

백서

ANSIBLE
IN DEPTH

"Ansible은 지금 당장 사용하고 싶을 정도로 매우 흥미롭습니다. 단 5줄의 코드를 작성하기만 하면 바로 당신이 원하는 대로 실행됩니다. SSH와 Ansible을 이용하여 이전 서버들을 사용하지 않고도 500대의 서버로 명령을 보낼 수 있습니다."

MARK MAAS
UNIX/LINUX 시스템
관리자
BINCKBANK

들어가는 글

Ansible은 오픈 소스로 만들어진 IT 설정 관리, 배포 및 오케스트레이션 툴입니다. 많은 측면에서 다른 관리 툴과는 분명하게 차별화되며 여타 자동화 솔루션들의 많은 핵심 기능들에 대한 보다 생산적인 대안으로서 매우 다양한 자동화 관련 과제에서 막대한 생산성 향상 효과를 실현하는 데 그 목적을 두고 있습니다. 뿐만 아니라, Ansible은 복잡한 다계층 워크플로우의 오케스트레이션과 단일 배너 아래에 OS 설정 및 애플리케이션 소프트웨어 배포를 명확하게 통합하는 등 해결되지 않은 IT 과제를 해결할 수 있습니다.

Ansible은 그 속성상 최소화되고 일관되며 안전할 뿐만 아니라 매우 안정적으로 설계되었으며 운영자, 개발자 및 IT 관리자들이 이를 익히는 데 필요한 학습 기간은 매우 짧습니다. Ansible은 IT 작업에 대한 설명을 쉽게 작성하고 쉽게 이해될 수 있도록 하는 데 중점을 두고 있기 때문에 새로운 사용자들은 신속하게 신규 프로젝트에 참여할 수 있으며 심지어 몇 개월 간 프로젝트에서 빠져 있었던 경우에도 오랜 기간 동안 누적된 자동화 콘텐츠를 손쉽게 이해할 수 있습니다. Ansible은 전문가 사용자들을 위해 기능들을 강력하게 만드는 동시에, 기술 수준이 다른 모든 사용자들이 동등하게 접근할 수 있도록 함으로써 IT 프로젝트가 시장에 출시되는 시간을 단축하고 IT 설정 변경 과정에서 발생하는 소요 시간과 실수가 발생할 가능성을 줄일 수 있도록 합니다.

아키텍처, 에이전트 및 보안

Ansible이 이 분야의 여타 많은 툴들과 구분되는 중요한 차이점 중 하나는 아키텍처입니다. Ansible은 '푸시(push)' 모델로 실행되는 에이전트리스(agentless) 툴이기 때문에 원격 머신들을 관리하기 위해 그 어떤 에이전트 소프트웨어도 설치할 필요가 없습니다. Ansible은 기본적으로 SSH(Linux 및 UNIX) 또는 WinRM(Windows)으로 원격 머신들을 관리하며 플랫폼들에서 이미 기본적으로 실행되고 있는 원격 관리 프레임워크를 이용합니다.

Ansible은 별도의 전용 사용자 또는 자격 증명을 요구하지 않습니다. Ansible을 실행할 때 사용자가 제공한 자격 증명을 그대로 사용합니다. 마찬가지로, Ansible은 관리자의 접근을 요구하지 않으며 필요에 따라 요청 시 sudo, su 및 기타 권한 확대 방법을 활용합니다.

이 방법은 Ansible이 더욱 안전하게 보호될 수 있도록 합니다. 사용자가 전달한 자격 증명을 이용하여 컨트롤 서버(또는 소스 컨트롤)에 접근한 경우, 원격 시스템에 대한 자격 증명을 보유하지 않고서는 원격 시스템으로 푸시되는 콘텐츠를 작성하거나 이에 여타 명령을 내릴 수 없습니다. 마찬가지로 필요한 코드(일명 Ansible의 '모듈')만 원격 머신으로 전달되는 푸시 기반 모델에서 운영함으로써 원격 머신은 여타 머신들이 어떻게 설정되어 있는지를 보거나 이에 영향을 미칠 수 없습니다.

