splunk> turn data into doing™

안녕하세요. 스플렁크 코리아입니다.

지난 6 월 12 일 스플렁크는 TalkIT 플랫폼에서 스플렁크 클라우드 서울 리전(Region) 도입을 기념하여 "스플렁크 클라우드 서울 상륙!" 이라는 제목으로 웨비나 방송을 진행하였습니다. 올해 4 월 말부터 스플렁크 아마존웹서비스(AWS) 서울 리전을 통해 서비스를 제공을 시작한 스플렁크 클라우드의 서울 리전 도입 배경과, 아키텍쳐, 고객 사례 등을 설명 드렸습니다.

방송 중 진행된 실시간 Q&A 답변을 정리하여 드리니, 업무에 참고하여 도움 되시길 바랍니다. 추가 문의 사항이 있으시면, 스플렁크 코리아 대표 번호 (02-6007-2003) 또는 해당 사이트에서 문의를 남겨주시면, 응대해드리도록 하겠습니다.

클라우드 관련

[질문] 스플렁크 서비스를 쓰면서 걱정하는 스플렁크쪽에서의 **데이터 유출에** 대한 우려는 어떻게 조치되고 있나요?

- Splunk Cloud 는 SOC2 Type II, ISO/IEC27001:2013 과 같은 국제 감사기관의 Compliance 인증 뿐만 아니라, Cloud 사용 고객을 위한 HIPAA, PCI DSS 서비스를 제공하고 있습니다.

[질문] Splunk **서버 접근**이 안된다면 conf 수정은 직접 할 수 없는 건가요? 아니면 티켓을 통해 문제를 이슈해 하면 Splunk 측에서 직접 문제에 맞게 수정해 주시는 건가요?

➔ 서비스 티켓을 오픈하면 해당 이슈에 대한 도움을 받을 수 있습니다.

[질문] 스플렁크에서 빅데이터 수집 및 가공을 하기 전 단계인 **사전 데이터 정제** 작업에 대한 가이드 및 지원 솔루션이 있는지 궁금합니다.

➔ 사전 데이터 정제 작업도 스플렁크 플랫폼 안에서 가능 하십니다.

[질문] 스플렁크는 클라우드 서비스로만 구현이 가능한가요? 온프레미스나 프라이빗 클라우드로도 구현 가능한가요?

➔ 온프레미스/프라이빗/하이브리드 구성이 모두 가능합니다.

[질문] 인트라넷 로그들을 Cloud 로 올릴려면 손이 좀 가겠네요?

➔ 인트라넷 로그를 마이그레이션하는 PS (Professional Service) 서비스를 제공하고 있습니다.

[질문]클라우드에서 **DLP 암호화** 등도 지원이 되나요?

➔ 클라우드 구매 시 데이터 암호화 하는 옵션을 선택하셔서 구매 가능 하십니다.

[질문] Azure 나 기타 클라우드서비스에서 간혹 심각한 장애로 인한 장시간 **서비스 장애**가 발생하는데 이에 대해 차별화된 대책이 있을까요?

➔ 실제로 AWS 위에서 운영이 되기 때문에 완벽하게 특화 된 별도의 차별화 대책을 가지기는 힘들 수 있지만, 클라우드 서비스를 위한 전담 서비스팀들이 운영되어서 서비스의 운영에 최선을 다하고 있습니다.

[질문] 클라우드의 독립성에 관하여 고객 데이터의 독립성을 위해서는 별도의 전용 시스템을 구축한다는 의미로 일반적인 클라우드서비스와 비교해서 서비스 비용이 더올라가는지요?

➔ 스플렁크 클라우드 서비스는 다른 고객과 공유되지 않는 독립적인 환경에서 운영됩니다. 그래서 별도의 서비스 비용에 대한 구별은 없습니다.

[질문] 클라우드 서비스는 고객의 데이타를 맡아 보관하는 최고의 서비스라고 말할 수가 있는데요, 고객 데이타의 안벽한 백업을 위한 장소를 달리하는 제 2 의 **백업정책**이 있는지요?

➔ 스플렁크 클라우드는 데이터를 서로 다른 AZ 에 세벌을 복사해서 저장하기 때문에 데이터를 안전하게 보관할 수 있습니다. 그리고 스플렁크내의 설정들과 데이터들도 주기적으로 백업을 하여 별도의 공간에 보관하고 있습니다. 또한 오랜된 데이터는 스플렁크에서 제공하는 별도의 저장소나 고객이 사용하는 S3 같은 저장소에 압축해서 저장할 수 있는 환경을 제공하고 있습니다.

