1. Splunk Enterprise와 Splunk Observability 차이

Q: 기존 Splunk 엔터프라이즈/모니터링 기능 과의 차이점이 무엇인가요?
A: 옵저버빌리티는 IT 모니터링 인프라/앱 모니터링에 특화된 것으로 예측적 예방적 모니터링에 가까운 모니터링으로 해석할 수 있습니다. IT 모니터링에 필요한 모든 제품군을 모아 놓은 것이 Splunk 옵저버빌러티 스위트입니다.

Q: Observability Suite는 정보수집 에이전트가 기존 Splunk용 에이전트와 다릅니까? Splunk 엔터프라이즈와는 별개로 운영할 수 있습니까?
A: Splunk 엔터프라이즈와 다른 전용 에이전트로, 별도 운영이 가능합니다.

2. Splunk Observability 특장점

Q: 이 장비를 도입함으로써 얻을 수 있는 가장 큰 이점이 무엇입니까?
A: 실시간으로 다양한 클라우드 환경에 있는 App + Infra에 대해서 실시간으로 Log, Metric, Trace까지 모니터링이 가능하고, No-sampling trace를 통하여 오차가 적습니다. 특히 복잡한 환경을 가지는 MSA 환경에서 빠르게 원인 분석이 가능하다는 점이 가장 큰 이점이라고 할 수 있을 것 같네요."

Q: 실시간은 리얼타임입니까?
A: 기존 모니터링이 배치(batch) 방식이라고 한다면 Splunk 서비스는 초단위(milliseconds) 단위의 스트림(stream)으로 처리됩니다. 커스터마이징한 위젯으로 복잡한 계산식을 사용하더라도 빠른 모니터링이 가능합니다.

Q: 장애 발생시 alert 기능 외에 장애 로그를 분석하여 장애 분석과 문제 해결 기능이 있습니까?
A: Tag insight 기능을 통해서 장애 원인에 대해서 즉각적으로 트러블슈팅(troubleshooting)이 가능합니다.

3. Splunk Observability 도입과 라이센싱 구조

Q: 요즘과 같은 복잡하고 다양한 멀티 클라우드 환경에서 Splunk 옵저버빌리티를 통한 데이터 수집 및 모니터링 단계나 준비는 어떻게 합니까? (Agent/API 수집 방식 등)
A: On-prem 과 멀티 클라우드 환경에서 모두 사용 가능하며 Agent, API 방식 모두 가능합니다. 모니터링을 위한 전용 agent가 제공되고 있습니다.

Q: 도입 시 가장 고려해야할 사항과 최소의 비용으로 최대의 효과를 볼 수 있는 방법은 무엇입니까?
A: 최우선으로 고려해야 하는 부분은 "클라우드 적용과 모니터링 대상 범위"입니다. 범위에 따라 도입에 필요한 시간과 비용이 계산되기 때문에 어디까지 모니터링이 필요한 것인지 확인하는 것이 중요합니다. 모든 서비스가 public cloud 환경에 있는 경우와 모든 서비스가 하나의 플랫폼에 운영되는 경우가 가장 효율적인 방법입니다.

Q: Observability suite의 subscription 조건과 과금 방식은 어떻게 됩니까?
A: 사용량 기반 과금과, 호스트기반(컨테이너 기반) 과금 중에 선택할 수 있으며 SaaS 서비스로 월간/년간 비용을 계획하여 시작하실 수 있습니다.

Q: 현재 Splunk ES를 운영하고 있는 경우, Observability Suite를 추가 연동할 때 어떠한 부분을 고려해야 하며, 이점은 무엇인가요? 또 클라우드 기반이 아닌 온프레미스 사용할 수 있습니까?
A: Observability를 통해서 (온프렘 뿐아니라 클라우드 환경에서도) 실시간으로 애플리케이션과 인프라 모니터링을 쉽게 수행할 수 있고, 기존 사용하고 있는 Splunk와 연동해서 빠르게 문제에 대한 원인을 분석할 수 있도록 해줍니다. On-prem 환경에서도 Agent를 설치하여 모니터링이 가능합니다.