

TP N°1

La Collecte des Logs avec Syslog et Sysmon

I- Rsyslog sur Linux

Introduction à Syslog

Le protocole Syslog est un standard largement utilisé pour la collecte, le stockage et la transmission des journaux système (logs) dans les environnements informatiques. Introduit à l'origine sur les systèmes Unix, Syslog est devenu un élément fondamental pour la supervision, l'audit et la sécurité des systèmes d'exploitation modernes, qu'ils soient Linux, macOS ou Windows (via des agents de compatibilité).

Son objectif principal est de centraliser les messages générés par les différents services, applications et composants du système, tels que le noyau, le serveur SSH, ou les services réseau. Ces messages sont classés selon deux critères :

- La priorité (severity) — indiquant le niveau d'importance ou de gravité du message (de *debug* à *emergency*).
- La facilité (facility) — représentant la source ou la catégorie du message (par exemple : *auth*, *daemon*, *kern*, *mail*).

Les messages Syslog peuvent être stockés localement dans des fichiers de log (comme `/var/log/syslog` ou `/var/log/messages`), ou bien transmis à un serveur distant via le réseau pour permettre une gestion centralisée des événements. Ce mécanisme est essentiel pour la corrélation d'événements de sécurité, la détection d'incidents et la traçabilité dans les environnements distribués.

Afin d'étendre les fonctionnalités du protocole Syslog traditionnel, plusieurs implémentations modernes ont vu le jour, dont rsyslog (The Rocket-fast Syslog). Rsyslog est une version améliorée et modulaire de Syslog offrant :

- Une performance accrue grâce au multithreading,
- Le chiffrement et la transmission sécurisée via TLS,
- Le filtrage et le routage avancé des messages,
- La compatibilité avec d'autres formats de logs (JSON, Elasticsearch, etc.).

Dans ce TP, vous allez explorer le fonctionnement de rsyslog, comprendre sa configuration locale et distante, et apprendre à centraliser les logs de plusieurs machines dans un serveur unique de supervision.

1. Installation de serveur Rsyslog

Le serveur Rsyslog intégré dans les distributions Linux installer le avec la commande apt install rsyslog.

```
[# apt install rsyslog
Installing:
  rsyslog

Installing dependencies:
  libestri0  libfastjson4  liblognorm5
  Home

Suggested packages:
  rsyslog-mysql    rsyslog-mongodb  rsyslog-openssl  rsyslog-gssapi
  | rsyslog-pgsql   rsyslog-doc      | rsyslog-gnutls  rsyslog-relp

Summary:
  Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 2086
  Download size: 858 kB
  Space needed: 2,346 kB / 56.7 GB available

  Continue? [Y/n] y
```

2. Configuration de serveur

Décommenter les 2 lignes surlignées dans le fichier « /etc/rsyslog.conf »

```
[root@kali]# nano /etc/rsyslog.conf
```

Ayant :

```
# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")
```

```
# provides TCP syslog reception  
#module(load="imtcp")  
#input(type="imtcp" port="514")
```

Après :

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

3. Redémarrer le service Rsyslog

Redémarrer le service Rsyslog avec la commande : `systemctl restart rsyslog.service`

```
[root@kali]# systemctl restart rsyslog.service
```

4. Vérification

- Les logs d'authentification : tail -f /var/log/auth.log

```
[root@kali)-[~/home/kali]
# tail -f /var/log/auth.log
2025-03-22T06:18:35.818688-04:00 kali lightdm: gkr-pam: unable to locate daemon control file
2025-03-22T06:18:35.820653-04:00 kali lightdm: gkr-pam: stashed password to try later in open session
2025-03-22T06:18:36.373612-04:00 kali lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
2025-03-22T06:18:36.374353-04:00 kali lightdm: pam_systemd(lightdm-greeter:session): New sd-bus connection (system-bus-pam-sy
stemd-213697) opened.
2025-03-22T06:18:36.392057-04:00 kali lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
2025-03-22T06:18:36.421784-04:00 kali lightdm: pam_systemd(lightdm-greeter:session): Failed to release session: Transport end
point is not connected
2025-03-22T06:18:36.465968-04:00 kali systemd-logind[466]: Removed session c12.
2025-03-22T06:18:47.133125-04:00 kali systemd-logind[466]: Removed session 84.
2025-03-22T06:45:01.860213-04:00 kali CRON[227325]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-03-22T06:45:01.870001-04:00 kali CRON[227325]: pam_unix(cron:session): session closed for user root
```

