Lateral Movement and Data Access (LMDA) Artifacts for Velociraptor: Implementation Guide

2025-10-27

Table of Contents

Introduction 3

Prerequisites... 3

Importing LMDA Artifacts 5

Running the Artifacts 9

Visualizing Lateral Movement Results 13

Presenting Data Access Results...19

Excel Template Structure and Usage... 20

Introduction

This document describes how to leverage the Lateral Movement and Data Access (LMDA) artifacts developed by Stroz Friedberg for Velociraptor, a remote endpoint forensic tool. The document contains information about:

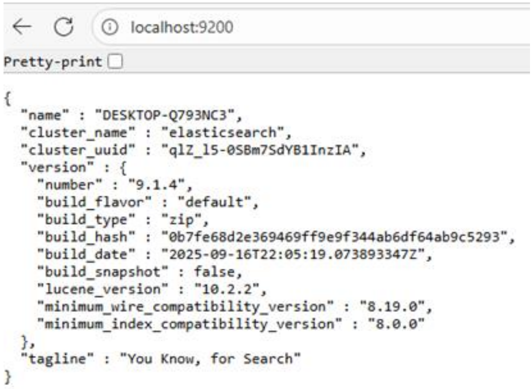
- Importing LMDA artifacts in Velociraptor
- Executing LMDA artifacts via Velociraptor
- Visualizing lateral movement using ElasticSearch and Grafana
- Visualizing lateral movement using Jupyter Notebook and PyVelociraptor Python library
- Presenting data access results through a predefined Excel template

The techniques and workflows described here assume that you are working with the latest version of Velociraptor (0.75.2 as of writing).

Prerequisites

Before proceeding, ensure you have the following components installed:

1. Velociraptor (greater than or equal to version 0.75.2). Official documentation can be used for installation.
2. ElasticSearch and Kibana. Official documentation can be used for installation. Verify that ElasticSearch is operational by navigating to http://localhost:9200/ in your web browser. A successful connection should display the following ElasticSearch output:



```
{
  "name" : "DESKTOP-Q793NC3",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "qlZ_l5-0SBm7SdYB1InzIA",
  "version" : {
    "number" : "9.1.4",
    "build_flavor" : "default",
    "build_type" : "zip",
    "build_hash" : "0b7fe68d2e369469ff9e9f344ab6df64ab9c5293",
    "build_date" : "2025-09-16T22:05:19.073893347Z",
    "build_snapshot" : false,
    "lucene_version" : "10.2.2",
    "minimum_wire_compatibility_version" : "8.19.0",
    "minimum_index_compatibility_version" : "8.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Image 1: ElasticSearch verification

Verify that Kibana is operational by navigating to http://localhost:5601/app/home#/ in your web browser. A successful connection should display Kibana homepage.

3. Grafana (if you prefer creating visualizations in Grafana). Official documentation can be used for installation. Verify that Grafana is operational by navigating to http://localhost:3000 in your web browser. A successful connection should display Grafana homepage.
4. Python Environment (greater than or equal to version 3.12 and if you prefer creating visualizations in Jupyter Notebook). Official documentation can be used for installation. Ensure you have the following Python packages installed (you may use "*python -m pip install <package name>*" command to install packages):
