Microsoft Azure

Splunk on azure

Hyun Suk Shin (AZURE CSA)

2016

Splunk 개발 VM 구성하기

본 실습을 통해 ARM Template으로 개발용 Splunk VM을 만들고 Azure 상에서 Splunk를 체험해보도록 합니다. ARM Template으로, 개발용 Splunk VM을 구성하는데는 30분이 소요됩니다.

1. 실습을 위해서 사전에 계정과 구독 그리고 실습을 위한 관련 도구(tool)을 다운로드 받습니다.
   1. Azure 계정과 구독
      1. Azure에 접속하기 위해서는 Microsoft 계정이 필요합니다. Microsoft 계정이 없는 경우 <http://msn.com>에서 새로 생성할 수 있습니다.
         1. <http://msn.com> 을 방문하여 오른쪽 상단에 ‘로그인’을 클릭하고 ‘계정을 만드세요’를 클릭합니다.

|  |  |
| --- | --- |
|  |  |

* + - 1. 계정을 생성 할 때 아래와 이미 존재하는 회사 메일 주소를 사용할 수 있습니다.

|  |
| --- |
|  |

* + 1. 제공된 Azure Free Pass를 사용하여 무료 구독을 생성합니다. Free Pass는 30일 동안 제공된 금액 미만으로 사용이 가능하며 제공된 비용을 초과하게되는 경우 또는 30일이 경과하는 경우는 자동으로 중지 됩니다.
  1. 리눅스 가상 컴퓨터에 접속하기 위해 도구를 다운로드 받습니다.
     1. 아래 홈페이지에서 Putty를 다운로드 받습니다. 또는 익숙한 도구를 미리 설치 합니다.

|  |
| --- |
| <http://putty.org> |

* 1. 실습 비용 한도에 따른 유의 사항
     1. 실습을 종료 하고나서 가급적 사용하지 않는 서비스들은 삭제합니다. 불필요한 비용 발생으로 무료 구독이 중지되면 실습 진행이 어렵습니다.
     2. 고사양의 가상 컴퓨터나 서비스를 생성하지 않습니다. 고사양 서비스들은 고비용이 청구되어 단시간에 제공된 무료 구독의 비용을 초과할 수 있습니다.

1. 서비스 구성 순서
   1. Azure Portal에 로그인합니다. [+ NEW]를 클릭합니다.

|  |
| --- |
|  |

* 1. 검색창에서 Splunk를 검색하면 연관 검색으로 Splunk Enterprise가 제안됩니다. Splunk Enterprise를 클릭하여 검색을 실시합니다.

|  |
| --- |
|  |

* 1. 검색결과에 Splunk Enterprise가 포함된 것을 볼 수 있습니다. 클릭하여 가상 컴퓨터 생성을 시작합니다.

|  |
| --- |
|  |

* 1. Splunk Enterprise에 대한 설명이 제공됩니다. 자세한 설명을 읽고 [Create]를 클릭하여 계속 진행합니다.

|  |
| --- |
|  |

* 1. Splunk Enterprise 생성을 위한 전체 6 단계 요약화면이 표시됩니다. 첫 번째 기본 정보를 입력합니다. Splunk가 설치되는 가상 컴퓨터의 사용자(관리자) 이름과 암호 그리고 리소스 그룹을 기입합니다. 입력이 완료되면 [OK]를 클릭하여 두 번째 단계로 넘어갑니다.

|  |  |
| --- | --- |
|  | |
|  |  |

* 1. 두 번째 단계는 네트워크 구성입니다. 가상 네트워크를 생성하는 옵션 정의하고 가상 네트워크 서브넷 이름을 명명합니다. 임의로 명명된 “(new) splunkVnet” 가상 네트워크를 클릭하여 세부 영역을 확인합니다. 조건에 따라 기존에 만들어진 가상 네트워크도 활용이 가능합니다. 이번 실습에서는 기본 옵션을 그대로 사용합니다. [OK]를 클릭합니다.