- Les logs des erreurs système : tail -f /var/log/kern.log

```
[root@kali]~[~/home/kali]
# tail -f /var/log/kern.log
2025-03-22T05:59:01.405520-04:00 kali kernel: pcnet32 0000:00:09.0 eth0: entered promiscuous mode
2025-03-22T05:59:01.405521-04:00 kali kernel: pcnet32 0000:00:09.0 eth0: left promiscuous mode
2025-03-22T05:59:01.405525-04:00 kali kernel: 10:48:04.883114 control Session 0 is about to close ...
2025-03-22T05:59:01.405525-04:00 kali kernel: 10:48:04.899078 control Stopping all guest processes ...
2025-03-22T05:59:01.405526-04:00 kali kernel: 10:48:04.926207 control Closing all guest files ...
2025-03-22T05:59:01.405526-04:00 kali kernel: 10:48:04.928662 control vbglR3GuestCtrlrDetectPeekGetCancelSupport: Supported (#1)
2025-03-22T05:59:01.405527-04:00 kali kernel: 09:52:58.172360 timesync vgsvcTimeSyncWorker: Radical host time change: 255 901
 680 000 000ns (HostNow=1 742 637 178 172 000 00
2025-03-22T06:39:01.148535-04:00 kali kernel: 09:53:08.174581 timesync vgsvcTimeSyncWorker: Radical guest time change: 255 901
 682 255 000ns (GuestNow=1 742 637 188 174 461
2025-03-22T06:39:01.148556-04:00 kali kernel: pcnet32 0000:00:09.0 eth0: entered promiscuous mode
2025-03-22T06:39:02.978159-04:00 kali kernel: pcnet32 0000:00:09.0 eth0: left promiscuous mode
```

- Logs des connexions utilisateurs : tail -f /var/log/wtmp

```
[root@kali]~[~/home/kali]
# tail -f /var/log/wtmp
~~reboot6.8.11-amd64#g~~runlevel6.8.11-amd64(%g|*Dtty1tty1D)%g[g(RDtty1tty1LOGIND)%g[R*tty7:0kali:0I%gq*Dtty1tty1D*g
~~reboot6.8.11-amd64#g+g~~shutdown6.8.11-amd64*g+z~~reboot6.8.11-amd64{'*g**' 5~~runlevel6.8.11-amd64'*g+chtty1tty1h+'*g
htt1tty1LOGINh+'*g*tty7:0kali:0a(*g+htt1tty1hh+g+U
tty7:0kali:0f*g9~~shutdown6.8.11-amd64@gM~~reboot6.8.11-amd64***gT*5~~runlevel6.8.11-amd64***g+
*ttty1tty1***gB
*ttty1tty1LOGIN****gB
~~reboot6.8.11-amd64H*g]*5~~runlevel6.8.11-amd64Y*g)yttt1tty1yZ**g**yttt1tty1LOGINyZ**g**+tty7:0kali:0m**gyttt1tty1y*Y*g
~~reboot6.8.11-amd64*Zgr*5~~runlevel6.8.11-amd64*Z*g)ntty1tty1n*Z*g+natty1tty1LOGINn*Z*g+ tty7:0kali:0*Z*g.
```

