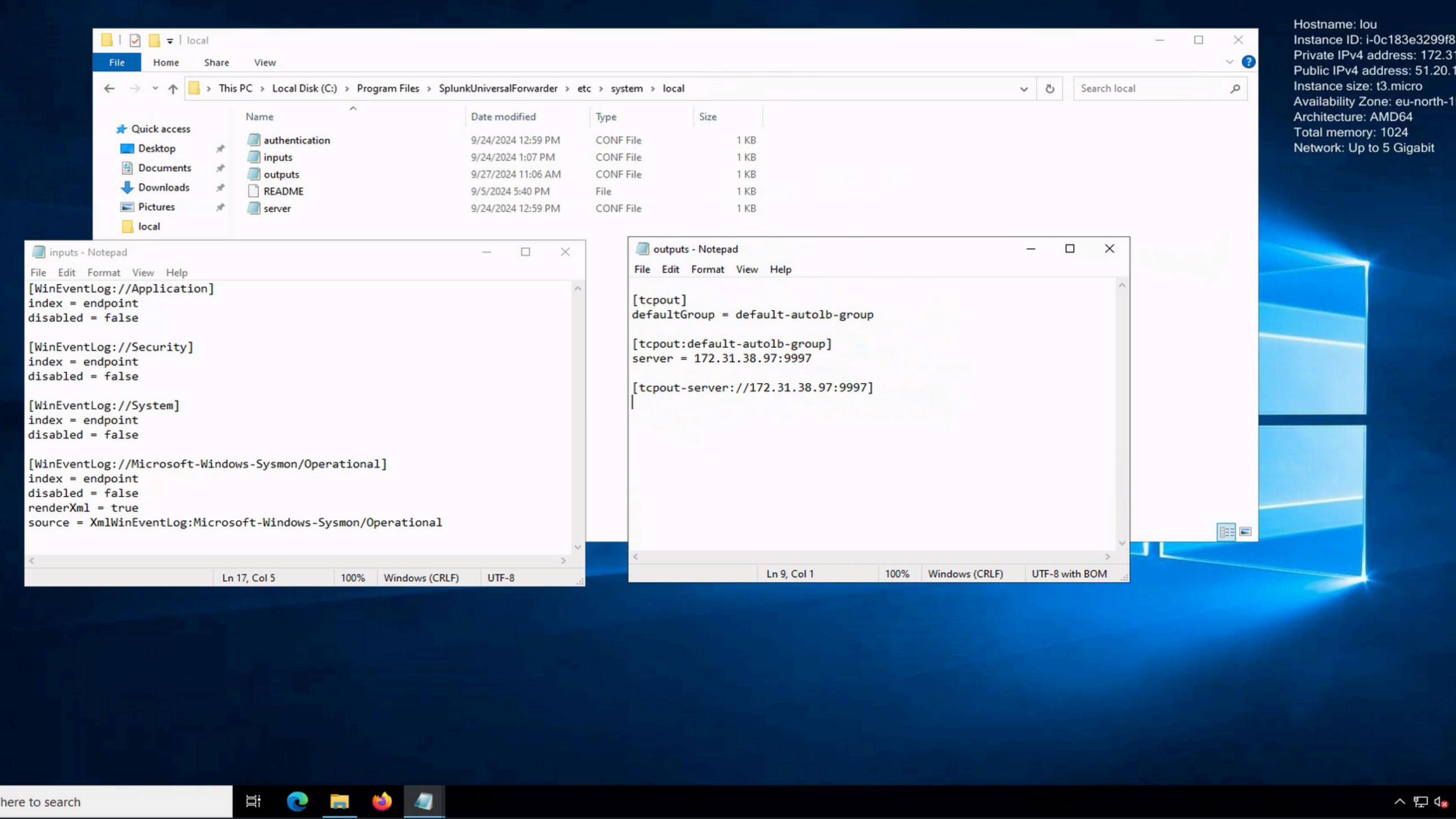
A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn

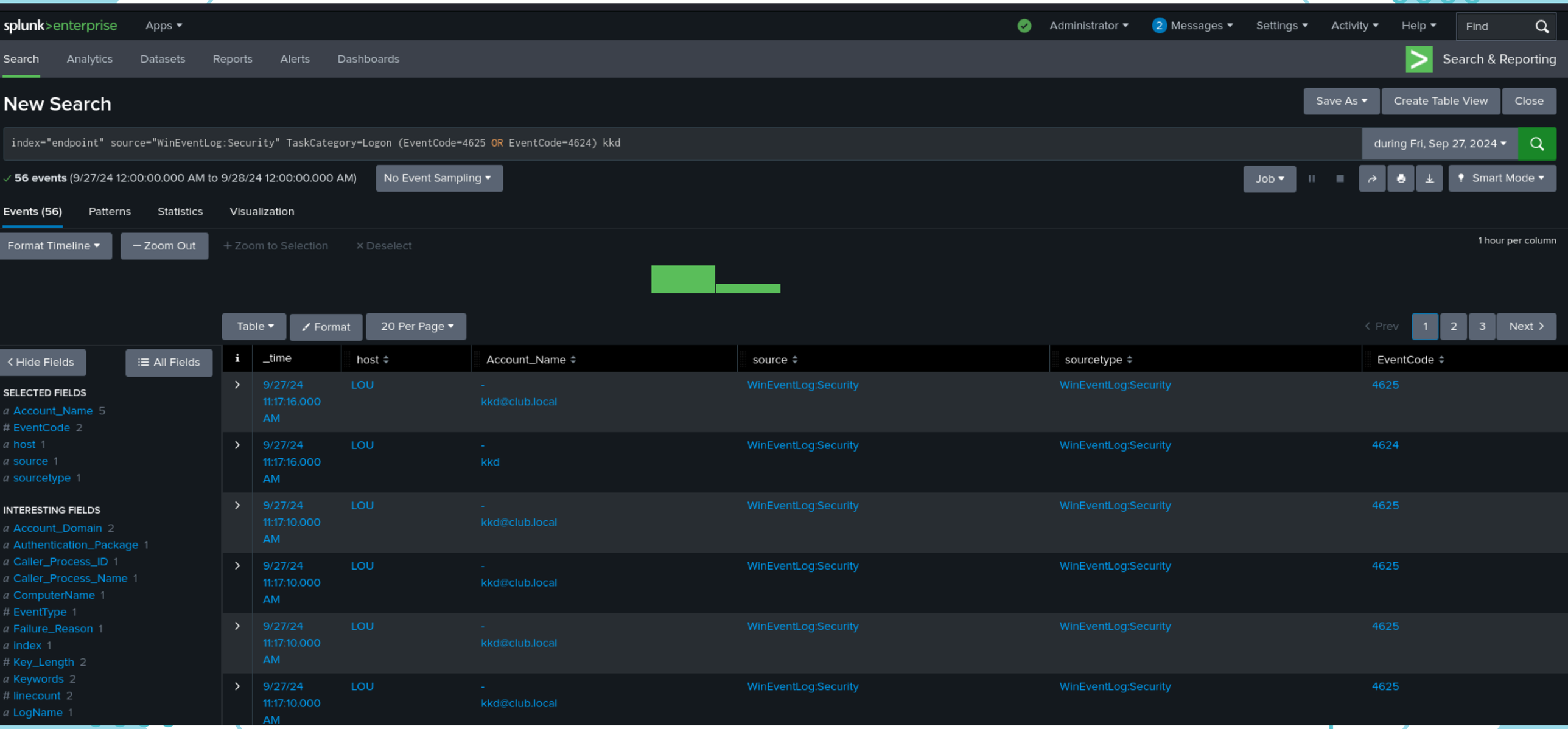
16 Indexes filter

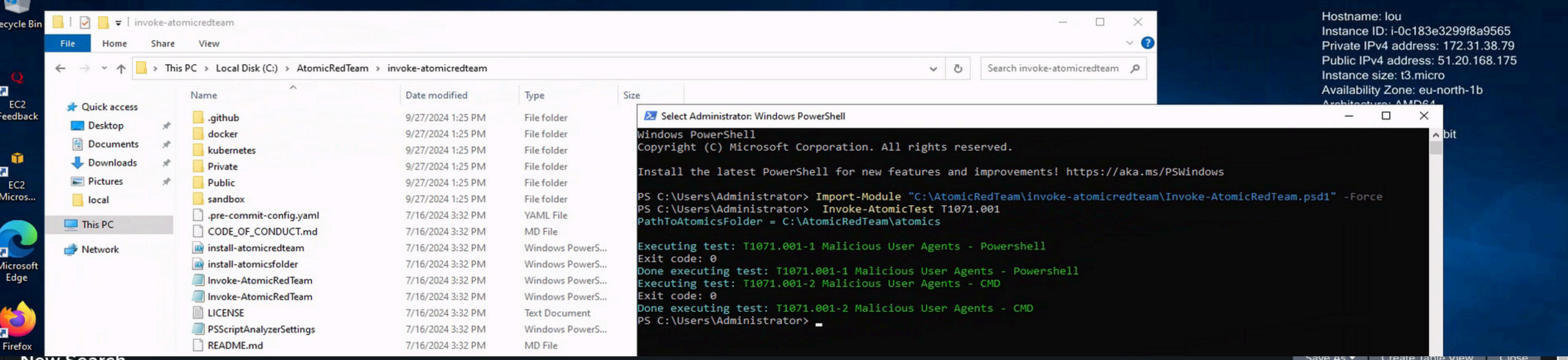
Name ▲	Actions	Type ⇕	App ⇕	Current Size ⇕
_audit	Edit Delete Disable	Events	system	6 MB
_configtracker	Edit Delete Disable	Events	system	1 MB
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB
_dsclient	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB
_dsphonehome	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB
_internal	Edit Delete Disable	Events	system	92 MB
_introspection	Edit Delete Disable	Events	system	304 MB
_metrics	Edit Delete Disable	Metrics	system	79 MB
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB
_telemetry	Edit Delete Disable	Events	system	1 MB
_thefishbucket	Edit Delete Disable	Events	system	1 MB
endpoint	Edit Delete Disable	Events	search	61 MB
history	Edit Delete Disable	Events	system	1 MB
main	Edit Delete Disable	Events	system	1 MB
splunklogger	Edit Delete Enable	Events	system	0 B
summary	Edit Delete Disable	Events	system	1 MB

```
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1015-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Oct  1 09:58:38 UTC 2024

  System load:  0.4               Temperature:           -273.1 C
  Usage of /:   57.1% of 28.02GB  Processes:             118
  Memory usage: 45%               Users logged in:       0
  Swap usage:   4%                IPv4 address for ens5: 172.31.38.97

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Sun Sep 29 14:02:51 2024 from 13.48.4.202
ubuntu@ip-172-31-38-97:~$ sudo /opt/splunk/bin/splunk status
splunkd is running (PID: 2482).
splunk helpers are running (PIDs: 2483 2672 2677 2737 2839 420631 425447 430087 430089 430091).
ubuntu@ip-172-31-38-97:~$
```


Hostname: ace
Instance ID: i-0baa0f2d91bf9
Private IPv4 address: 172.31
Public IPv4 address: 51.20.2
Instance size: t3.micro
Availability Zone: eu-north-1a
Architecture: AMD64
Total memory: 1024
Network: Up to 5 Gigabit
local
File Home Share View
This PC › Local Disk (C:) › Program Files › SplunkUniversalForwarder › etc › system › local
Quick access
Desktop