    - PyVelociraptor
    - Matplotlib
    - Networkx
    - Bokeh
    - Pandas
5. Jupyter Notebook (if you prefer creating visualizations in Jupyter Notebook). Official documentation can be used for installation. Verify that Jupyter Notebook is operational by navigating to http://127.0.0.1:8888/lab

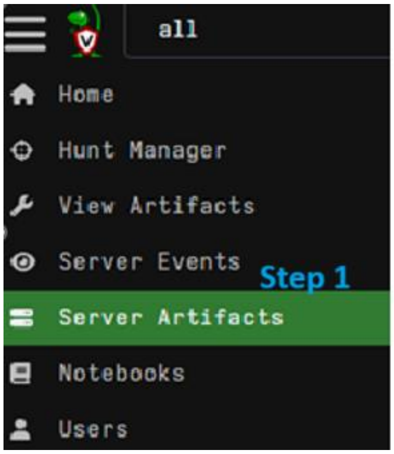
in your web browser. A successful connection should display the Jupyter Notebook interface.

Importing LMDA Artifacts

The LMDA artifacts are published in a public repository maintained by Stroz Friedberg. To get started:

1. Navigate to the GitHub repository: https://github.com/strozfriedberg/Velociraptor_LMDA
2. To obtain the LMDA artifacts, you can either download or clone the repository by running *git clone https://github.com/strozfriedberg/Velociraptor_LMDA.git* in a command prompt or manually copy the code from the relevant YAML files.

3. Prior to importing the LMDA artifacts, navigate to the Server Artifacts section within the Velociraptor GUI. Execute the Server.Import.ArtifactExchange and Server.Import.Extras artifacts, as illustrated in the images below. Completing this step enables the import of artifacts and hunts associated with the LMDA artifacts. For guidance on hunt creation, please refer to the official documentation.



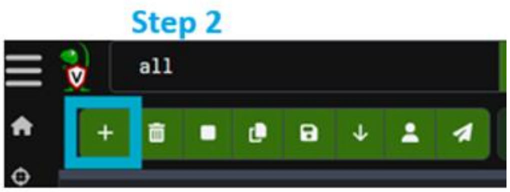
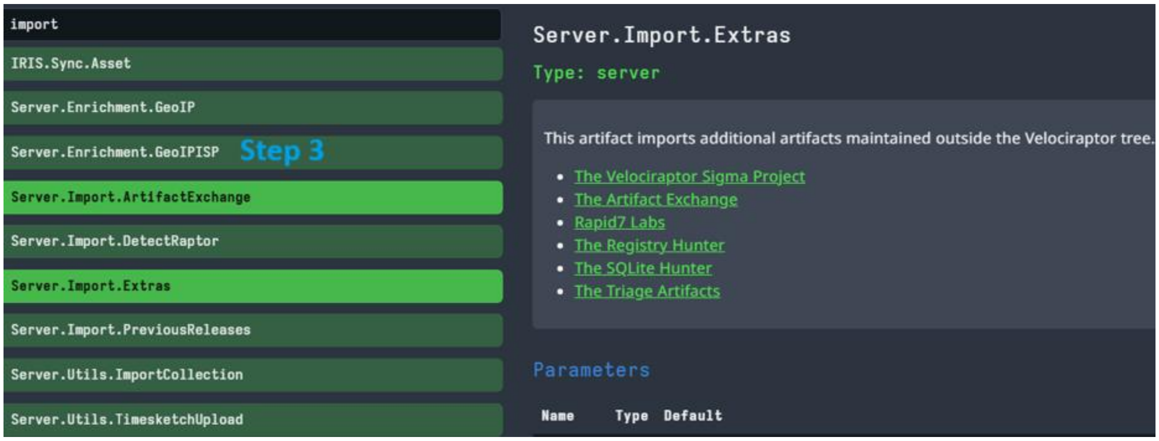


Image 2: Velociraptor server artifacts execution


import
IRIS.Sync.Asset
Server.Enrichment.GeoIP
Server.Enrichment.GeoIPISP
Step 3
Server.Import.ArtifactExchange
Server.Import.DetectRaptor
Server.Import.Extras
Server.Import.PreviousReleases
Server.Utils.ImportCollection
Server.Utils.TimesketchUpload
Parameters
Name
Type
Default

Server.Import.Extras

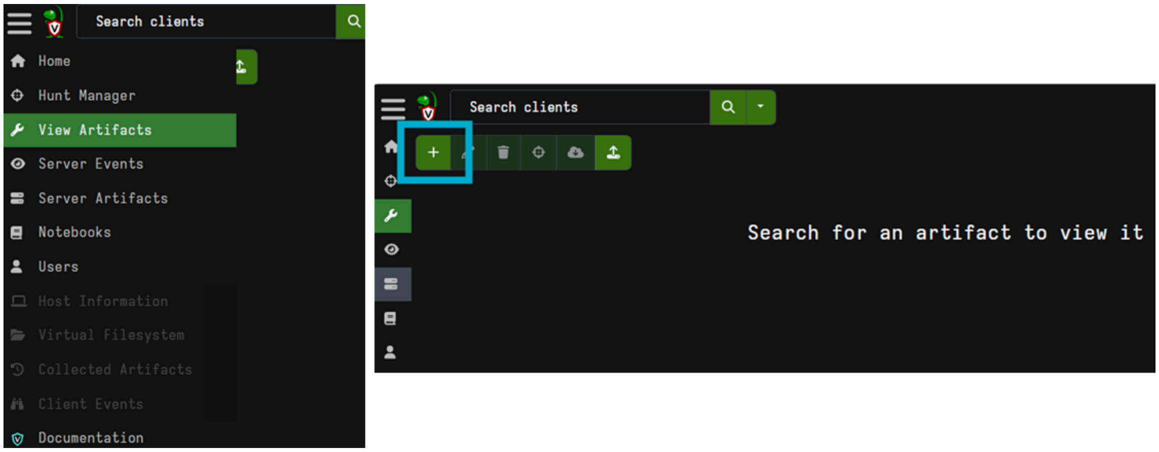
Type: server

This artifact imports additional artifacts maintained outside the Velociraptor tree.

- The Velociraptor Sigma Project
- The Artifact Exchange
- Rapid7 Labs
- The Registry Hunter
- The SQLite Hunter
- The Triage Artifacts

Image 3: Velociraptor server artifacts execution

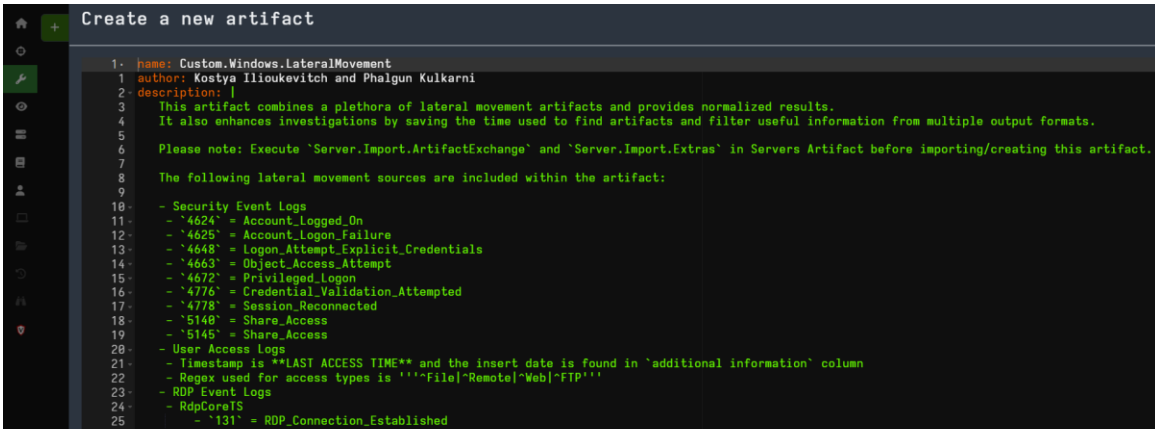
4. To add new artifacts within Velociraptor, navigate to the View Artifacts section and select the + icon. In the “Create a new artifact” dialog, paste the YAML code for Custom.Windows.LateralMovement.yaml and Custom.Windows.DataAccess.yaml individually to create each artifact, as illustrated in the images below.



Search for an artifact to view it

Image 4: LMDA artifacts creation

5. Paste YAML code for each artifact in “Create a new artifact” box.

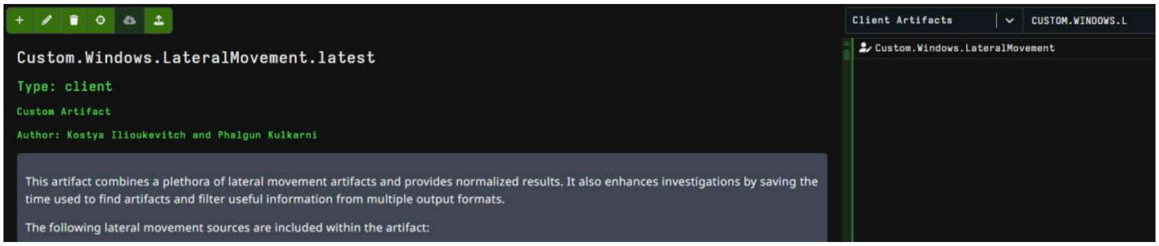


Create a new artifact

```yaml
name: Custom.Windows.LateralMovement
author: Kostya Ilioukevitch and Phalgun Kulkarni
description: |
   This artifact combines a plethora of lateral movement artifacts and provides normalized results.
   It also enhances investigations by saving the time used to find artifacts and filter useful information from multiple output formats.

   Please note: Execute `Server.Import.ArtifactExchange` and `Server.Import.Extras` in Servers Artifact before importing/creating this artifact.

   The following lateral movement sources are included within the artifact:

   - Security Event Logs
    - `4624` = Account_Logged_On
    - `4625` = Account_Logon_Failure
    - `4648` = Logon_Attempt_Explicit_Credentials
    - `4663` = Object_Access_Attempt
    - `4672` = Privileged_Logon
    - `4776` = Credential_Validation_Attempted
    - `4778` = Session_Reconnected
    - `5140` = Share_Access
    - `5145` = Share_Access
   - User Access Logs
    - Timestamp is **LAST ACCESS TIME** and the insert date is found in `additional information` column
    - Regex used for access types is '''^File|^Remote|^Web|^FTP'''
   - RDP Event Logs
    - RdpCoreTS
        - `131` = RDP_Connection_Established
```

Image 5: LMDA artifacts creation

6. After importing, confirm that “Custom.Windows.LateralMovement” and “Custom.Windows.DataAccess” appear in your artifact list, as illustrated in the image below.



Custom.Windows.LateralMovement.latest

Type: client

Custom Artifact

Author: Kostya Ilioukevitch and Phalgun Kulkarni

This artifact combines a plethora of lateral movement artifacts and provides normalized results. It also enhances investigations by saving the time used to find artifacts and filter useful information from multiple output formats.

The following lateral movement sources are included within the artifact:

Image 6: LMDA artifacts verification

7. Similarly, import the Elastic.LateralMovement.Visualization.Flows.Upload.yaml artifact and execute it by navigating to Server Events within the Velociraptor GUI, as illustrated in images below. This artifact is designed to automatically transmit results generated by the Lateral Movement artifact to ElasticSearch instance. Once the data is available in ElasticSearch, we can leverage Grafana to integrate and visualize the results.

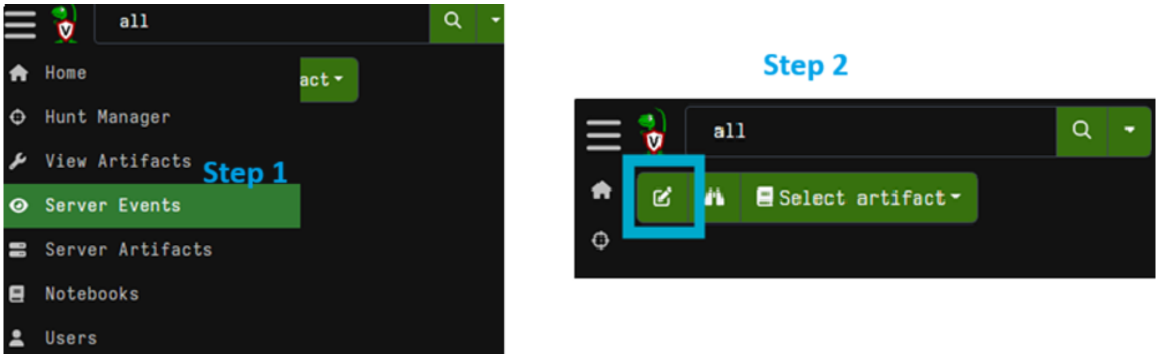
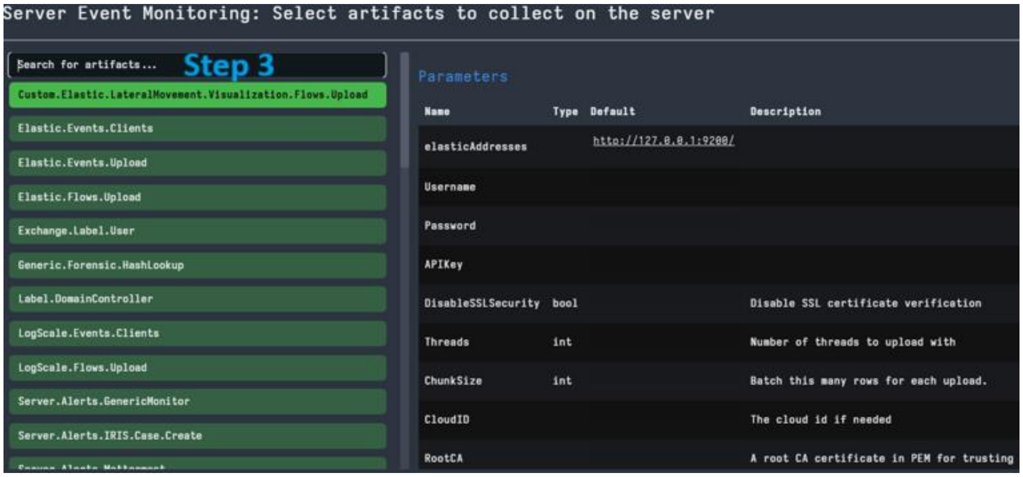


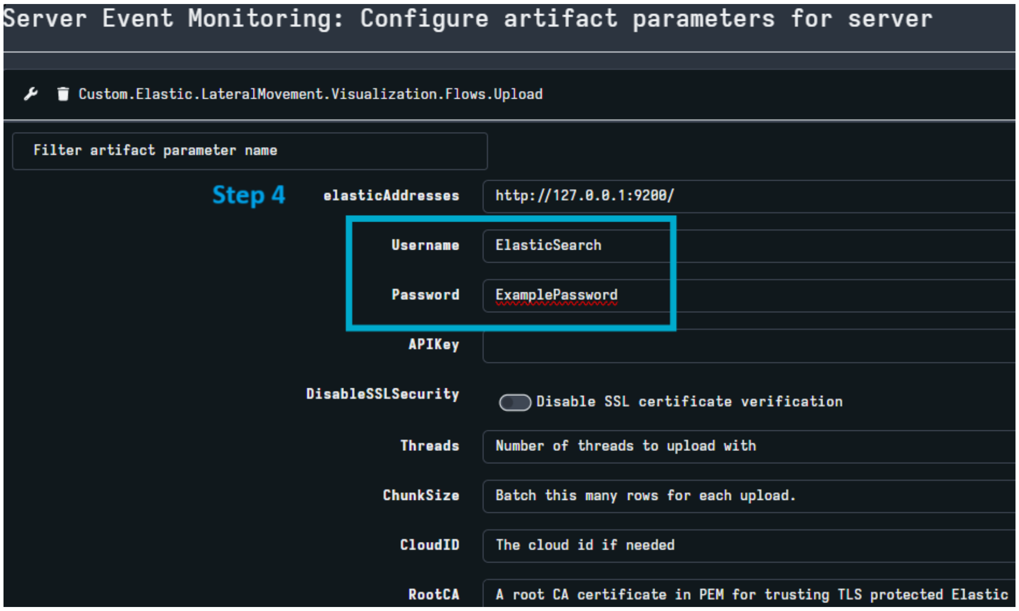
Image 7: Custom ElasticSearch server artifact execution

Please enter authentication credentials (username and password) associated with your ElasticSearch instance in the Configure Parameters window, as illustrated in images below.


Server Event Monitoring: Select artifacts to collect on the server
Search for artifacts...
Step 3
Custom.Elastic.LateralMovement.Visualization.Flows.Upload
Elastic.Events.Clients
Elastic.Events.Upload
Elastic.Flows.Upload
Exchange.Label.User
Generic.Forensic.HashLookup
Label.DomainController
LogScale.Events.Clients
LogScale.Flows.Upload
Server.Alerts.GenericMonitor
Server.Alerts.IRIS.Case.Create
Parameters

Name	Type	Default	Description
elasticAddresses		http://127.0.0.1:9200/	
Username			
Password			
APIKey			
DisableSSLSecurity	bool		Disable SSL certificate verification
Threads	int		Number of threads to upload with
ChunkSize	int		Batch this many rows for each upload.
CloudID			The cloud id if needed
RootCA			A root CA certificate in PEM for trusting

Image 8: Custom ElasticSearch server artifact execution



Server Event Monitoring: Configure artifact parameters for server

Custom.Elastic.LateralMovement.Visualization.Flows.Upload

Filter artifact parameter name

Step 4

elasticAddresses: http://127.0.0.1:9200/

Username: ElasticSearch

Password: ExamplePassword

APIKey:

DisableSSLSecurity: ○ Disable SSL certificate verification

Threads: Number of threads to upload with

ChunkSize: Batch this many rows for each upload.

CloudID: The cloud id if needed

RootCA: A root CA certificate in PEM for trusting TLS protected Elastic

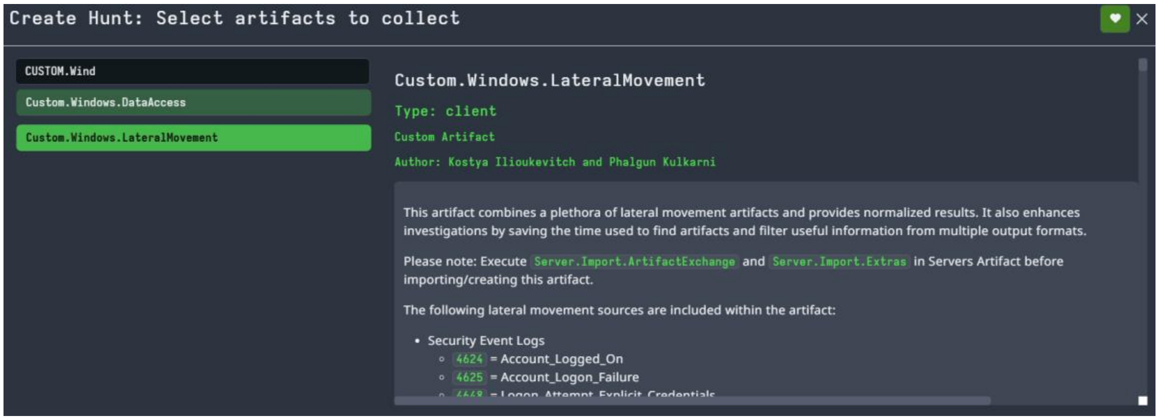
Image 9: Custom ElasticSearch server artifact configuration

Running the Artifacts

Lateral Movement Artifact Execution

To execute the Lateral Movement artifact, navigate to the Hunt Manager within the Velociraptor GUI.

1. Select the Custom.Windows.LateralMovement artifact from the list, as illustrated in the image below.



Create Hunt: Select artifacts to collect

CUSTOM.Wind

Custom.Windows.DataAccess

Custom.Windows.LateralMovement

Custom.Windows.LateralMovement

Type: client

Custom Artifact

Author: Kostya Ilioukevitch and Phalgun Kulkarni

This artifact combines a plethora of lateral movement artifacts and provides normalized results. It also enhances investigations by saving the time used to find artifacts and filter useful information from multiple output formats.

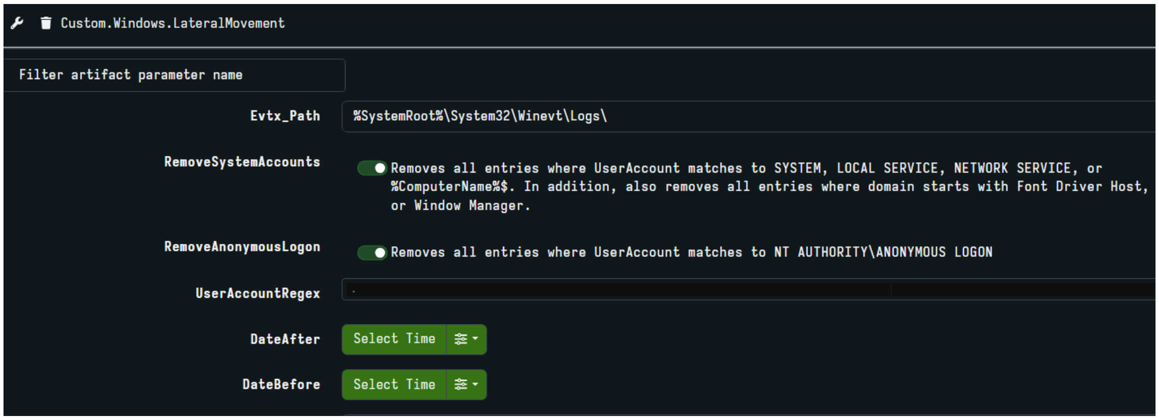
Please note: Execute `Server.Import.ArtifactExchange` and `Server.Import.Extras` in Servers Artifact before importing/creating this artifact.

The following lateral movement sources are included within the artifact:

- Security Event Logs
  - `4624` = Account_Logged_On
  - `4625` = Account_Logon_Failure
  - `4648` = Logon_Attempt_Explicit_Credentials

Image 10: Lateral Movement artifact execution

2. For the Lateral Movement artifact, it is recommended to thoroughly review the available configuration options to ensure proper alignment with your investigative objectives.



Custom.Windows.LateralMovement

Filter artifact parameter name

Evtx_Path: %SystemRoot%\System32\Winevt\Logs\

RemoveSystemAccounts: ● Removes all entries where UserAccount matches to SYSTEM, LOCAL SERVICE, NETWORK SERVICE, or %ComputerName%$. In addition, also removes all entries where domain starts with Font Driver Host, or Window Manager.

RemoveAnonymousLogon: ● Removes all entries where UserAccount matches to NT AUTHORITY\ANONYMOUS LOGON

UserAccountRegex: .

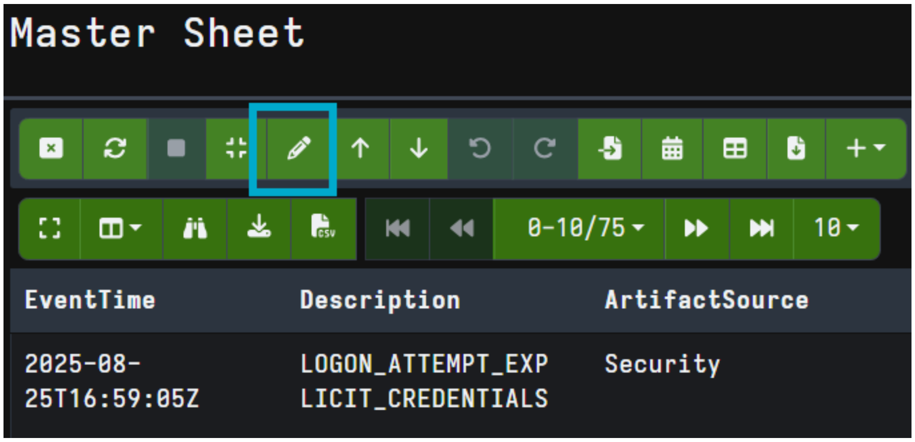
DateAfter: Select Time

DateBefore: Select Time

Image 11: Lateral Movement artifact configuration

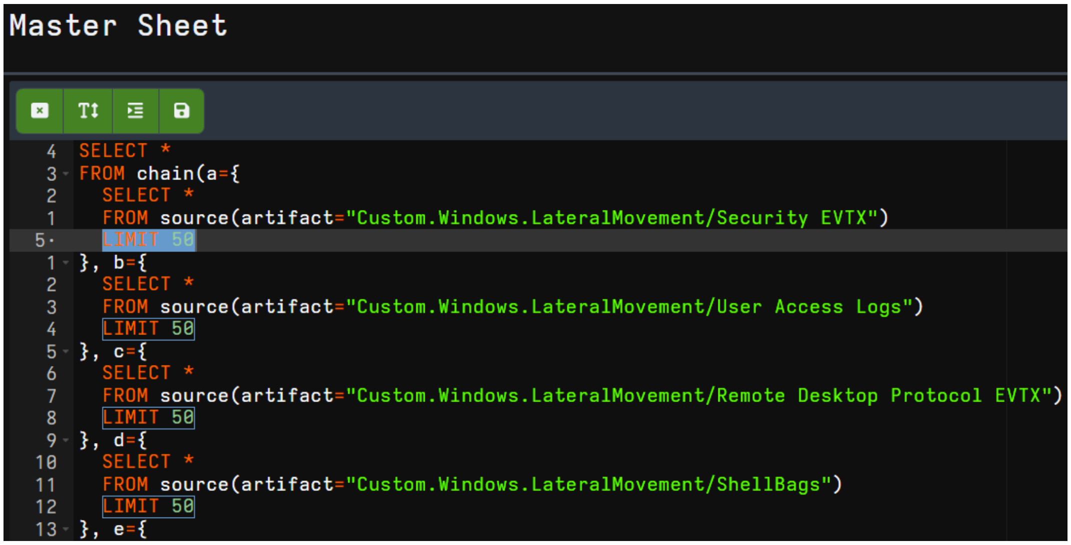
3. Two distinct result formats are provided, beginning with the Master Sheet. The Master Sheet aggregates results from all relevant artifacts, including event logs, registry keys, and any additional artifacts generated during the hunt. It is important to note that, by default, results from all artifacts are limited to 50 rows. To access the complete set of results, you may need to

remove the line “LIMIT 50” for each source in the Edit Cell section, as illustrated in the images below.



EventTime	Description	ArtifactSource
2025-08-25T16:59:05Z	LOGON_ATTEMPT_EXPLICIT_CREDENTIALS	Security

Image 12: Lateral Movement artifact Master sheet results modification

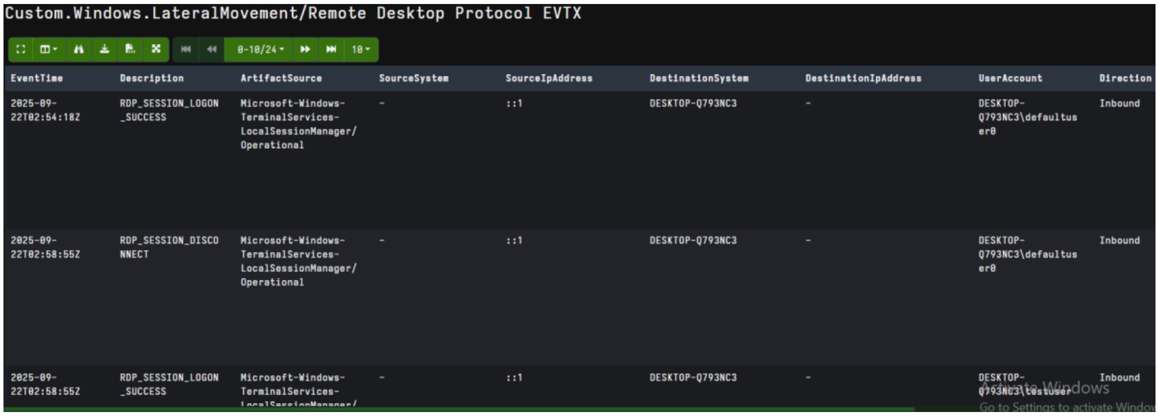


```
SELECT *
FROM chain(a={
  SELECT *
  FROM source(artifact="Custom.Windows.LateralMovement/Security EVTX")
  LIMIT 50
}, b={
  SELECT *
  FROM source(artifact="Custom.Windows.LateralMovement/User Access Logs")
  LIMIT 50
}, c={
  SELECT *
  FROM source(artifact="Custom.Windows.LateralMovement/Remote Desktop Protocol EVTX")
  LIMIT 50
}, d={
  SELECT *
  FROM source(artifact="Custom.Windows.LateralMovement/ShellBags")
  LIMIT 50
}, e={
```

Image 13: Lateral Movement artifact Master sheet results modification

4. Additionally, individual sheets are available, each presenting results generated from a single artifact. For instance, if your investigation requires an exclusive focus on RDP event logs, you may utilize the corresponding

individual sheet to isolate and review those specific results, as illustrated in image below.



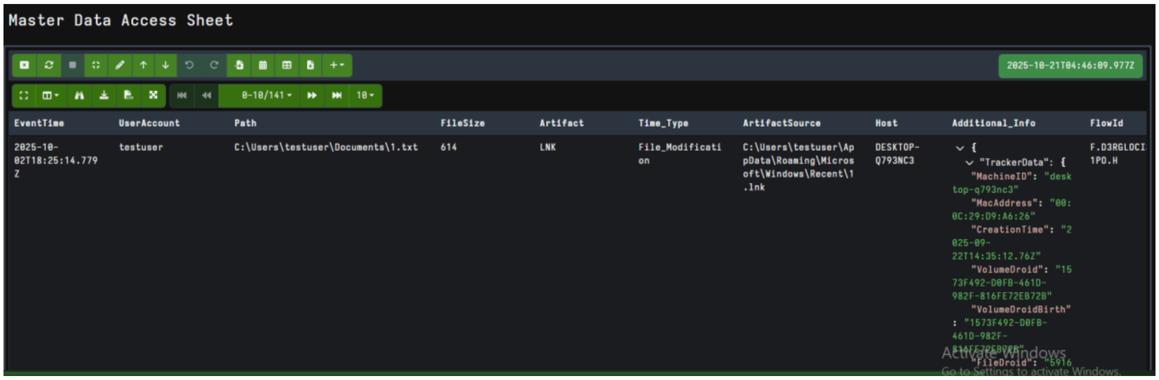
Custom.Windows.LateralMovement/Remote Desktop Protocol EVTX

EventTime	Description	ArtifactSource	SourceSystem	SourceIpAddress	DestinationSystem	DestinationIpAddress	UserAccount	Direction
2025-09-22T02:54:18Z	RDP_SESSION_LOGON_SUCCESS	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	-	::1	DESKTOP-Q793NC3	-	DESKTOP-Q793NC3\defaultuser0	Inbound
2025-09-22T02:58:55Z	RDP_SESSION_DISCONNECT	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	-	::1	DESKTOP-Q793NC3	-	DESKTOP-Q793NC3\defaultuser0	Inbound
2025-09-22T02:58:55Z	RDP_SESSION_LOGON_SUCCESS	Microsoft-Windows-TerminalServices-LocalSessionManager/	-	::1	DESKTOP-Q793NC3	-	DESKTOP-Q793NC3\testuser	Inbound

Image 14: Lateral Movement artifact individual artifact results

Data Access

1. To execute Data Access artifact, navigate to the Hunt Manager within the Velociraptor GUI and select the Custom.Windows.DataAccess artifact from the available list.
2. For parsing artifacts related to data access, two distinct options are provided: utilizing the built-in parsers or opting for third-party parsers. It is strongly recommended to thoroughly review the artifact description to gain a comprehensive understanding of the Data Access artifact's functionality and configuration requirements.
3. The results generated by the Data Access artifact mirror those of the Lateral Movement artifact in terms of structure. Both Master Sheet, which aggregate results from all relevant sources, and Individual Sheets, which present data from single artifacts, are available for review, as illustrated in the image below.



EventTime	UserAccount	Path	FileSize	Artifact	Time_Type	ArtifactSource	Host	Additional_Info	FlowId
2025-10-02T18:25:14.779Z	testuser	C:\Users\testuser\Documents\1.txt	614	LNK	File_Modification	C:\Users\testuser\AppData\Roaming\Microsoft\Windows\Recent\1.lnk	DESKTOP-Q793NC3	{ "TrackerData": { "MachineID": "desktop-q793nc3" "MacAddress": "00:0C:29:D9:A6:26" "CreationTime": "2025-09-22T14:35:12.76Z" "VolumeDroid": "1573F492-D0FB-461D-982F-816FE72EB72B" "VolumeDroidBirth": "1573F492-D0FB-461D-982F-816FE72EB72B" "FileDroid": "5916	F.D3RGLOCI1PO.H

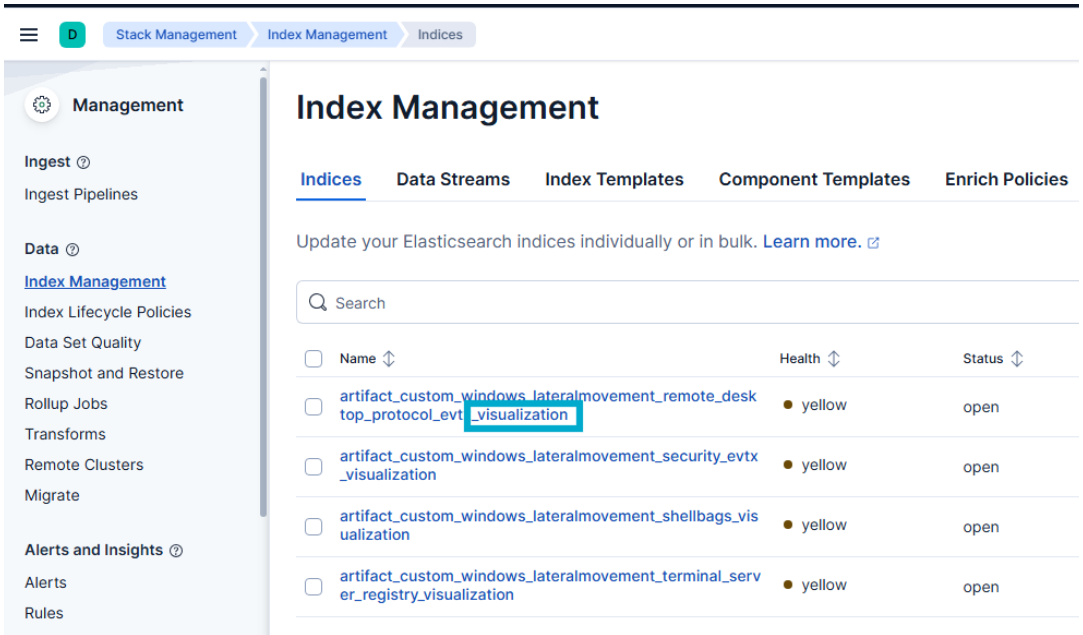
Image 15: Data Access artifact Master sheet results

Visualizing Lateral Movement Results

We showcase two primary methods for visualizing Lateral Movement results in a node-edge graph format: Grafana and Jupyter Notebook.

Visualization using Grafana

1. To begin with Grafana, first ensure that the results from the Lateral Movement hunt are accessible within the Velociraptor GUI. Next, navigate to Kibana and proceed to Stack Management > Index Management to locate the Lateral Movement indexes designated for visualization; these indexes are identified by the "_visualization" suffix. Indexes are specifically formatted for integration and visualization within Grafana, as illustrated in the image below. The index names can be copied and entered in Grafana configuration to facilitate integration with ElasticSearch.



Index Management

Update your Elasticsearch indices individually or in bulk. Learn more.

	Name	Health	Status
□	artifact_custom_windows_lateralmovement_remote_desktop_protocol_evt_visualization	● yellow	open
□	artifact_custom_windows_lateralmovement_security_evtx_visualization	● yellow	open
□	artifact_custom_windows_lateralmovement_shellbags_visualization	● yellow	open
□	artifact_custom_windows_lateralmovement_terminal_server_registry_visualization	● yellow	open

Image 16: Lateral movement visualization indexes in Kibana

2. In Grafana, proceed by adding an ElasticSearch data source within the Connections section, as illustrated in the image below.

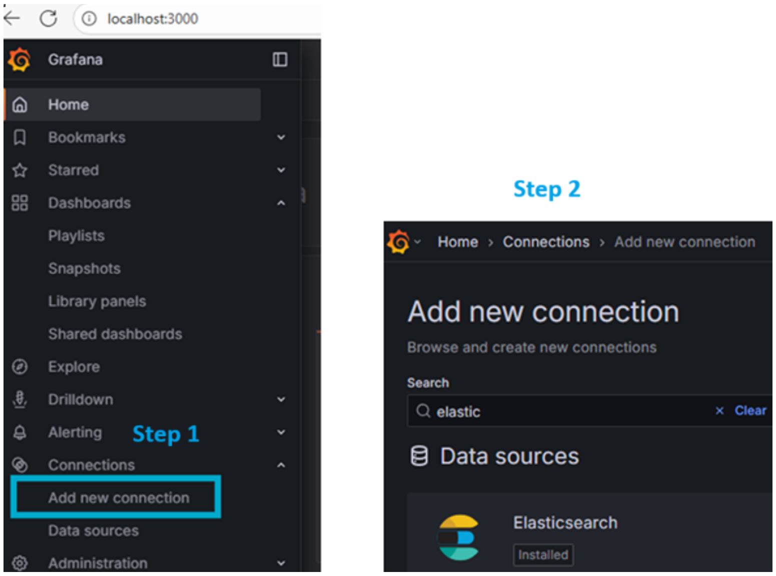
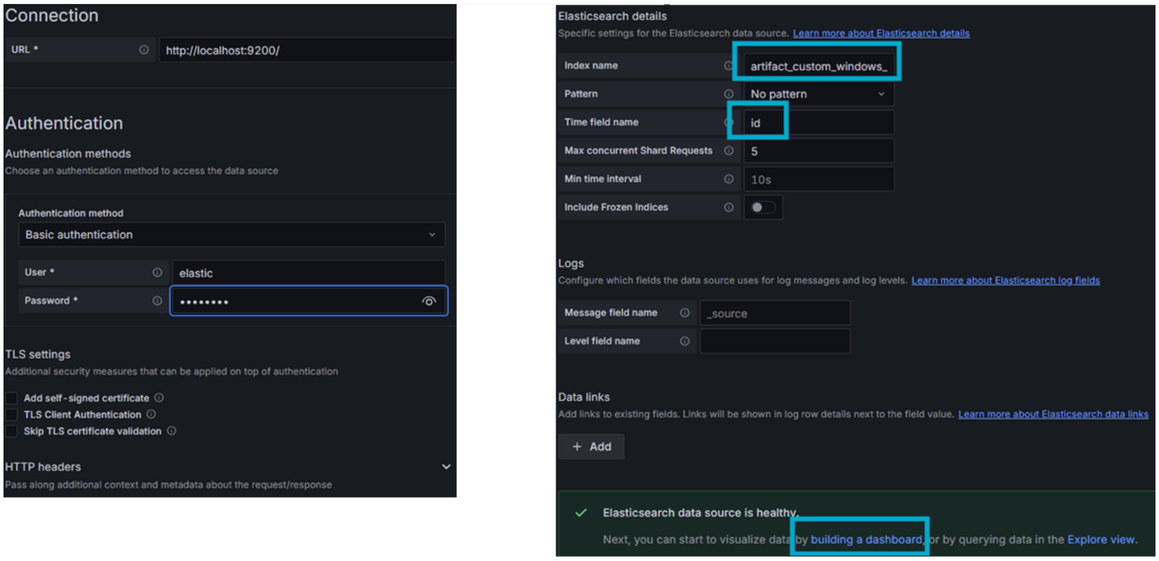


Image 17: Adding ElasticSearch connection in Grafana

3. Provide the necessary connection details for ElasticSearch instance. It is essential to modify the Time field name to “id” to ensure proper functionality. After entering all required information, select “Save & Test” to validate the configuration. Upon successful connection, a confirmation message stating “data source is healthy” will appear. You may then proceed by selecting “Building a Dashboard” to initiate the creation of a node-edge graph, as illustrated in the image below.



Connection

URL * http://localhost:9200/

Authentication

Authentication methods

Choose an authentication method to access the data source

Authentication method: Basic authentication

User * elastic

Password * ••••••••

TLS settings

Additional security measures that can be applied on top of authentication

□ Add self-signed certificate

□ TLS Client Authentication

□ Skip TLS certificate validation

HTTP headers

Pass along additional context and metadata about the request/response

Elasticsearch details

Specific settings for the Elasticsearch data source. Learn more about Elasticsearch details

Index name: artifact_custom_windows_

Pattern: No pattern

Time field name: id

Max concurrent Shard Requests: 5

Min time interval: 10s

Include Frozen Indices: ○

Logs

Configure which fields the data source uses for log messages and log levels. Learn more about Elasticsearch log fields

Message field name: _source

Level field name:

Data links

Add links to existing fields. Links will be shown in log row details next to the field value. Learn more about Elasticsearch data links

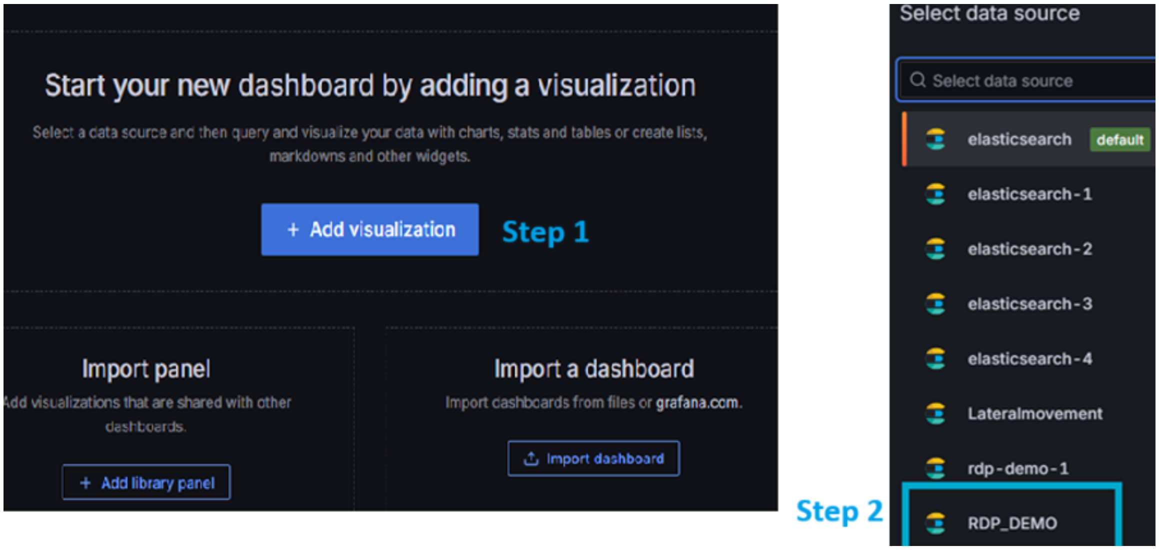
+ Add

✓ Elasticsearch data source is healthy.

Next, you can start to visualize data by building a dashboard, or by querying data in the Explore view.

Image 18: Adding ElasticSearch connection in Grafana

4. Begin by clicking Add visualization button and selecting the newly configured data source, as illustrated in the image below.



Start your new dashboard by adding a visualization

Select a data source and then query and visualize your data with charts, stats and tables or create lists, markdowns and other widgets.

+ Add visualization

Step 1

Import panel

Add visualizations that are shared with other dashboards.

+ Add library panel

Import a dashboard

Import dashboards from files or grafana.com.

Import dashboard

Step 2

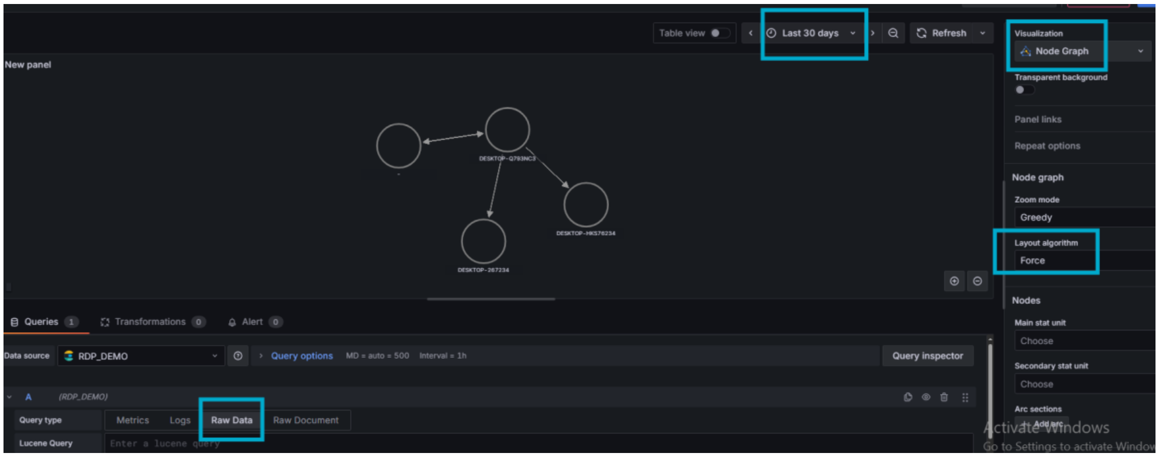
Select data source

Select data source

- elasticsearch default
- elasticsearch-1
- elasticsearch-2
- elasticsearch-3
- elasticsearch-4
- Lateralmovement
- rdp-demo-1
- RDP_DEMO

Image 19: Creating Lateral Movement visualization in Grafana

5. Once the data source has been selected, configure the visualization settings as follows: set the query type to “Raw Data,” apply the appropriate time filter, select “Node Graph” as the visualization format, and adjust the layout algorithm to ensure the visual is appropriately scaled, as illustrated in the image below.



Data source: RDP_DEMO

Query type: Raw Data

Visualization: Node Graph

Zoom mode: Greedy

Layout algorithm: Force

Image 20: Creating Lateral Movement visualization in Grafana

Visualization using Jupyter Notebook

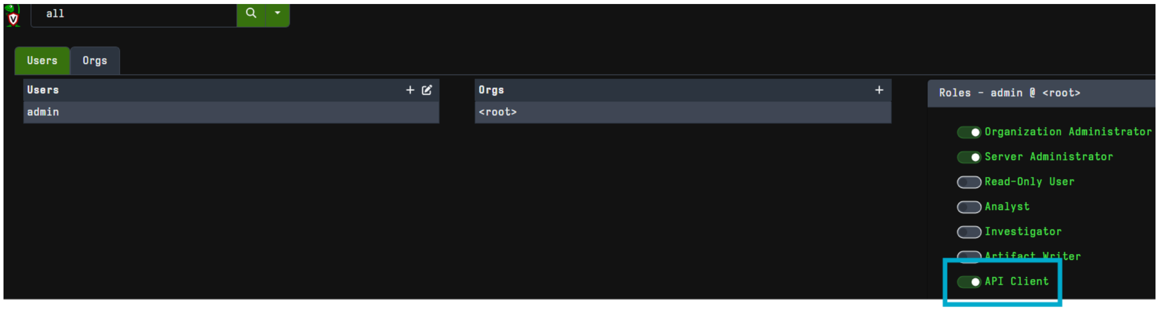
1. To visualize Lateral Movement artifact results using Jupyter Notebook, begin by generating a Velociraptor API configuration file by executing the following Velociraptor command in an elevated command prompt:

   ```
   $ velociraptor --config server.config.yaml config api_client --name   --role administrator api.config.yaml
   ```

2. After creating the API configuration file, verify API connectivity by executing the following Python command in an elevated command prompt:

   ```
   $pyvelociraptor --config api.config.yaml "SELECT * FROM info()"
   ```

   If you encounter permission issues, then confirm that API Client permission has been assigned to respective user within the Velociraptor GUI, as illustrated in the image below.

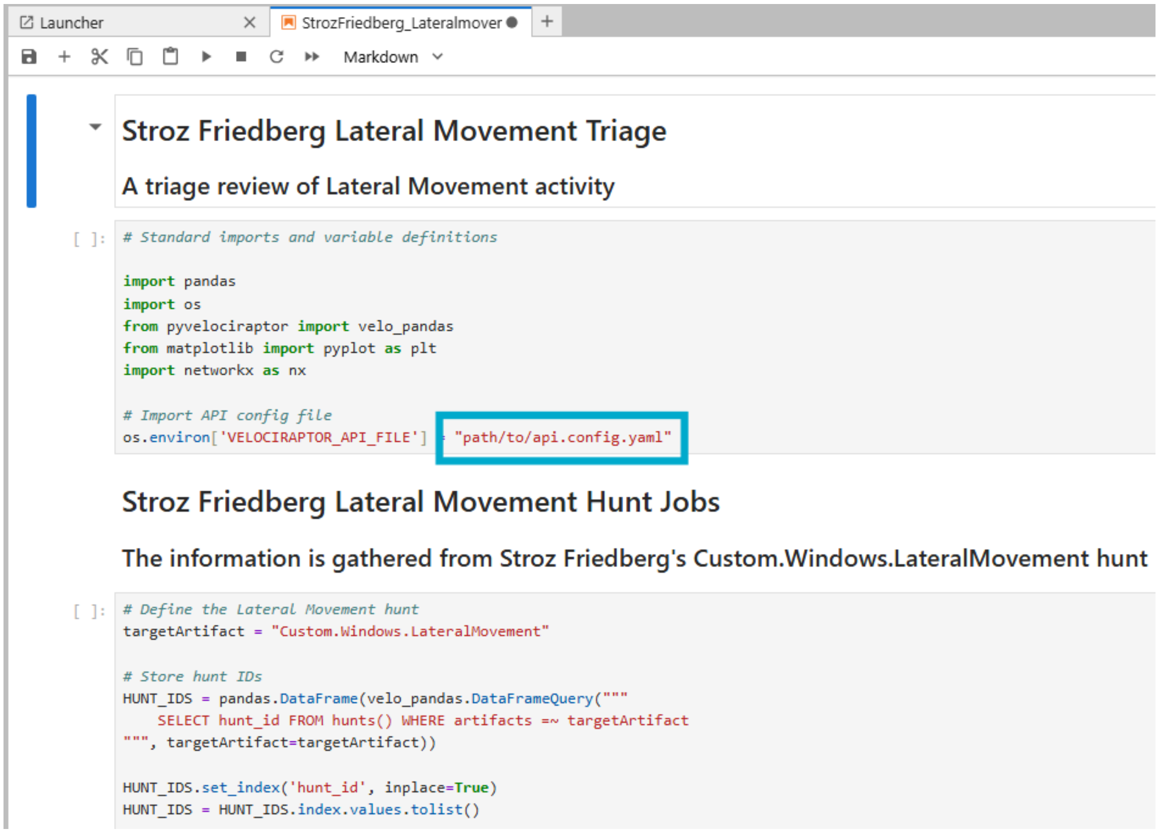


Roles - admin @ <root>

- ● Organization Administrator
- ● Server Administrator
- ○ Read-Only User
- ○ Analyst
- ○ Investigator
- ○ Artifact Writer
- ● API Client

Image 21: Setting API Client permission in Velociraptor

3. Navigate to Jupyter Notebook and import the StrozFriedberg_Lateralmovement_visualization.ipynb notebook.
4. Ensure that you specify the complete file path for the api.config.yaml configuration file in the code highlighted in the image below, then execute the corresponding cells to proceed.



Stroz Friedberg Lateral Movement Triage

A triage review of Lateral Movement activity

```
[ ]: # Standard imports and variable definitions

     import pandas
     import os
     from pyvelociraptor import velo_pandas
     from matplotlib import pyplot as plt
     import networkx as nx

     # Import API config file
     os.environ['VELOCIRAPTOR_API_FILE'] = "path/to/api.config.yaml"
```

Stroz Friedberg Lateral Movement Hunt Jobs

The information is gathered from Stroz Friedberg's Custom.Windows.LateralMovement hunt

```
[ ]: # Define the Lateral Movement hunt
     targetArtifact = "Custom.Windows.LateralMovement"

     # Store hunt IDs
     HUNT_IDS = pandas.DataFrame(velo_pandas.DataFrameQuery("""
         SELECT hunt_id FROM hunts() WHERE artifacts =~ targetArtifact
     """, targetArtifact=targetArtifact))

     HUNT_IDS.set_index('hunt_id', inplace=True)
     HUNT_IDS = HUNT_IDS.index.values.tolist()
```

Image 22: Jupyter notebook for Lateral Movement visualization

The final cell will generate a node-edge graph representing the results derived from the Lateral Movement artifact. The resulting visualization should closely resemble the example provided in the image below.

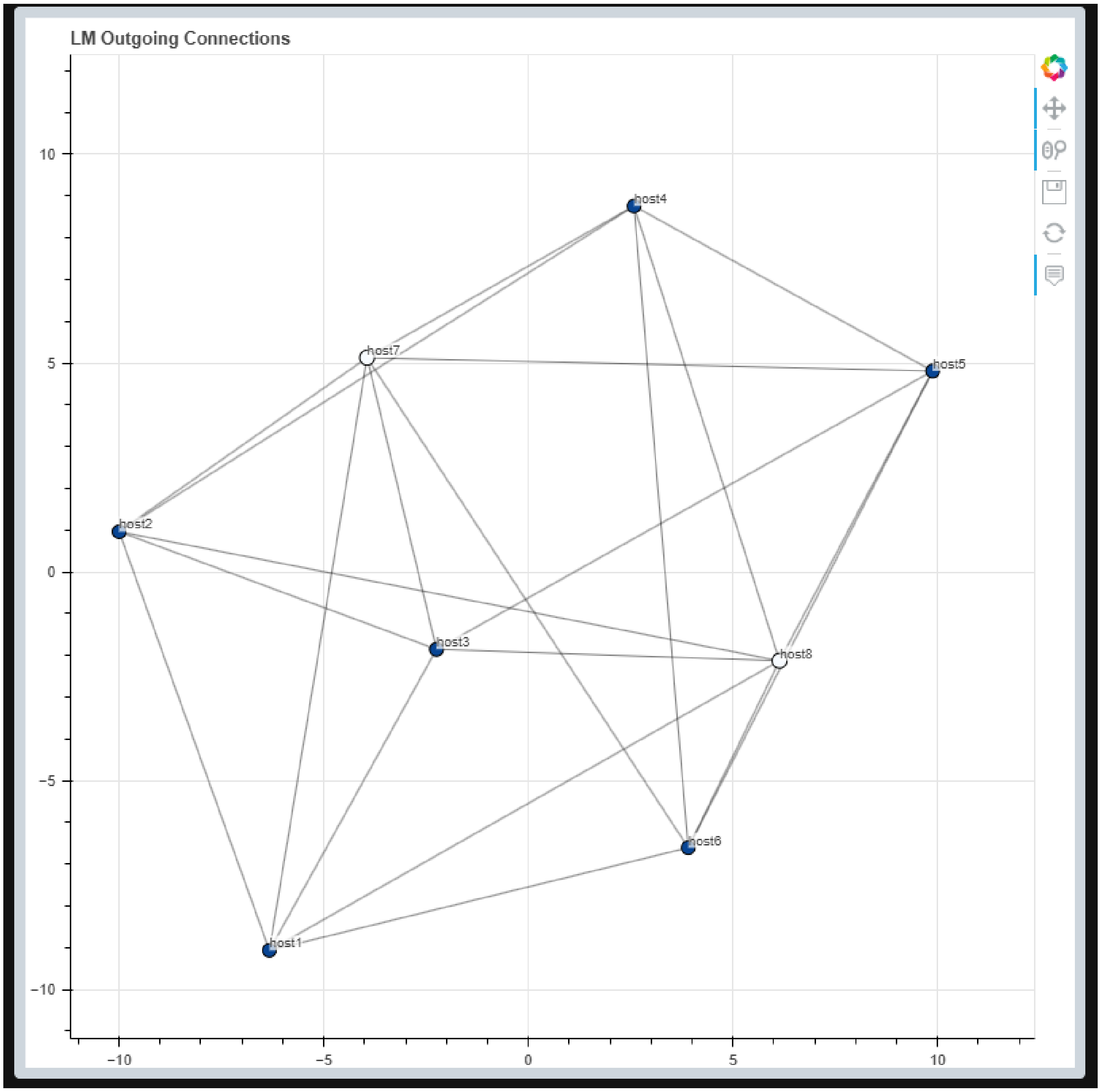
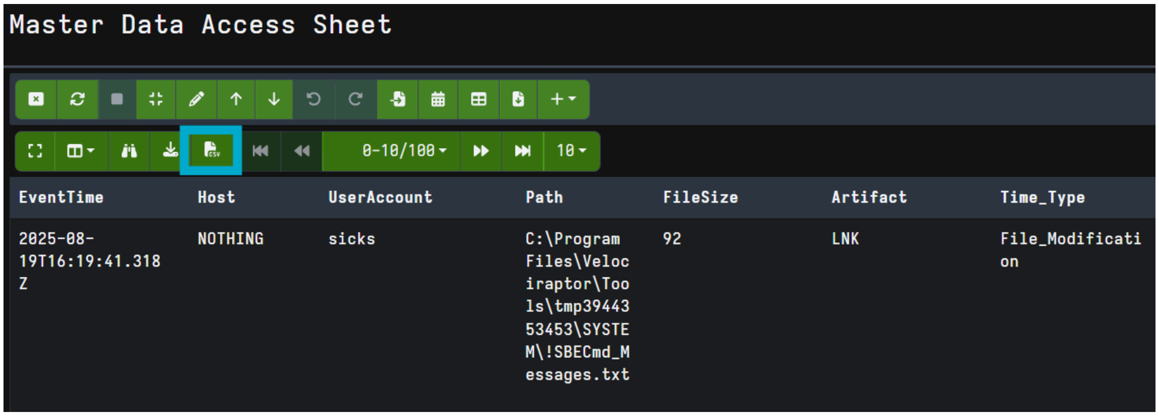


Image 23: Creating Lateral Movement visualization in Jupyter Notebook

Presenting Data Access Results

The Data Access artifact is engineered to generate results in a timeline format, facilitating integration with a custom Excel template specifically designed to efficiently present data access findings to stakeholders. You may export the Master sheet generated by DataAccess artifact in a CSV format from Velociraptor

GUI, as illustrated in the image below and paste results into appropriate columns present in the excel template can be accessed here.



Master Data Access Sheet

EventTime	Host	UserAccount	Path	FileSize	Artifact	Time_Type
2025-08-19T16:19:41.318Z	NOTHING	sicks	C:\Program Files\Velociraptor\Tools\tmp3944353453\SYSTEM\!SBECmd_Messages.txt	92	LNK	File_Modification

Image 24: Downloading Data Access Master sheet results in CSV format from Velociraptor

Excel Template Structure and Usage

The Excel template provided for presenting Data Access artifact results is organized into three distinct tabs, each designed to facilitate effective review and communication of findings to stakeholders.

Overview Tab

- Coloring Legend and Conditional Formatting: The overview tab includes a coloring legend to assist users in highlighting rows that match specific criteria. Conditional formatting rules are implemented to automatically highlight cells containing keywords such as “finance” or “human resources,” thereby enabling identification of potentially sensitive data access.
- Forensic Artifact Definitions: Definitions for forensic artifacts are provided to ensure that non-technical audiences can understand the sources of data access.

- Review Methods: The tab outlines several recommended review methods that can be employed to identify anomalous data access activity.

What-if Scenarios Tab

- This tab documents various scenarios in which a threat actors' actions may or may not produce data access artifacts on source or target systems. These scenarios can be essential for explaining instances where evidence of data access is absent.

Data Touching Events Tab

- The Data Touching Events tab is configured to accept results from the Data Access (DA) artifact. The DA artifact output is tailored to align with the columns present in the tab.
- Conditional rules are applied to the Path column, automatically highlighting cells containing specified keywords with corresponding colors.
- It is important to note that timestamps associated with Shellbags and Most Recently Used (M.R.U) registry keys do not reflect the precise time of data access. Instead, these timestamps indicate the time of registry key modification, which may differ from the actual access time due to the nature of forensic artifact.