Terraform 시작하기: AWS CDK 및 AWS CloudFormation 전문가를 위한 지침

AWS 권장 가이드

AWS 권장 가이드: Terraform 시작하기: AWS CDK 및 AWS CloudFormation 전문가를 위한 지침

Table of Contents

Terraform 시작하기: AWS CDK 및 AWS 전문가를 위한 지침 CloudFormation

스티븐 구겐하이머, Amazon Web Services ()AWS

2024년 3월 (문서 기록)

클라우드 리소스 프로비저닝 경험이 독점적으로 의 영역에 속한다면 AWS, AND 이외의 코드형 인프라 (IaC) 도구에 대한 경험은 제한적일 수 있습니다. AWS 클라우드 개발 키트 (AWS CDK)AWS CloudFormation 사실 Hashicorp Terraform과 같은 유사한 도구는 전혀 익숙하지 않을 수 있습니다. 하지만 클라우드 여정에 깊이 들어갈수록 Terraform을 접할 수밖에 없게 됩니다. 핵심 개념에 익숙해지는 것이 분명 여러분에게 유리할 것입니다.

Terraform AWS CDK, 및 는 비슷한 목표를 CloudFormation 달성하고 많은 핵심 개념을 공유하지만 몇 가지 차이점이 있습니다. Terraform을 처음 사용하는 경우 이러한 차이점에 대비하지 못할 수도 있습니다. 결국 CloudFormation 스택은 모두 내부에 AWS 계정기반을 두고 있기 때문에 유지 관리하는 대부분의 AWS CDK 리소스와 직접적인 관계를 맺게 됩니다. Terraform은 단일 클라우드 공급자의 환경을 기반으로 하지 않습니다. 따라서 다양한 공급자를 지원할 수 있는 유연성이 제공되지만, 어느 정도의 리소스부터 원격 위치까지 리소스를 유지해야 합니다.

이 가이드는 Terraform의 핵심 개념을 이해하기 쉽게 설명하여 발생하는 모든 IaC 문제를 해결하는 데 도움이 됩니다. Terraform이 공급자, 모듈 및 상태 파일과 같은 개념을 사용하여 리소스를 프로비저닝하는 방법에 중점을 둡니다. 또한 Terraform 개념을 및 가 유사한 작업을 수행하는 방식과 대조합니다 AWS CDK . CloudFormation

> **Note**
>
> 개발자가 프로그래밍 방식의 코딩 언어를 사용하여 CloudFormation 스택을 배포하는 AWS CDK 데 도움이 됩니다. 실행한 `cdk synth` 후에는 코드가 템플릿으로 CloudFormation 변환됩니다. 그 시점부터 프로세스는 과 (와) AWS CDK 모두 동일합니다 CloudFormation. 간결하게 설명하기 위해 이 안내서에서는 일반적으로 AWS IaC 프로세스를 CloudFormation 용어로 언급하지만 비교 역시 IaC 프로세스를 참조하기에 적합합니다. AWS CDK

CloudFormation 및 테라폼 용어

AWS CDK Terraform과 CloudFormation AND를 비교할 때 IaC 핵심 개념을 설명하는 데 사용되는 용어가 일치하지 않아 IaC 핵심 개념을 조정하는 것이 어려울 수 있습니다. 다음은 이러한 용어와 이 가이드에서 이러한 용어를 참조하는 방법입니다.