- Les logs en temps réel : journalctl -f

```
[root@kali)-[~/home/kali]
# journalctl -f
Mar 22 06:47:00 kali systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service ...
Mar 22 06:47:00 kali dbus-daemon[459]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Mar 22 06:47:00 kali systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Mar 22 06:47:10 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Mar 22 06:52:00 kali NetworkManager[517]: <info> [1742640720.6963] dhcpc4 (eth0): state changed new lease, address=192.168.5.
4
Mar 22 06:52:00 kali dbus-daemon[459]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.5' (uid=517 comm="/usr/sbin/NetworkManager --no-daemon")
Mar 22 06:52:00 kali systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service ...
Mar 22 06:52:00 kali dbus-daemon[459]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Mar 22 06:52:00 kali systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Mar 22 06:52:10 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
```

- Un service spécifique, comme rsyslog : journalctl -u rsyslog -f

```
[root@kali)-[~/home/kali]
# journalctl -u rsyslog -f
Mar 22 06:39:50 kali rsyslogd[224742]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8
.2412.0]
Mar 22 06:39:50 kali rsyslogd[224742]: [origin software="rsyslogd" swVersion="8.2412.0" x-pid="224742" x-info="https://www.rs
ylog.com"] start
Mar 22 06:41:06 kali systemd[1]: Stopping rsyslog.service - System Logging Service ...
Mar 22 06:41:06 kali rsyslogd[224742]: [origin software="rsyslogd" swVersion="8.2412.0" x-pid="224742" x-info="https://www.rs
ylog.com"] exiting on signal 15.
Mar 22 06:41:06 kali systemd[1]: rsyslog.service: Deactivated successfully.
Mar 22 06:41:06 kali systemd[1]: Stopped rsyslog.service - System Logging Service.
Mar 22 06:41:06 kali systemd[1]: Starting rsyslog.service - System Logging Service ...
Mar 22 06:41:06 kali systemd[1]: Started rsyslog.service - System Logging Service.
Mar 22 06:41:06 kali rsyslogd[225420]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8
.2412.0]
Mar 22 06:41:06 kali rsyslogd[225420]: [origin software="rsyslogd" swVersion="8.2412.0" x-pid="225420" x-info="https://www.rs
ylog.com"] start
```

- Tester si **rsyslog** enregistre bien les logs, utilisez la commande :

logger "commentaire" → exemple : logger "bienvenue les IDOCS201"

```
[root@kali]# logger "bienvenue les IDOCS201"
```

Puis vérifiez dans **/var/log/syslog** avec la commande : tail -f /var/log/syslog

```
[root@Kali)-[~/home/kali]
# tail -f /var/log/syslog
2025-03-22T06:52:00.733892-04:00 kali systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
2025-03-22T06:52:10.751303-04:00 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
2025-03-22T06:55:01.883205-04:00 kali CRON[232181]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2025-03-22T06:57:00.695269-04:00 kali NetworkManager[517]: <info> [1742641020.6947] dhcpc (eth0): state changed new lease, address=192.168.5.4
2025-03-22T06:57:00.697816-04:00 kali dbus-daemon[459]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.5' (uid=0 pid=517 comm="/usr/sbin/NetworkManager --no-daemon")
2025-03-22T06:57:00.712004-04:00 kali systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service ...
2025-03-22T06:57:00.723308-04:00 kali dbus-daemon[459]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
2025-03-22T06:57:00.723428-04:00 kali systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
2025-03-22T06:57:09.866750-04:00 kali root: bienvenue les IDOCS201
2025-03-22T06:57:10.742882-04:00 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
```

- Vérifier si rsyslog tourne bien : `systemctl status rsyslog`

```
(root㉿kali)-[~/home/kali]
# systemctl status rsyslog

● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-03-22 06:41:06 EDT; 18min ago
     Invocation: 925ad24860b74067b47705c28e027667
TriggeredBy: ● syslog.socket
  Docs: man:rsyslogd(8)
        man:rsyslog.conf(5)
        https://www.rsyslog.com/doc/
 Main PID: 225420 (rsyslogd)
   Tasks: 10 (limit: 2269)
  Memory: 1.6M (peak: 1.8M)
    CPU: 65ms
   CGroup: /system.slice/rsyslog.service
           └─225420 /usr/sbin/rsyslogd -n -iNONE locally administered

Mar 22 06:41:06 kali systemd[1]: Starting rsyslog.service - System Logging Service ...
Mar 22 06:41:06 kali systemd[1]: Started rsyslog.service - System Logging Service.
Mar 22 06:41:06 kali rsyslogd[225420]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v>
Mar 22 06:41:06 kali rsyslogd[225420]: [origin software="rsyslogd" swVersion="8.24.12.0" x-pid="225420" x-info="https://www.r
lines 1-19/19 (END)
```

