

# Sysmon

- Microsoft의 Sysinternal suite에 포함된 시스템 모니터링 툴
- 기본 윈도우 이벤트 로그로는 한계가 있는 프로세스 생성, 네트워크 연결, 파일 생성 시간 변경 등의 정보를 추출한 후 윈도우 이벤트 저장소에 저장

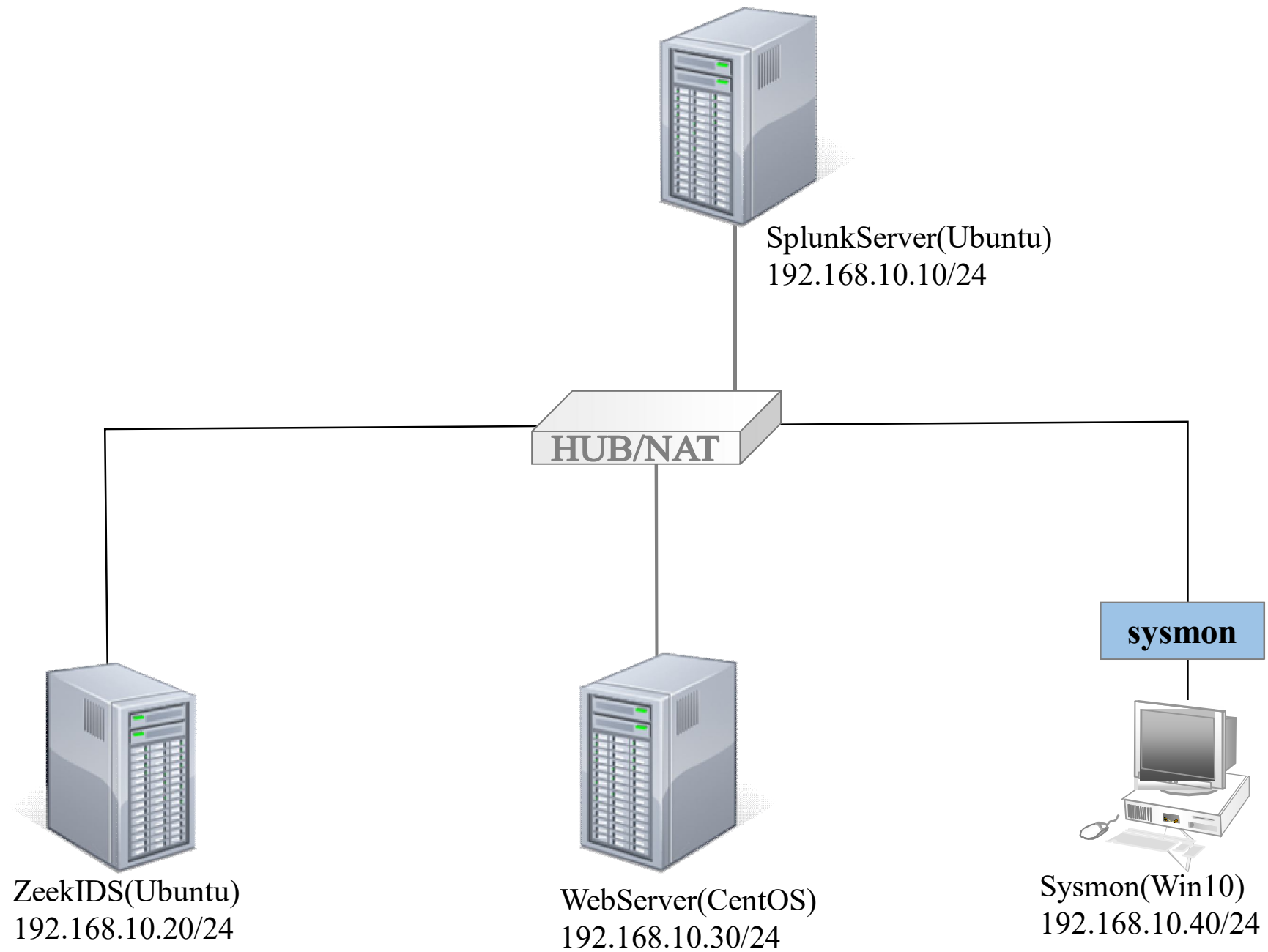
\* 이벤트 기반 정보가 아닌 ‘행동 기반 정보’를 수집에서 이벤트 저장소에 저장

# Sysmon 기능

- 실행 프로세스와 부모 프로세스의 전체 명령 줄을 로그로 저장
- MD5, SHA1, SHA256 알고리즘으로 실행 프로그램의 해시 값을 기록
- 여러 종류의 해시 값을 동시에 기록
- 네트워크 연결에서 IP주소, 포트번호, 호스트명, 포트명 등을 기록
- 레지스트리에서 환경 설정이 변경된 경우 자동으로 다시 읽어 들임