에이전트리스 방식으로 실행되기 때문에 Ansible이 관리하지 않는 관리 대상 머신에서는 그 어떤 자원도 소모되지 않습니다. 이와 같은 특징들 모두는 Ansible은 관리 에이전트의 안정성 또는 성능에 대해 민감한 고도의 보안 또는 고성능이 요구되는 사례에 이상적일 뿐만 아니라, 모든 컴퓨팅 영역 전반에 유용합니다.

PLAYBOOK 및 Role

Ansible은 playbook을 통해 IT 환경의 자동화 및 오케스트레이션을 실행합니다. Playbook은 자동화의 특정 영역이 실행되어야 하는 방식을 기술한 YAML 정의입니다. 그 이름에서 알 수 있듯이, Ansible playbook은 작업 실행 방법 - 이 경우, IT 자동화 - 에 대한 규범적이면서도 이해하기 쉬운 설명으로서, IT 인프라의 각 구성 요소가 무엇을 실행해야 하는지를 명확하게 기술하고 있는 동시에, 계속해서 구성 요소들이 발견된 정보에 반응하고 상호 연계하여 실행할 수 있도록 합니다.

Ansible playbook은 자동화를 정의하는 일련의 '플레이들'(plays)로 구성되어 있으며 이 플레이들(plays)은 인벤토리(inventory)로 정의된 호스트들을 대상으로 작동됩니다. 각 '플레이'는 여러 '작업(task)'으로 구성되어 있으며 인벤토리 내에 정의된 하나의 호스트, 다수의 호스트 또는 모든 호스트를 대상으로 작동할 수 있습니다. 각 작업은 Ansible 모듈 - 특정 작업을 실행하기 위한 소규모 코드를 호출하여 실행됩니다. 이들 작업들은 타깃 머신상에 설정 파일을 배포하거나 소프트웨어 패키지를 설치하는 것처럼 간단할 수도 있고, Amazon EC2의 전체 CloudFormation 인프라를 스피ن 업(spin up)하는 것과 같이 복잡할 수도 있습니다. Ansible은 단순한 설정 관리에서 네트워크 장치 관리, 모든 주요 클라우드 서비스 업체들에 대한 인프라 관리를 위한 모듈에 이르기까지 수백 개의 모듈을 포함하고 있습니다.

Ansible 모듈에 포함된 핵심 사상은 사용자가 원하는 상태로 시스템을 손쉽게 바꾸도록 하는 것입니다. 실제로 Ansible 모듈은 지정된 작업이 이를 실행하기 전에 완료되어야 하는 지 확인합니다. 예를 들어, Ansible 작업이 웹 서버를 시동하도록 정의된 경우, 작업은 웹 서버가 시동되지 않은 경우에만 수행됩니다. 이 목표 상태 설정(desired state configuration)은 종종 '멱등성(idempotency)'으로도 불리며 해당 설정이 부작용 없이 반복적으로 적용되고 이미 적용된 경우에는 신속하고 효율적으로 실행될 수 있도록 합니다.

Ansible은 또한 playbook 작업을 일명 'Role'로 캡슐화하도록 지원합니다. Ansible Role은 개발, 테스트 및 프로덕션 자동화에 사용될 수 있는 공통 웹 서버 설정 Role을 구성하는 등 다양한 시나리오에서 공통적인 설정을 손쉽게 적용하는 데 이용될 수 있습니다. Ansible Galaxy 커뮤니티 사이트는 playbook을 개발하는 데 사용되고 사용자가 지정할 수 있는 수많은 Role을 포함하고 있습니다.