Documents
Downloads
Pictures
local
System32
This PC
Network
Name Date modified Type Size
authentication 9/27/2024 11:13 AM CONF File 1 KB
inputs 9/27/2024 11:14 AM CONF File 1 KB
outputs 9/27/2024 11:13 AM CONF File 1 KB
README 7/19/2024 9:51 PM File 1 KB
server 9/27/2024 11:13 AM CONF File 1 KB
5 items
inputs - Notepad
File Edit Format View Help
[WinEventLog://Application]
index = endpoint
disabled = false
[WinEventLog://Security]
index = endpoint
disabled = false
[WinEventLog://System]
index = endpoint
disabled = false
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
Ln 8, Col 1 100% Windows (CRLF) UTF-8
outputs - Notepad
File Edit Format View Help
[tcpout]
defaultGroup = default-autolb-group
[tcpout:default-autolb-group]
server = 172.31.38.97:9997
[tcpout-server://172.31.38.97:9997]
Ln 1, Col 1 100% Windows (CRLF) UTF-8 with BOM
here to search


Hostname: lou
Instance ID: i-0c183e3299f8
Private IPv4 address: 172.31
Public IPv4 address: 51.20.1
Instance size: t3.micro
Availability Zone: eu-north-1
Architecture: AMD64
Total memory: 1024
Network: Up to 5 Gigabit
local
File Home Share View
This PC › Local Disk (C:) › Program Files › SplunkUniversalForwarder › etc › system › local
Search local
Quick access
Desktop
Documents
Downloads
Pictures
local
Name Date modified Type Size
authentication 9/24/2024 12:59 PM CONF File 1 KB
inputs 9/24/2024 1:07 PM CONF File 1 KB
outputs 9/27/2024 11:06 AM CONF File 1 KB
README 9/5/2024 5:40 PM File 1 KB
server 9/24/2024 12:59 PM CONF File 1 KB
inputs - Notepad
File Edit Format View Help
[WinEventLog://Application]
index = endpoint
disabled = false
[WinEventLog://Security]
index = endpoint
disabled = false
[WinEventLog://System]
index = endpoint
disabled = false
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
Ln 17, Col 5 100% Windows (CRLF) UTF-8
outputs - Notepad
File Edit Format View Help
[tcpout]
defaultGroup = default-autolb-group
[tcpout:default-autolb-group]
server = 172.31.38.97:9997
[tcpout-server://172.31.38.97:9997]
Ln 9, Col 1 100% Windows (CRLF) UTF-8 with BOM
here to search