[질문] Saas 형 Splunk Cloud 와 온프레미스형 Splunk Enterprise 는 기능적인 차이점이 있을까요?

➔ _Splunk 를 사용하는데 기능 제약은 없습니다. 단지 클라우드를 사용하는 경우에는 직접 운영체제에 들어가서 작업을 할 수 없기 때문에 서비스 요청 티켓을 등록한 후 진행하여야 합니다. 또한 이러한 제약 때문에 splunkbase 에 대한 일부 앱들은 클라우드 환경에서 사용할 수 없습니다. 그래서 splunkbase 에서 앱을 다운받아서 사용할 경우 cloud 적용 가능한 앱인지 먼저 체크해보는것이 필요합니다.

[질문] 해외에서의 클라우드서비스 **구축사례**와 국내에서도 도입이 되었는지요?

➔ 이곳에서 다양한 글로벌 클라우드 사례를 확인 하실 수 있습니다.

[질문] 스플렁크 클라우드는 현재 구글 클라우드에서 베타 테스트 상태이며, 일부 고객들만 사용해볼 수 있으며. 정식 출시 일자는 아직 공개되지 않았다 라고 하고, 스플렁크 클라우드는 무료 버전을 제공하지 않지만 15 일 무료 평가판을 통해 AWS 와 같은 다른 클라우드 환경에서 테스트해볼 수 있다 라고 하는데요, 정식 출시 일정은 언제정도 인지요?

➔ AWS 의 서울리전서비스는 정식으로 오픈되어 있고 무료로 스플렁크 클라우드를 사용해 볼 수 있는 기간을 15 일 제공합니다.

[질문] 스플렁크 클라우드는 네이티브 클라우드, 하이브리드 및 멀티 클라우드 환경에서 데이터 수집을 지원한다 알고 있는데요, 국내에서도 이런 서비스가 지원이 되는지요?

➔ 똑같은 형태로 지원을 하고 있습니다.

클라우드 **서울 리전** 도입 관련

[질문] 서울 리전이 생기면서 국내 이용자들이 네트워크 속도 개선 이외에 어떤 장점들을 가질 수 있을까요? / 고객 입장에서 스플렁크에서 서울리전을 도입함으로서 볼수 있는 혜택이 어떤게 있나요?

➔ 가장 큰 부분이 국내 업체에서 데이터를 외국의 리전에 저장하는 것을 꺼리는 부분이 있어서 클라우드 활성화가 되지 않는 문제가 있습니다. 한국리전 도입으로 데이터 주권 및 보안 관련 요구사항을 충족해야 하는 국내 기업들이 타국가가 아닌 국내 지역으로 데이터를 보관 및 처리 함으로써 보안 및 컴플라이언스 이슈 없이 클라우드를 사용할 수 있습니다.

[질문] Splunk as a Service(SaaS) 는 한국에서 **Azure / AWS** 모두 사용할 수 있나요? / 다른방식의 클라우드에서 사용 가능한가요? / 스플렁크 클라우드 서울 리전은 AWS 에서만 사용 가능한가요? Azure 나 GCP 를 사용중인 상태에서는 스플렁크 클라우드 사용이 가능한지 궁금합니다

➔ 현재 서울 리전은 AWS 에 있습니다. 그러나 GCP 나 Azure 에 있는 데이터들을 수집을 해서 사용할 수 있습니다. 그리고 글로벌에서는 GCP,Azure 를 통해 SaaS 형태의 서비스를 오픈하고 또 준비하고 있습니다.

[질문] 한국 리전이 AWS 를 사용하시고, 5 월에 Google DC 도 사용한다고 하셨는데, AWS 에서도 멀티 AZ 로 구성되어 현재 서비스 되고 있는 것인가요 ? 아니면 5 월 이후에 AWS 와 GDC 간에 **멀티 AZ 서비스가** 가능한가요?

➔ 아직까지 Google 과 AWS 간의 AZ 구성은 계획에 없습니다. AWS 에서 스플렁크의 데이터는 세 벌의 복사본이 서로 다른 AZ 에 저장되기 때문에 AZ 장애에 대한 서비스의 연속성을 보장하고 있습니다.