첨단 기능

Ansible playbook 언어는 작업의 조건부 실행, 원격 시스템에서 변수 및 정보를 수집하는 기능, 비동기식 장시간 실행 작업을 스폰닝(spawn)하는 기능, 푸시(push) 또는 풀(pull) 설정 중 하나로 운영하는 기능, 변경을 적용하지 않고 보류하기 위한 "검사(check)" 모드, 특정 play 및 작업에 태그하여 해당 설정 부분만 적용될 수 있도록 하는 기능 등을 비롯해 복잡한 자동화 플로우를 지원하는 다양한 기능들을 포함하고 있습니다. 이들 기능들은 귀사의 애플리케이션과 환경이 자동화 개발자뿐만 아니라 개발자에서 운영자, 그리고 CIO에 이르는 모든 사람들이 쉽게 이해할 수 있는 논리 프레임워크 내에서 간편하고 손쉽게 모델링될 수 있도록 지원합니다.

복잡한 오케스트레이션을 위한 PLAYBOOK 활용

여러 작업들을 하나의 playbook으로 결합함으로써 복잡한 자동화를 수행할 수 있습니다. 상세한 예시로서, 전통적인 3 티어 웹 애플리케이션과 다음으로 구성된 환경을 생각해 보도록 하겠습니다.

- 애플리케이션 서버
- 데이터베이스 서버
- 콘텐츠 서버
- 로드 밸런서
- 추가로 호출기 알림 서비스와 같은 경보 시스템에 연결된 모니터링 시스템

이 예시에서, Ansible은 다음으로 구성된 복잡한 클러스터 전체 롤링 업데이트(rolling update) 프로세스를 구현하는 데 손쉽게 이용될 수 있습니다.

- 관련 서버에 대한 정보를 위한 구성/설정 리포지터리 컨설팅
- 모든 머신상의 기반 OS 설정 및 목표 상태 적용
- 업데이트할 서버 애플리케이션 서버 부분 파악
- 서버를 오프라인으로 전환하기 전에 모니터링 시스템으로 중단 윈도우 신호 전송
- 애플리케이션 서버를 로드 밸런싱된 풀에서 배제시키기 위해 로드 밸런서로 신호 전송
- 웹 애플리케이션 서버 작동 정지
- 웹 애플리케이션 서버 코드, 데이터 및 콘텐츠 배포 또는 업데이트
- 웹 애플리케이션 서버 작동 시작
- 새로운 서버 및 코드상에서 적절한 테스트 실행
- 애플리케이션 서버를 로드 밸런싱된 풀에 추가하기 위해 로드 밸런서로 신호 전송
- 해당 서버들에서 감지된 모든 이슈에 대한 경보를 재개하기 위해 모니터링 시스템으로 신호 전송
- 롤링 업데이트 프로세스에서 나머지 애플리케이션 서버들에 대해 이러한 프로세스 반복
- 데이터베이스 또는 콘텐츠 티어 등 다른 티어들에 대해 이들 롤링 업데이트 프로세스 반복
- 업데이트가 완료되면, 이메일 보고서 전송 및 필요 시 로깅

머신 그룹 내 클러스터 전반에서 이 playbook을 실행함으로써 다운타임 없이 애플리케이션 업데이트가 수행될 수 있습니다.

"처음에는 Ansible가 오케스트레이션에도 뛰어나다는 것을 인식하지 못했지만, 곧 그 사실을 깨달았습니다. 경쟁 업체들을 훨씬 능가한다는 점에서 더할 나위 없이 만족하고 있습니다."

BEIER CAI
기술 담당 디렉터
HOOTSUITE MEDIA, INC.

확장성

Ansible은 여러 차원으로 확장될 수 있습니다.

위에서 언급했듯이 Ansible은 원격 호스트상에서 실행되는 소규모 코드인 '모듈'에 의해 실행됩니다. 450개 이상의 모듈 세트를 포함한 Ansible에서 지원하지 않는 IT 인프라의 일정 부분을 처리하기 위해 새로운 모듈이 필요한 경우, Ansible을 손쉽게 확장할 수 있습니다. Ansible과 함께 제공된 모듈들은 Python과 PowerShell로 구현되지만, Ansible 모듈들은 원하는 모든 언어로 작성될 수 있습니다. 단, JSON을 인풋으로, product JSON을 아웃풋으로 해야 합니다.