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="endpoint" source="WinEventLog:Security" TaskCategory=Logon (EventCode=4625 OR EventCode=4624) kkd
during Fri, Sep 27, 2024
56 events (9/27/24 12:00:00.000 AM to 9/28/24 12:00:00.000 AM)
No Event Sampling
Job
Smart Mode
Events (56)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 hour per column
Table
Format
20 Per Page
Prev
1
2
3
Next
Hide Fields
All Fields
SELECTED FIELDS
a Account_Name 5
EventCode 2
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 2
a Authentication_Package 1
a Caller_Process_ID 1
a Caller_Process_Name 1
a ComputerName 1
EventType 1
a Failure_Reason 1
a index 1
Key_Length 2
a Keywords 2
linecount 2
a LogName 1
i
_time
host
Account_Name
source
sourcetype
EventCode
9/27/24 11:17:16.000 AM
LOU
- kkd@club.local
WinEventLog:Security
WinEventLog:Security
4625
9/27/24 11:17:16.000 AM
LOU
- kkd
WinEventLog:Security
WinEventLog:Security
4624
9/27/24 11:17:10.000 AM
LOU
- kkd@club.local
WinEventLog:Security
WinEventLog:Security
4625
9/27/24 11:17:10.000 AM
LOU
- kkd@club.local
WinEventLog:Security
WinEventLog:Security
4625
9/27/24 11:17:10.000 AM
LOU
- kkd@club.local
WinEventLog:Security
WinEventLog:Security
4625
9/27/24 11:17:10.000 AM
LOU
- kkd@club.local
WinEventLog:Security
WinEventLog:Security
4625



New Search

Save As ▾ Create Table View Close

index="endpoint" useragent

All time ▾

✓ **1 event** (before 10/1/24 7:00:40.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ − Zoom Out + Zoom to Selection × Deselect 1 millisecond per column

List ▾ Format 20 Per Page ▾

< Hide Fields ☰ All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Guid 1
a IMPHASH 1
a index 1
linecount 1
a MD5 1
a Name 1
a ProcessID 1
a punct 1
a SHA1 1

i	Time	Event
›	10/1/24 6:55:05.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-10-01T18:55:05.3506915Z'/><EventRecordID>25556</EventRecordID><Correlation/><Execution ProcessID='2240' ThreadID='2844'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>lou.club.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2024-10-01 18:55:05.322</Data><Data Name='ProcessGuid'>{f28b91e2-4589-66fc-bc03-00000000f101}</Data><Data Name='ProcessId'>1084</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='FileVersion'>10.0.20348.2340 (WinBuild.160101.0800)</Data><Data Name='Description'>Windows PowerShell</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>PowerShell.EXE</Data><Data Name='CommandLine'>"powershell.exe" & {Invoke-WebRequest www.google.com -UserAgent \""HttpBrowser/1.0\""	out-null Invoke-WebRequest www.google.com -UserAgent \""Wget/1.9+cvs-stable (Red Hat modified)\""	out-null Invoke-WebRequest www.google.com -UserAgent \""Opera/8.81 (Windows NT 6.0; U; en)\""	out-null Invoke-WebRequest www.google.com -UserAgent \""*<|>*\""	out-null}</Data><Data Name='CurrentDirectory'>C:\Users\ADMINI~1\AppData\Local\Temp\2\</Data><Data Name='User'>LOU\Administrator</Data><Data Name='LogonGuid'>{f28b91e2-3342-66fc-c637-190000000000}</Data><Data Name='LogonId'>0x1937c6</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=A2D8D23854E33984C08DCF8B03EDC619C9C5EC69,MD5=0BC8A4CD1E07390BAFD741E1FC0399A3,SHA256=75D6634A676FB0BEA5BFD8D424E2BD4F685F3885853637EA143B2671A3BB76E9,IMPHASH=AFACF6DC9041114B198160AAB4D0AE77</Data><Data Name='ParentProcessGuid'>{f28b91e2-4565-66fc-b403-00000000f101}</Data><Data Name='ParentProcessId'>6088</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" </Data><Data Name='ParentUser'>LOU\Administrator</Data></EventData></Event> host = LOU source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational