LOGPOINT

Integrations

Process Tree

V5.0.0 (latest)

CONTENTS

CHAPTER

ONE

PROCESS TREE

Process tree is a hierarchical representation of processes and their relationships within a Windows operating system. It details parent-child processes, showing how one process can spawn or create other processes over time. In Logpoint, Process Tree supports WindowsSysmon logs that assign each process a unique identity, *process_guid*.

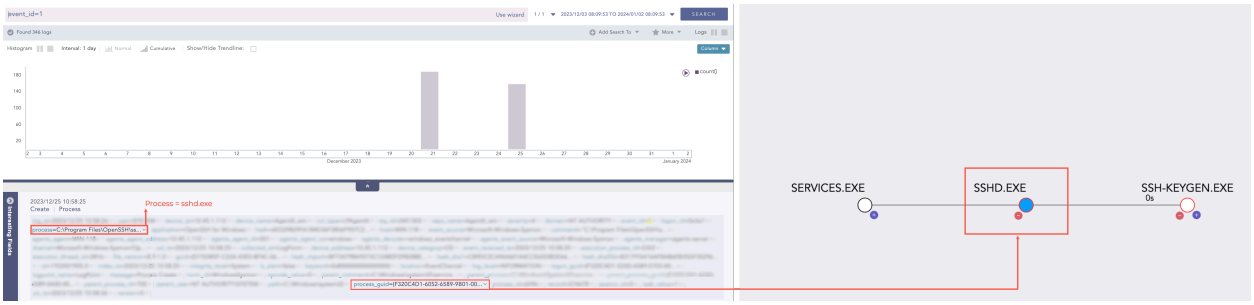
For example:

In a Sysmon indexed log with the event ID 1, a **LogonUI.exe** process is assigned the GUID **{F320C4D1-6051-6589-9A01-00000000A400}**. Its parent process **winlogon.exe** is assigned the GUID **{F320C4D1-5A94-6589-5201-00000000A400}**.

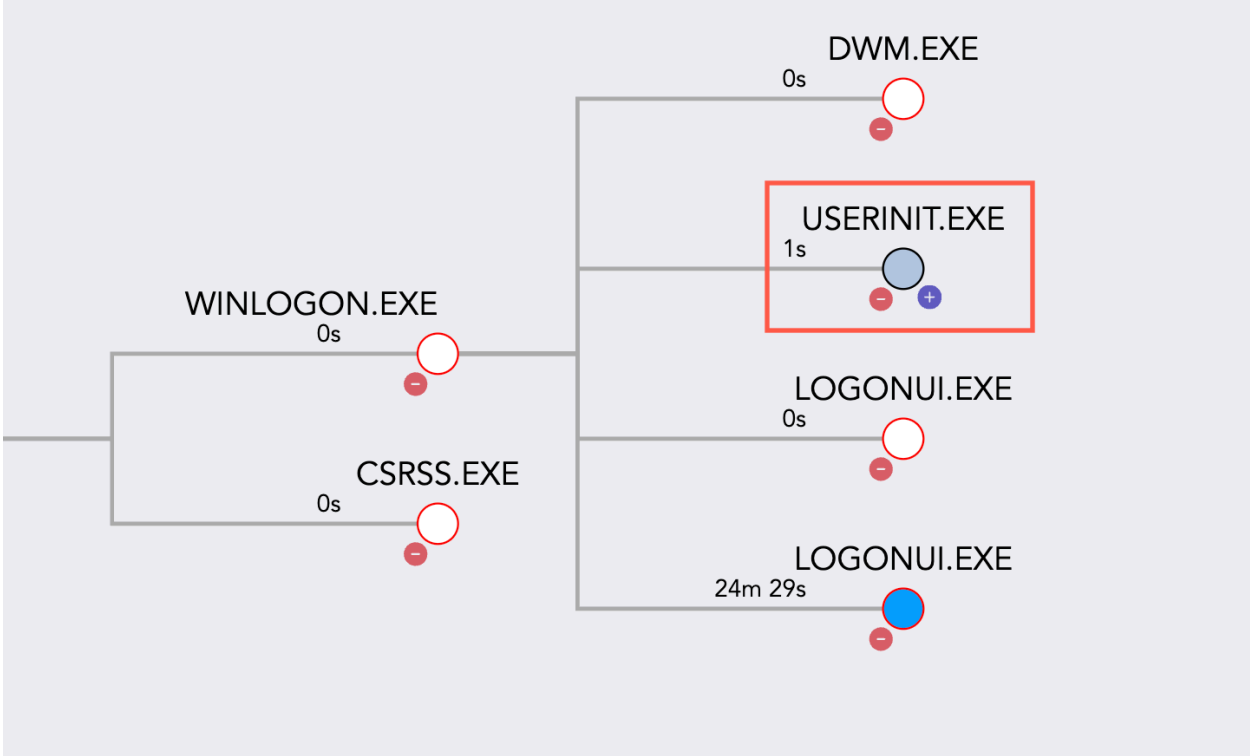
Process Tree helps you study the relationships between active processes, discover resource utilization, and debug process execution issues. Unusual process linkages or unexpected child processes might indicate security concerns. Viewing the Process Tree can help spot such anomalies or irregularities. To view a tree, search for Sysmon logs from Search, then click *Visualize Process Tree With {guid}* from the *parent_process_guid* or *process_guid* value drop-down.

Process Tree UI Labels

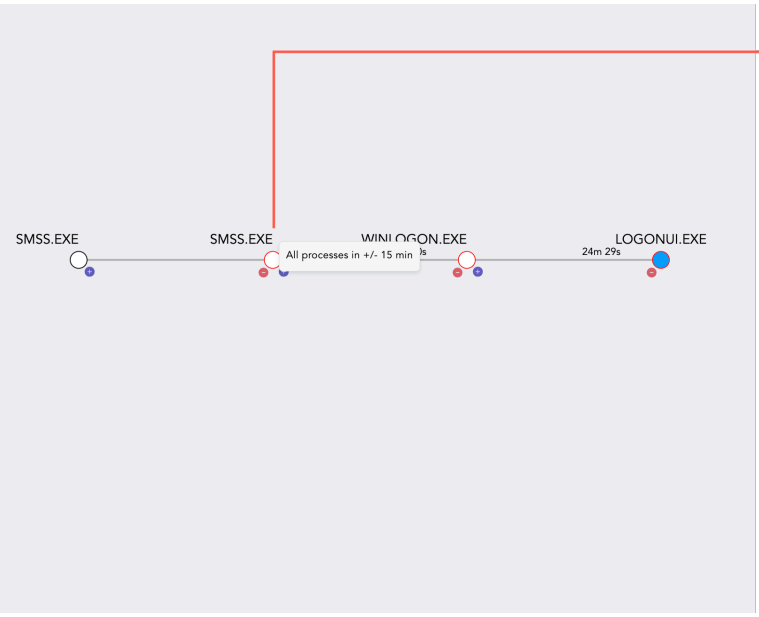
- Each node in the tree represents a process, and the lines connecting nodes indicate parent-child relationships. A line displays the relative time a child process was created after the creation of its parent process.
- A bright blue color node represents the focused node in Process Tree. It indicates from where in Search you are directed to a Process Tree. It can be **parent_process_guid** or **process_guid**.

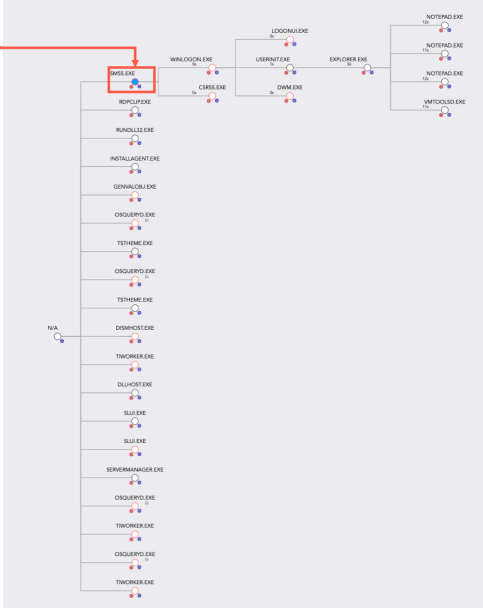


- A light blue node represents the process's child nodes are present but not expanded.

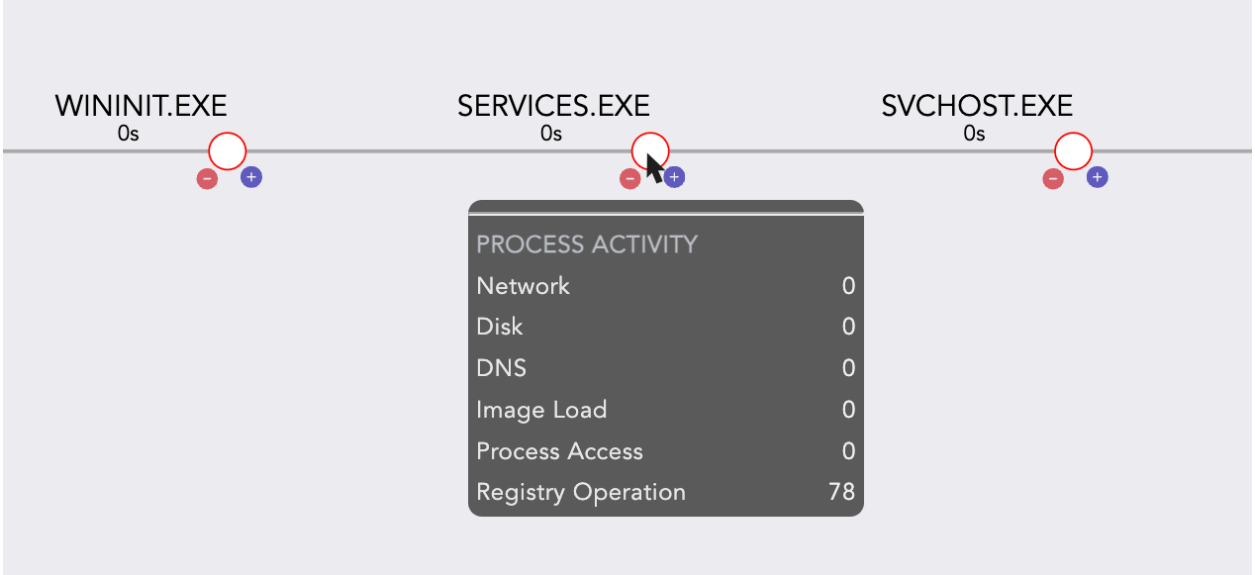


- button fetches and displays the child processes nodes related to the parent process.
- button hides the child processes nodes from its parent process node.
- Right-click any node, you will get the **All processes in +/- 15min** button. Click it and you will see a new process tree that shows all the processes created 15 minutes prior and later, relative to the node you selected.





- Hover on a node to view its process activity details like network, DNS, disk and registry operation.



CHAPTER

TWO

INSTALLING PROCESS TREE

Prerequisite

Logpoint v6.12.2 or later

To install Process Tree:

1. Download the .pak file from the Help Center.
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

After installing Process Tree, you can find it under *Settings >> System Settings >> Plugins*.

CHAPTER

THREE

UNINSTALLING PROCESS TREE

1. Go to *Settings >> System Settings* from the naviagtion bar and click **Applications**.
2. Click the **Uninstall** icon from **Actions** of ProcessTree.
3. Click **Yes**.

CHAPTER

FOUR

ACCESSING PROCESS TREE

You must have configured Sysmon Configuration in your Windows to collect Sysmon logs. Go to Sysmon Configuration to learn how to configure it correctly. Logpoint allows you to access Process Tree from **Search**. Go to Search to learn about search.

1. In the navigation bar, click **Search**.
2. In **Search Bar**

   2.1 Enter a query to search WindowsSysmon logs. You must use **parent_process_guid** or **process_guid** fields for search queries to avoid errors. For example, *"process_guid" = ** and *"parent_process_guid" = **.

   2.2 Select a **Repo**.

   2.3 Set a time range.
3. Click **Search**.

The search results must contain the **process**, **parent_process**, **parent_process_guid** and **process_guid** fields.

Fig. 1: Searching WindowsSysmon Indexed Log

4. In search results, click **parent_process_guid** or **process_guid** value drop-down.

5. Click **Visualize Process Tree With {guid}** which takes you to **PROCESS TREE**. The **{guid}** value varies depending on whether they are based on the **parent_process_guid** or **process_guid** field.

Fig. 2: Accessing Process Tree

6. Click a node to view its process details in **Preview Selected**. In **SHA1**, click **Analyze VirusTotal Score** to go to the VirusTotal website for hash analysis of the selected process. The hash analysis enables you to identify known files without manually opening and inspecting them.

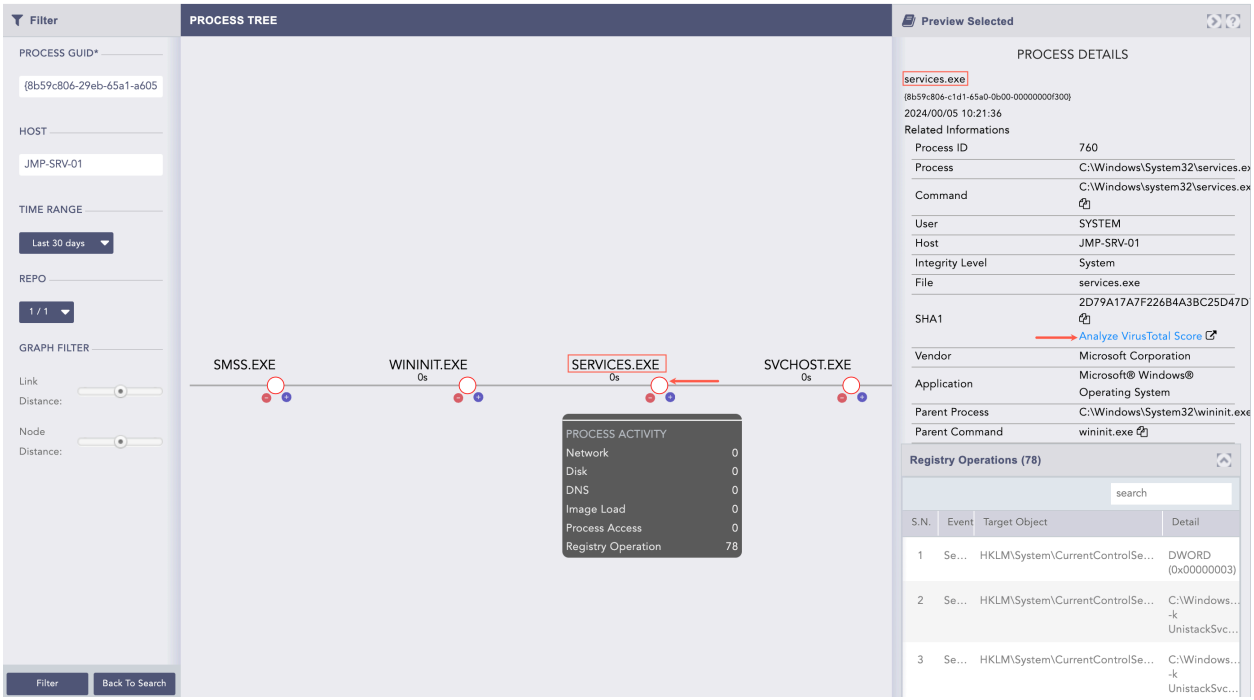


Fig. 3: Generating a Process Tree

To return to **Search**, click **Back To Search**. You can now enter a new query to get new **parent_process_guid** and **process_guid** or edit the filter to generate a new process tree. The **PROCESS GUID**, **HOST**, **TIME RANGE** and **REPO** are auto-fetched from Search, which can still be edited.

To edit Filter:

You need to first access the Process Tree from Search to enable editing the filter. The filter allows you to generate a new process tree by entering a **PROCESS GUID**, setting a **TIME RANGE** and selecting a **REPO** only. It reduces the need to search for Sysmon logs.

1. Enter a valid **PROCESS GUID**.
2. Enter a **HOST** if you have one.
3. Set a **TIME RANGE**.
4. Select a **REPO**.
5. Click **Filter**.

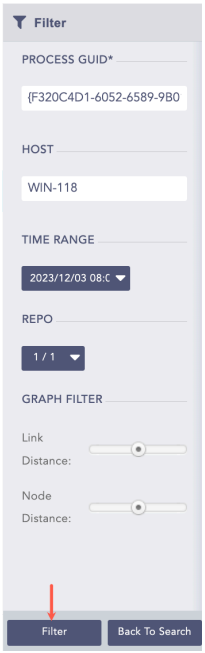


Fig. 4: Editing Filter

Use the **Link Distance** and **Node Distance** to adjust the tree view.

Click on a node to view its process details. The **Preview Selected** expands which contains process's informations like Process ID, Process, Command and SHA1 along with process detail process activities like network operation, disk operation, dns request, registry operation , image load and process access.