II- Sysmon sur Windows

Introduction à Sysmon

Sysmon est un outil de monitoring des journaux d'événements sous Windows. Avec Sysmon, vous pouvez monitorer les actions sur votre système telles que la création de processus ou de comptes utilisateurs, les connexions réseaux ou encore la création de fichiers. Couplé avec un serveur configuré avec Windows Event Collector, il récupère les logs Windows de plusieurs machines en un point unique.

Par défaut, Windows enregistre tous les événements du système. Ils peuvent être visualisés dans l'Event Viewer (observateur d'événements).

Sysmon fournit des informations détaillées sur les créations de processus, les connexions réseau et les modifications apportées, ainsi que l'heure de création des fichiers. Il permet la collecte, et vous permet d'identifier les activités malveillantes ou anormales. Il se configure sur chaque machine de votre réseau grâce à l'utilisation de fichiers de config.

Sysmon permet de monitorer les éléments suivants :

- Création de processus de journaux avec ligne de commande complète pour les processus actuels et parents.
- Enregistrement du hash des processus sur le système.
- Inclusion d'un *Globally Unique Identifier* (GUID) de processus dans les événements de création de processus, pour permettre la corrélation des événements.
- Inclusion d'un GUID de session dans chaque événement pour permettre la corrélation des événements sur la même session.
- Enregistrement du chargement des pilotes ou des DLL avec leurs signatures et leurs hashs.
- Enregistrement éventuellement des connexions réseau, y compris le processus source de chaque connexion, les adresses IP, les numéros de port, les noms d'hôtes et les noms de port.
- Filtrage de règles pour inclure ou exclure certains événements de manière dynamique.
- Génération des événements dès le début du processus de démarrage pour capturer l'activité créée par des logiciels malveillants.
- Détection des changements au moment de la création de fichier, pour comprendre quand un fichier a vraiment été créé.

1. Installer et configurer Sysmon

Pour assurer un monitoring complet, vous allez voir comment configurer Sysmon.

Tout d'abord [télécharger la dernière version de Sysmon](#). Une fois le répertoire décompressé, vous pouvez y accéder via l'invite de commande.

Par défaut, l'aide va s'afficher.

```
Administrator: Command Prompt
C:\Users\userbox\Desktop\sysmon>Sysmon64.exe

System Monitor v12.02 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Usage:
Install:           Sysmon64.exe -i [<configfile>]
Update configuration: Sysmon64.exe -c [<configfile>]
Install event manifest: Sysmon64.exe -m
Print schema:       Sysmon64.exe -s
Uninstall:          Sysmon64.exe -u [force]
-c   Update configuration of an installed Sysmon driver or dump the
     current configuration if no other argument is provided. Optionally
     take a configuration file.
-i   Install service and driver. Optionally take a configuration file.
-m   Install the event manifest (done on service install as well).
-s   Print configuration schema definition of the specified version.
-u   Uninstall service and driver. Adding force causes uninstall to proceed
     even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On
older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

Neither install nor uninstall requires a reboot.

C:\Users\userbox\Desktop\sysmon>
```

Pour installer Sysmon et commencer à monitorer le réseau, il suffit d'utiliser Sysmon avec l'option “-i”.

C:\Users\userbox\Desktop\sysmon>Sysmon64.exe -i

À partir de ce moment, Sysmon est en train de moniturer votre système avec la configuration par défaut.

Pour visualiser les logs, ouvrez l'Event Viewer Windows, puis "Applications and Services Logs" > "Microsoft" > "Windows" > "Sysmon".