또한, Ansible은 동적 인벤토리(dynamic inventory)에 대한 지원을 통해 확장될 수 있습니다. 동적 인벤토리는 정적으로 정의된 것이 아니라, 런타임 시 발견된 머신 및 인프라 세트에서 실행될 수 있도록 합니다. 일반적으로 이는 퍼블릭 또는 프라이빗 클라우드 서비스 업체, 가상화 업체 또는 CMDB 등의 정보를 판독하여 수행됩니다. Ansible은 모든 주요 클라우드 서비스 사업자에 대한 즉각적인 지원을 포함하고 있으며 필요에 따라 신규 사업자와 새로운 데이터 소스에 대한 지원을 추가하도록 손쉽게 확장될 수 있습니다. 모든 스크립팅 또는 컴파일 언어로 커스텀 프로그램을 작성하기만 하면, JSON 인벤토리 정의를 반환할 수 있습니다.

많은 기능들이 플러그인 메커니즘으로 구현되어 있기 때문에 Ansible 자체의 런타임 실행도 쉽게 확장됩니다. Ansible의 정상적인 출력 디스플레이는 작업이 실행될 때 이벤트를 처리하는 콜백(callback) 플러그인 센트를 통해 처리되며 새로운 콜백 플러그인은 로그 어그리게이터(log aggregator)에 기록되고 알림 서비스에 메시지를 전송하는 등의 작업을 수행할 수 있습니다. 매니지드 머신에 연결하기 위한 Ansible의 SSH 및 WinRM 사용은 연결 플러그인을 통해 이루어지며 원하는 새로운 방식으로 매니지드 노드에 접근하기 위해 새로운 연결 플러그인을 작성할 수 있습니다. 런타임 시 새로운 자격 증명 스토리지 메커니즘 또는 CMDB에서 변수, 암호 및 자격 증명을 조회하기 위해 새로운 룩업(lookup) 플러그인을 작성할 수 있습니다.

이와 같은 Ansible의 확장성은 귀사의 환경을 어떻게 사용자 지정하건 관계 없이 Ansible과 쉽게 연동할 수 있다는 것을 의미합니다. Ansible의 오픈 소스 속성은 새로운 기능들을 추가해 모든 릴리스의 Ansible을 확장하고 변경 사항들을 손쉽게 되돌릴 수 있도록 합니다.

툴 통합

Ansible은 IT 설정 및 프로세스 모두를 심지어 이들 설정을 판독하는 것과 관련한 훈련을 받지 않은 이들도 쉽게 읽고 쓸 수 있도록 하는 데 목표를 두고 있습니다. Ansible은 모든 타입의 자동화 작업을 실행할 수 있지만, 소프트웨어 프로그래밍 언어가 아니라, 목표 상태 및 프로세스에 대한 기본적인 텍스트 설명에 가까우며 설명된 프로세스의 타입에 중립적입니다.

다른 전통적인 접근 방식에서는 사용자들이 일반적으로 많은 다른 툴들을 함께 결합하여 IT OS 및 소프트웨어 설정을 관리하기 위한 기본 요건들을 지원해야 합니다. 하지만, Ansible의 단순한 작업 기반 속성에 힘 입어 다음과 같은 다양한 유스 케이스에 적용할 수 있습니다.

- 설정 관리 - 시스템의 목표 상태 설명을 위해, 수작업으로 또는 프로비저닝 툴을 통해 호출
- 애플리케이션 구축 - 호스팅 애플리케이션 소프트웨어를 1대의 머신 또는 일련의 머신들로 푸시하기 위해
- 오케스트레이션 - 롤링 클러스터 업그레이드와 같은 다중 머신 프로세스의 조율을 위해
- 필요 시(as-needed) 작업 실행 - 일괄 서버 재부팅과 같이 이전 모델에서는 적합하지 않았던 작업들을 즉시 수행하기 위해

Ansible은 단일 툴에서 이들 접근 방식들을 이용할 수 있도록 합니다. 이는 여러 다양한 프로세스들을 단일 프레임워크로 통합함으로써 훈련, 교육 및 운영을 용이하게 할 뿐만 아니라, Ansible이 다른 툴들과 함께 원활하게 연동될 수 있다는 것을 의미합니다. 이는 이미 사용 중인 기존 인프라의 중단 없이 이들 모든 유스 케이스에서 활용될 수 있습니다.