[질문] 스플렁크가 클러우드 리전에 들어오면 AWS 와 같은 **퍼블릭 클라우드의** 서비스로 동작하는건가요? 그리고 스플렁크에 들어오는 데이터는 퍼블릭 클라우드에서 서비스하는 여러 유형의 디스크/데이터 저장 서비스에서 어떤 유형으로 저장되고 관리하게 되나요?

➔ 스플렁크 클라우드 서비스는 퍼블릭 클라우드인 AWS 에서 운영 되지만, 개인의 스플렁크는 클라우드 서비스 내에서 독립적인 환경에서 운영이 되기 때문에 서로 다른 스플렁크들과 자원을 공유하지 않습니다. 데이터는 구입한 라이센스에 따라 스플렁크의 스토리지를 제공하고, 스토리지만 추가로 구매할 수 있습니다. 그리고 오래된 데이터들은 설정을 통해 자동 보관소나 나만의 S3 같은 스토지에 백업해서 보관할 수 있습니다.

[질문] AWS 서울 리전 도입이긴 하나 스플렁크의 SaaS 제품들이 **타 벤더사의 IaaS 나 PaaS** 에도 호환 시 복잡하지 않게 연계 구성이 가능한가요?

➔ 네. 기존의 splunk 와 같은 형태로 다른 IaaS, PaaS 수의 데이터를 수집해서 사용이 가능합니다.

스플렁크 솔루션 관련

[질문] 기존 빅데이터플랫폼(On-Premise, Cloud) 대비 Splunk 플랫폼은 어떤 점이 다른가요?

➔ 기존 빅데이터 플랫폼 대비, 수집부터, 분석, 비쥬얼라이제이션 까지 한번에 해줄 수 있는 단일 솔루션입니다. 그리고 스플렁크의 고유의 쉬운 언어(SPLK)들 통해서 데이터 핸들링이 가능하고, machine learning 까지 이 언어를 통해 한번의 flow 로 수행할 수 있다는 것이 장점입니다.

[질문] 수집된 데이타로부터 분석된 결과에 대한 대쉬보드나 화면 구성의 편의성을 제공하는지요? 사용자별로 권한을 부여하여 관리하는 기능등은 제공되니요?

➔ 가지고 있는 데이터를 이용해 쉽게 대시보드를 구현할 수 있으며, 대시보드별로 사용자 권한을 설정할 수 있습니다.

[질문] 수집된 정보를 **Open API** 로 받을 수 있나요?

➔ 스플렁크는 API 를 제공하고 있어서, API 를 통해 검색을 통해 데이터를 받아서 활용할 수 있습니다.

[질문] 스플렁크에서 제공해주는 솔루션으로 **공장 등에 설치된 설비에 부착된 센서에서** 직접 데이터를 끌어올 수 있나요?

➔ 센서 데이터 로그들을 바로 스플렁크에서 수집, 모니터, 분석이 가능 하십니다. 국내 사례로는 현대제철 사례가 있습니다. '전기로 원료 운영 최적화 시스템'이라고 하는 스마트팩토리 운영을 도입하였는데요. 관련된 자세한 내용은 해당 블로그 글에서 확인하실 수 있습니다.

[질문] 스플렁크를 활용하여 정보보안 로그분석등을 원하는 만큼 구현하기위해서 **개발자**가 필요한가요? 제품 자체에서 구현이 가능한가요? 동종 타사에서는 스플렁크를 도입하고 개발을 통해서만 시스템 관제기능 구현이 가능한 것이 많아서 NMS/SMS 의 기본 관제기능만 사용하고있어서 문의드립니다.

➔ 실제로 Splunk Enterprise 를 통해 많은 정보보안 기능들이 구현되어 있습니다. 하지만 스플렁크 기능을 완전히 사용하기 위해서는 약간의 개발이 필요합니다.

[질문] 클라우드 로그 분석 서비스는 일반적으로 **엘라스틱서치**를 많이 사용하는데, 검색, 리포팅, 데이터 수집 기능을 기준으로, ELK 대비 스플렁크의 강점이 있는지요? 그리고 국내에서 스플렁크 서비스 지원업체가 많이 있는지요?

➔ 스플렁크는 어떤 종류의 데이터든 사전 데이터 모델을 생각하지 않고 데이터를 바로 수집할 수 있습니다. 그리고 대용량의 데이터 수집과 검색이 가능하고, 수집부터 비쥬얼라이제이션까지 하나의 제품으로 가능하다는 점도 장점입니다.