|  |
| --- |
|  |

* 1. 두 번째 단계에서 “Congifure subnets”를 클릭하고 세부적인 서브넷 이름과 각 서브넷의 주소 영역을 설정합니다. 기본적으로 Search Head와 Index 서버 구성을 구분하여 배포하기 위해 2 개의 서브넷이 설정된 것을 볼 수 있습니다. 이번 실습에서는 별도 변경없이 그대로 진행합니다. [OK]를 클릭하여 설정 정보를 저장합니다. [OK]를 클릭하여 두 번째 단계를 마치고 세 번째 단계로 넘어 갑니다.

|  |
| --- |
|  |

* 1. 세 번째 단계는 Splunk Node Settings 입니다. 이 단계에서 Splunk를 단일 가상 컴퓨터로 구성할지 또는 클러스터 형태로 구성할지 설정할 수 있습니다.
     1. “Single Node”를 선택하는 경우 아래와 같이 가상 컴퓨터 한 대 사이즈를 설정하는 옵션만 보이게 됩니다.

|  |
| --- |
|  |

* + 1. “Cluster”를 선택하는 경우 아래와 같이 Search Header와 Index 가상 컴퓨터의 사이즈와 수량을 각각 설정할 수 있도록 양식이 제공됩니다.

|  |
| --- |
|  |

* + 1. 본 실습에서는 제한 된 비용으로 “Cluster” 구성이 불가능합니다. 따라서 “Single node”를 선택합니다. 또한 “VM size”를 F8에서 F4로 낮추어 진행하도록 합니다. F4가 안보이는 경우 우측에 “View All”을 클릭하여 전체 가상 컴퓨터 리스트 중에서 찾아 [Select]하도록 합니다.

|  |
| --- |
|  |

* + 1. “Single node”와 “1x Standard F4”를 확인하고 [OK]를 클릭하여 다은 네 번째 단계로 넘어갑니다.

|  |
| --- |
|  |

* 1. 네 번째 단계에서는 Splunk Enterprise 를 서비스 하기위한 추가 정보들을 입력합니다. 공용 IP 주소 및 Splunk 관리자의 암호 등을 설정합니다. 순서대로 살펴 보도록 하겠습니다.

|  |
| --- |
|  |

* + 1. “New public IP name”이라는 항목은 인터넷을 통해 Splunk를 접근하기 위한 또는 서비스하기 위한 공용 IP 주소를 의미합니다. 세부설정을 위해 클릭하여 아래와 같이 IP 주소를 Azure 관리자가 관리하기위한 이름을 설정할 수 있으며, 공용 IP를 고정하여 할당 받을 것인지를 선택할 수 있습니다. 본 실습에서는 기본 설정된 정보를 그대로 사용합니다. [OK]를 클릭하여 확인합니다.

|  |
| --- |
|  |

* + 1. 공용 IP에 할당될 DNS 이름을 명명합니다. 임의의 IP 주소가 할당되면서 해당 IP 주소와 매핑되는 DNS입니다. 설정시 주의해야할 사항은 DNS는 인터넷상에서 유일해야하기 때문에 기존 다른 서비스와 이름이 중복되는 경우 사용할 수 없으며 다른 이름으로 생성해야할 수 있습니다. 아래와 동일한 이름을 사용하는 경우 이미 사용 중이라는 경고가 발생할 수 있음에 주의하여 명명하도록 합니다.

|  |
| --- |
|  |

* + 1. Splunk 관라자의 암호를 설정합니다. 또한 Splunk 관리자가 ID와 암호를 사용하여 Linux SSH로 원격 접속할 때 접속을 승인할 IP 주소 범위를 설정할 수 있습니다. CIDR 양식으로 입력해야하며 전세계 어디서든 접속이 가능하도록 하는 경우 기본값 ‘0.0.0.0/0’으로 설정합니다. 데이터를 수신하기 위한 영역 설정도 동일하게 구성할 수 있습니다. 본 실습에서는 가급적 기본 설정을 유지하고 실습을 진행 합니다. [OK]를 클릭하고 다음 다섯 번째 단계로 진행합니다.