# **Sysmon Installation**

[Win10] Sysmon Installation



# [Win10] Sysmon Installation

## ❶ 파일 다운로드 후 설치

<https://download.sysinternals.com/files/Sysmon.zip>

```
C:\Users\sysmon\Desktop\Sysmon>dir
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: 1C9F-4DF9

C:\Users\sysmon\Desktop\Sysmon 디렉터리

2022-07-30 오후 03:29 <DIR> .
2022-07-30 오후 03:29 <DIR> ..
2022-05-11 오후 04:49          7,490 Eula.txt
2022-05-11 오후 04:49    7,291,792 Sysmon.exe
2022-05-11 오후 04:49   3,925,928 Sysmon64.exe
                3개 파일             11,225,210 바이트
                2개 디렉터리    10,781,904,896 바이트 남음
```

## ② sysmon 활성화

C:\>cd /user/sysmon/desktop/sysmon

C:\> sysmon64.exe -accepteula -i

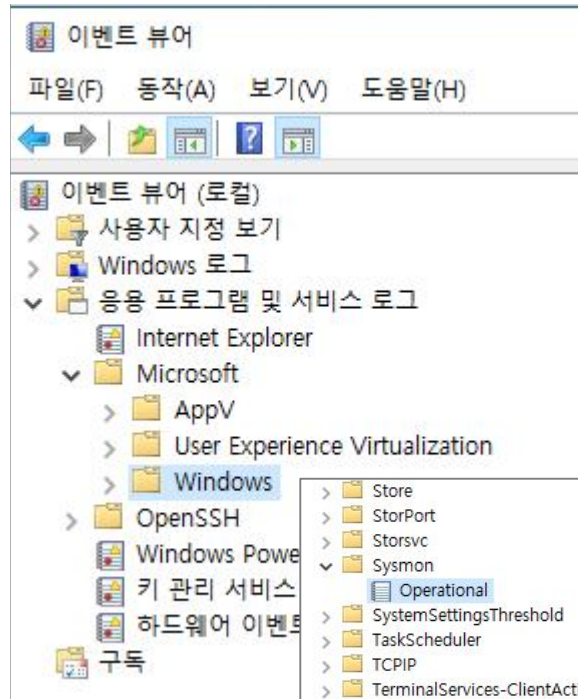
```
C:\Users\sysmon\Desktop\Sysmon>sysmon64.exe -accepteula -i

System Monitor v13.34 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

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

### ③ 이벤트뷰어 확인



Operational 이벤트 수: 80 (1) 새 이벤트를 사용할 수 있음

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2022-07-30 오후 3:48:44	Sysmon	5	Process terminated (rule: ProcessTerminate)
정보	2022-07-30 오후 3:48:44	Sysmon	1	Process Create (rule: ProcessCreate)
정보	2022-07-30 오후 3:48:15	Sysmon	5	Process terminated (rule: ProcessTerminate)
정보	2022-07-30 오후 3:48:14	Sysmon	1	Process Create (rule: ProcessCreate)
정보	2022-07-30 오후 3:48:14	Sysmon	5	Process terminated (rule: ProcessTerminate)
정보	2022-07-30 오후 3:48:14	Sysmon	1	Process Create (rule: ProcessCreate)
정보	2022-07-30 오후 3:47:49	Sysmon	5	Process terminated (rule: ProcessTerminate)
정보	2022-07-30 오후 3:47:49	Sysmon	1	Process Create (rule: ProcessCreate)
정보	2022-07-30 오후 3:47:28	Sysmon	5	Process terminated (rule: ProcessTerminate)
정보	2022-07-30 오후 3:47:27	Sysmon	1	Process Create (rule: ProcessCreate)
정보	2022-07-30 오후 3:46:53	Sysmon	5	Process terminated (rule: ProcessTerminate)
정보	2022-07-30 오후 3:46:27	Sysmon	5	Process terminated (rule: ProcessTerminate)
정보	2022-07-30 오후 3:46:26	Sysmon	5	Process terminated (rule: ProcessTerminate)

이벤트 5, Sysmon

일반 자세히

Process terminated:  
 RuleName: -  
 UtcTime: 2022-07-30 06:48:44.854  
 ProcessGuid: {a6df5543-d44c-62e4-9402-000000000300}  
 ProcessId: 6716  
 Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe  
 User: DESKTOP-7GILHFM\Sysmon

로그 이름(M): Microsoft-Windows-Sysmon/Operational  
 원본(S): Sysmon  
 이벤트 ID(E): 5  
 수준(L): 정보  
 사용자(U): SYSTEM

로그된 날짜(D): 2022-07-30 오후 3:48:44  
 작업 범주(Y): Process terminated (rule: ProcessTerminate)  
 키워드(K):  
 컴퓨터(R): DESKTOP-7GILHFM