The screenshot shows the Windows Event Viewer interface. The left pane lists various system categories like Security, System, and Network. The right pane is focused on the 'Operational' log, which contains 400 events. Most events are from the 'Sysmon' source, showing processes being created or terminated. One event is highlighted, labeled 'Event 5, Sysmon', which provides a detailed view of a process termination. The event details include the source (Microsoft-Windows-Sysmon/Operational), level (Information), date and time (11/7/2020 4:50:54 PM), and task category (Process terminated (rule: ProcessTerminate)). The event ID is 5. The right pane also includes an 'Actions' sidebar with various management options.

Vous verrez vos logs Sysmon depuis Event Viewer

Vous pouvez voir ici des informations de création de processus système. Les informations remontées incluent le statut, le timestamp, le *Process ID* (PID) pour un processus, le GUID et l'emplacement du fichier sur le système.

2. Configurer Sysmon pour affiner votre monitoring

Vous allez à présent configurer Sysmon pour utiliser un fichier de configuration, afin de moniter certains éléments d'intérêt. Pour ce faire, vous allez utiliser [ce fichier de configuration mis à disposition](#).

Ce fichier propose une bonne base ; il faudra toutefois l'adapter en fonction de vos besoins. Vous pouvez choisir si vous voulez moniter ou non certaines créations de processus. Il est conseillé en effet d'exclure certains processus système de votre monitoring, qui génèrent trop d'informations et par conséquent peuvent noyer ceux qui vous sont utiles.

Par exemple, le fichier inclut des extraits permet d'exclure le monitoring de logs en lien avec certains processus système et également des extraits pour moniter les connexions réseaux :

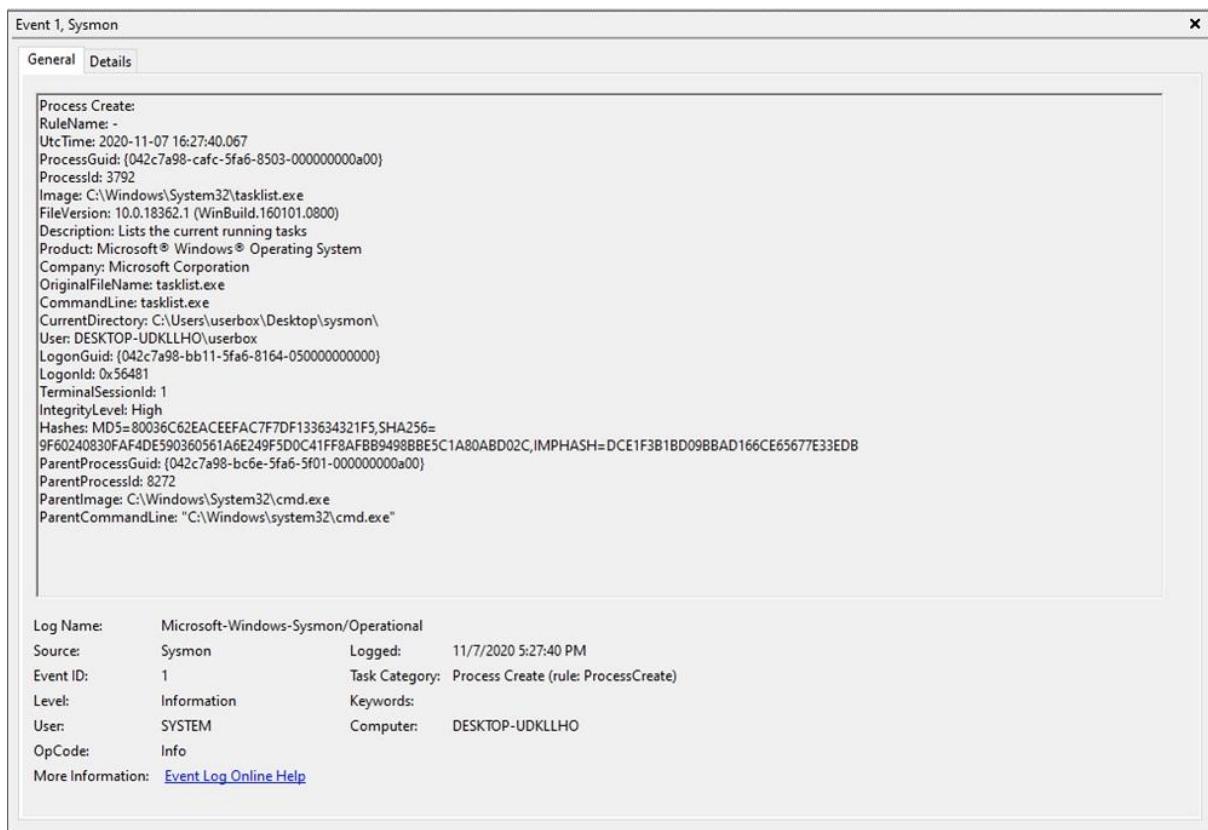
Pour charger votre fichier de configuration, il suffit d'utiliser l'option “-c” :

```
>Sysmon64.exe -c sysmonconfig-export.xml
```