|  |
| --- |
|  |

* 1. 다섯 번째 단계는 지난 네 단계에서 진행한 설정 정보들을 요약하여 보여 줍니다. 동시 입력된 값이나 해당 양식 (Template)에 이상이 없는지 검사를 수행하게 됩니다. 유효성 검사가 통과되면 “Validation passed”라고 파란색 알림이 표시 됩니다. [OK]를 클릭하여 마지막 단계로 넘어 갑니다.

|  |
| --- |
|  |

* 1. 마지막 여섯 번째 단계는 Terms of use에 동의하는 것 입니다. Azure외 추가로 배포되는 소프트웨어에 대한 사용 동의가 포함되어 있습니다. 해당 제품을 사용하는 조건등을 잘 살펴보고 [Purchase]를 클릭하여 마법사를 종료하도록 합니다. 참고로 본 실습에 사용되는 Splunk 이미지는 체험판으로 구성되며 실제로 구매되어 비용이 지불되는 것은 없습니다.

|  |
| --- |
|  |

1. 설치된 Splunk 관리자 페이지에 접속합니다.
   1. 리소스 그룹을 클릭하고 “Deployments”를 클릭하면 진행 중인 과정을 볼 수 있습니다. 가상 컴퓨터 구성과 Splunk 설치에는 약 7분 ~ 10분정도 소요될 수 있습니다.

|  |
| --- |
|  |

* 1. 리소스 그룹 “splunk-dev”에서 가상 컴퓨터 “standalone-vm”을 클릭합니다. 가상 컴퓨터에대한 자세한 정보가 표시됩니다. 여기에는 가상 컴퓨터에 접근할 수 있는 IP주소와 DNS도 함께 확인할 수 있습니다.

|  |
| --- |
|  |

* 1. “Public IP Address/DNS Name label”에 마우스를 가져가면 “Click to Copy”로 주소를 복사 할 수 있습니다.

|  |
| --- |
|  |

* 1. 웹 브라우저를 띄우고 주소창에 아래와같이 입력 합니다. “https”로 접속합니다.

|  |
| --- |
|  |

* 1. 브라우저에 따라 화면은 다를 수 있으나, 믿을 수 없다는 오류를 보게될 수 있습니다. 테스트용 인증서로 인해 경고 화면을 볼 수 있지만 보안 문제가 없으니 “Continue to this webpage” 를 클릭하여 계속 진행합니다.

|  |
| --- |
|  |

* 1. Splunk 관리자 로그인 화면에서 ID는 “admin” 암호는 설정한 값을 입력하여 “Sing in” 합니다.

|  |
| --- |
|  |

1. 로그인 및 쿼리를 실행하여 테스트 합니다.
   1. 로그인에 성공하면 아래와 같이 “검색 및 보고”를 클릭합니다.

|  |
| --- |
|  |

* 1. 처음 로그인하는 경우 기본적인 투어를 진행하는데 본 실습에서는 해당 과정을 건너뛰도록 합니다.

|  |
| --- |
|  |

* 1. 검색창에 아래 쿼리를 실행합니다. 정상적으로 Splunk가 동작하는지 테스트 합니다.

|  |
| --- |
| index=”\_internal” \* |
|  |

1. 실습 환경을 삭제합니다.
   1. 리소스 그룹을 선택합니다. “Delete”를 클릭합니다.

|  |
| --- |
|  |

* 1. 삭제를 확인하기위해서 리소스 그룹 이름을 입력합니다. “splunk-dev”를 입력하고 하단에 [Delete]가 활성화 되면 클릭하여 삭제하도록 합니다. 리소스에 포함된 모든 리소스들이 삭제 됩니다.

|  |
| --- |
|  |

실습이 종료되었습니다. 불필요한 서비스를 삭제하여 비용 지출을 최소화 하도록 합니다.