가격/라이센스 구조 관련

[질문] 가격 및 라이센스 구조에 대하여 더 자세하게 궁금합니다.

➔ 라이센스 구조는 Data ingestion 기준 또는 vCPU 기준으로 라이센싱되는 Splunk Enterprise 를 기본 제품으로하고, 보안/IT 운영 등 각 Use case 에 대응하기 위한 Premium App 을 Add-on 으로 사용하시는 구조입니다.

[질문] **비용**적인 측면에서 경쟁사 대비 큰 기대를 할수 있을까요? / 비용의 높은 장벽을 허물수 있나요?

➔ Data to Everting Platform 이라는 새로운 슬로건을 발표하면서 스플렁크 가격 정책에도 변화가 있었습니다. 여러 옵션을 통해 고객은 각자의 비즈니스 성장에 적합한 가격 정책을 유연하게 선택할 수 있습니다. 직접 영업팀과의 상담을 원하시면 해당 링크를 통해 문의 남겨주시기 바랍니다.

기타 질문

[질문] 홍보활동 차원에서 **시연 데모 혹은 컨퍼런스 세미나** 등을 기획하고 계신가요?

➔ 매달 웨비나에서 기술 데모 등을 확인하실 수 있습니다. 7 월 7 일에 토크아이티 플랫폼에서 클라우드 후속으로 클라우드 모니터링에 유용한 제품인 시그날 FX 를 소개드릴 예정입니다.

[질문] 작년만 해도 Splunk **개발자** 찾기 쉽지 않았던 경험이 있었는데 제가 찾지를 않아서 그런건지 지금은 어떤가요?

➔ 페이스북의 한국 스플렁크 사용자 그룹 또는 스플렁크 엔지니어 카카오톡 공개 채팅방을 통해 활발한 교류가 가능 합니다.

[질문] 데이터 **분석/시각화** 관련한 솔루션들이 요즘 많던데요. 스플렁크는 타블로나 알타릭스 같은 제품에 비해 어떤 차이, 특장점이 있나요?

➔ 태블로나 알타릭스 같은 경우 분석을 할수 있는 형태의 데이터를 가지시고 최종 시각화를 하시기에 좋은 제품 입니다. 스플렁크 같은 경우는 분석을 위한 데이터의 전처리의 과정 필요없이 머신에서 나오는 모든 데이터를 바로 넣고 검색, 모니터, 분석, 액션을 할수 있는 제품입니다.

[질문] 클라우드 자원에서 발생하는 로그분석을 위해, ELK 를 활용중에 있는데, ELK 대비, 스플렁크 상용서비스를 이용(전환)할 만한 가치는 뭐가 있을까요?

➔ 타사 제품과의 비교는 별도로 문의주시면 설명드리도록 하겠습니다. 스플렁크는 대용량의 로그를 분석하고 풍부한 SPLUNK 언어로 데이터를 핸들링해서 비쥬얼라이제이션 해 줄 수 있는 툴입니다.

[질문] 스플렁크 엔터프라이즈 버전이 꼭 **하둡**과 통합이 되어야만 되는 이유가 있는가요? 궁금합니다

➔ 스플렁크와 하둡은 크게 상관이 없습니다. 하둡과 별도로 스플렁크 엔터프라이즈를 사용할 수 있습니다.

[질문/라이센스관련] **기존 엔터프라이즈 라이센스** 구매자가 클라우드로 **전환**할 경우 기존 라이센스는 어떻게 되나요?

➔ 기존 텀 라이선스를 클라우드 라이선스로 전화 가능합니다.

[질문] Splunk enterprise license 를 가지고 Splunk Cloud AWS 를 구성하려 합니다. 어떻게 진행해야하는지요? 또한, 기존 License 를 나눠서 사용하고 싶은데 구성 방법을 알고 싶습니다.

➔ 현재 사용 중이신 라이선스는 퍼블릭 클라우드의 데이터를 분석을 하실 경우 사용 가능하십니다

[질문] 스플렁크 관련 자료가 가장 잘 정리되고 많은 온라인 채널은 어디인가요? 추천 부탁드립니다.

➔ 스플렁크 코리아 사이트가 오픈되어 있으며, 비디오 자료는 스플렁크 TV 에서 보실 수 있습니다. 스플렁크 코리아의 소식은 스플렁크 카카오톡 채널 을 통해 제일 발빠르게 받아보실 수 있습니다.