Une fois le fichier de configuration créé, vous pouvez voir dans l'Event Viewer la mise à jour.

Pour tester notre configuration, vous exécutez le processus tasklist.exe pour afficher la liste des processus en cours d'exécution.

Dans la copie d'écran ci-dessous, vous pouvez voir les informations relatives à ce processus.



Le monitoring de tâches en temps réel est très utilisé pour identifier des comportements suspects tels que l'exécution de logiciels malveillants, ou encore des connexions réseaux. Cela peut être utilisé dans le cadre des activités d'un SOC, mais également dans le cadre d'une réponse sur incident.

3. Interpréter les logs remontés

Maintenant que vous avez vu comment mettre en place le monitoring de logs dans un environnement Windows, voyons comment les analyser avec Event Viewer.

Vous pouvez explorer les logs remontés à partir de l'Event Viewer. Le panneau du haut affiche tous les logs remontés. Vous verrez le niveau d'alerte, la date et l'heure, la source (ici Sysmon), ainsi que l'event id et la catégorie définie dans le fichier de configuration.

Le panneau du bas permet d'avoir plus de détails sur l'événement.

| Event 1, Sysmon | |
|---|--|
| General Details | |
| <input checked="" type="radio"/> Friendly View <input type="radio"/> XML View | |
| | |
| + System | |
| - EventData | |
| RuleName | - |
| UtcTime | 2020-11-07 17:09:49.023 |
| ProcessGuid | {042c7a98-d4dd-5fa6-ad03-000000000a00} |
| ProcessId | 6100 |
| Image | C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe |
| FileVersion | 86.1.16.72 |
| Description | Brave Browser |
| Product | Brave Browser |
| Company | Brave Software, Inc. |
| OriginalFileName | brave.exe |
| CommandLine | "C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe" --type=utility --utility-sub-type=features=AutoupgradeMixedContent,DnsOverHttps,LegacyTLSEnforced,MixedContentSiteSetting,OmniboxContent --disable-features=AllowPopupsDuringPageUnload,AutofillEnableAccountWalletStorage,AutofillServerCommunication,NativeLang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=5404 /prefetch:8 |
| CurrentDirectory | C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\86.1.16.72\ |
| User | DESKTOP-UDKLLHO\userbox |
| LogonGuid | {042c7a98-bb11-5fa6-ab64-050000000000} |
| LogonId | 0x564ab |
| TerminalSessionId | 1 |
| IntegrityLevel | Medium |
| Hashes | MDS=22985C1C0D8900943DCB8A5D75AB0B80,SHA256=795267BA7FD237CC9DB3E26A18B64ACE4ACB03, |
| ParentProcessGuid | {042c7a98-cac8-5fa6-7503-000000000a00} |
| ParentProcessId | 2832 |
| ParentImage | C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe |
| ParentCommandLine | "C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\brave.exe" |