클라우드 및 인프라 통합

Ansible은 Amazon Web Services, Microsoft Azure, Rackspace, Google Compute Engine 등과 같은 클라우드 서비스 사업자와 VMware, OpenStack 및 CloudStack 등과 같은 로컬 인프라 등을 비롯해 다양한 퍼블릭 및 온 프레미스 클라우드 환경에 손쉽게 작업 부하를 배포할 수 있습니다. 여기에는 컴퓨팅 프로비저닝뿐만 아니라, 스토리지와 네트워크도 포함됩니다. 앞서 밝힌 바와 같이 추가적인 통합은 손쉽게 수행되며 새로운 Ansible 릴리스가 발표될 때마다 더 많은 요소들을 추가할 수 있습니다.

"Ansible 팀이 수행하고 있는 작업에 대해 ... 모든 업계가 주목해야 합니다."

LEW TUCKER
클라우드 컴퓨팅 담당 부사장 겸 CTO
CISCO

네트워크 자동화

Ansible은 전통적인 IT 서버 및 소프트웨어 설치의 물론, 전통적인 IT 자동화 툴에서 지원되지 않는 영역을 포함하여 전체 IT 인프라를 자동화한다는 목표를 추구하고 있습니다. Ansible의 작업 기반 에이전트리스 속성은 네트워킹 영역에 손쉽게 적용할 수 있도록 하며 Cisco, Juniper, Hewlett Packard Enterprise, Cumulus 등과 같은 주요 벤더의 네트워킹을 자동화하기 위한 지원이 Ansible에 포함되어 있습니다.

이와 같은 네트워킹 지원을 활용함으로써 이제 더 이상 별도의 팀, 별도의 툴, 그리고 별도의 프로세스를 통해 네트워크 자동화를 추진할 필요가 없으며, 이미 보유하고 있는 여타 자동화 기술에서 사용하는 것과 동일한 툴 및 프로세스를 통해 수행할 수 있습니다. 새로운 서비스를 위한 스위칭과 VLAN의 설정은 이제 네트워킹 팀에게 지원을 요청해야 하는 어려운 작업이 아니라, 배포 playbook에 단 몇 개의 Ansible 작업만 추가하기만 되는 간단한 작업이 됩니다.

ANSIBLE TOWER BY RED HAT

자동화에 대한 통제력, 지식 및 권한 이임을 확대하려는 기업들을 위해, Ansible은 Ansible Tower를 제공합니다. Tower는 Ansible을 토대로 개발되어 모든 자동화를 위해 안전한 자격 증명 저장, 기본 내장된 권한 위임 및 작업 사용자 정의, 역할 기반 접근 제어 및 중앙 집중식 로깅 및 감사 기능을 제공합니다. Tower는 최종 사용자를 위한 웹 기반 콘솔과 Ansible Tower를 기존 툴 및 워크플로우에 내장하기 위한 완벽한 기능을 갖춘 REST API 모두를 포함하고 있습니다. 보다 자세한 정보는 ansible.com/tower에서 확인할 수 있습니다.

예제 및 자세한 정보

위에서 언급한 기업들을 구현하는 Ansible 콘텐츠의 몇 가지 기본 예제들이 github.com/ansible/ansible-examples에서 제공됩니다. 이와 같은 프로세스를 자체 소스 컨트롤과 통합하거나, 빌드 시스템을 구축하거나 자체 네트워크 환경을 통합하는 것과 관련한 보다 자세한 정보를 원하시면, 한국레드햇으로 문의해 주십시오.

자동화를 시작할 준비가 되셨습니까?

buy-kr@redhat.com

080-708-0880

ansible.com

redhat.com/ko/global/south-korea