- 스택 — 스택은 CI/CD 파이프라인에 배포되고 단일 유닛으로 추적할 수 있는 IaC입니다. 에서는 이 용어가 흔히 사용되지만 CloudFormation Terraform에서는 이 용어를 실제로 사용하지 않습니다. Terraform 스택은 모든 하위 모듈이 포함된 배포된 루트 모듈입니다. 하지만 모듈이라는 용어와 혼동되지 않도록 이 가이드에서는 스택이라는 용어를 사용하여 두 도구의 단일 배포를 설명합니다.
- 상태 - 상태는 IaC 배포 스택 내에서 현재 추적되는 모든 리소스와 해당 리소스의 현재 구성입니다. Terraform 상태 및 백엔드 이해섹션에서 설명한 것처럼 Terraform은 상태라는 용어를 보다 많이 사용합니다. CloudFormation Terraform에서는 상태를 유지하는 것이 더 잘 보이지만 상태를 추적하고 업데이트하는 것도 마찬가지로 중요하기 때문입니다. CloudFormation
- IaC 파일 — IaC 파일은 코드형 인프라 (IaC) 언어를 포함하는 단일 파일입니다. CloudFormation 단일 CloudFormation 파일을 템플릿이라고 합니다. 하지만 Terraform의 템플릿과 템플릿 파일은 완전히 다릅니다. Terraform의 CloudFormation 템플릿과 동일한 것을 구성 파일이라고 합니다. 이 안내서의 혼동을 최소화하기 위해 파일 또는 IaC 파일이라는 용어는 CloudFormation 템플릿과 Terraform 구성 파일을 모두 지칭하는 데 사용됩니다.

다음 표에서는 와 Terraform에 사용되는 용어를 비교합니다. CloudFormation 이 표의 목적은 유사점을 보여주는 것입니다. 이는 one-to-one 비교가 아닙니다. Terraform 간에는 각 개념이 최소한 CloudFormation 약간씩 다릅니다. 개념은 이 가이드의 관련 섹션에 자세히 설명되어 있습니다.

CloudFormation 용어	테라폼 용어	이 가이드의 섹션
CDK 인터페이스 (예: iBucket)	데이터 소스	테라폼 데이터 소스 이해
변경 세트	계획	테라폼 모듈에 대한 이해
조건 함수	조건식	Terraform 함수, 표현식 및 메타 인수 이해
`DependsOn` 속성	`depends_on` 메타 인수	Terraform 함수, 표현식 및 메타 인수 이해

CloudFormation 용어	테라폼 용어	이 가이드의 섹션
내장 함수	함수	Terraform 함수, 표현식 및 메타 인수 이해
모듈	모듈	테라폼 모듈에 대한 이해
결과	출력 값	테라폼 변수, 로컬 값 및 출력에 대한 이해
파라미터	Variables	테라폼 변수, 로컬 값 및 출력에 대한 이해
레지스트리	제공업체	테라폼 제공자에 대한 이해
템플릿	구성 파일	모두

Terraform 리소스 이해

AWS CloudFormation 및 Terraform이 모두 존재하는 주된 이유는 클라우드 리소스의 생성 및 유지 관리입니다. 하지만 클라우드 리소스란 정확히 무엇입니까? CloudFormation 리소스와 Terraform 리소스는 동일한가요? 답은... 예와 아니요입니다. 이를 설명하기 위해이 가이드에서는 CloudFormation을 사용한 다음 Terraform을 사용하여 Amazon Simple Storage Service(Amazon S3) 버킷을 생성하는 예를 제공합니다.

다음 CloudFormation 코드 예제에서는 샘플 Amazon S3 버킷을 생성합니다.

```
{
    "myS3Bucket": {
        "Type": "AWS::S3::Bucket",
        "Properties": {
            "BucketName": "my-s3-bucket",
            "BucketEncryption": {
                "ServerSideEncryptionConfiguration": [
                    {
                        "ServerSideEncryptionByDefault": {
                            "SSEAlgorithm": "AES256"
                        }
                    }
                ]
            },
            "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": true,
                "BlockPublicPolicy": true,
                "IgnorePublicAcls": true,
                "RestrictPublicBuckets": true
            },
            "VersioningConfiguration": {
                "Status": "Enabled"
            }
        }
    }
}
```

다음 Terraform 코드 예제에서는 동일한 Amazon S3 버킷을 생성합니다.

```
resource "aws_s3_bucket" "myS3Bucket" {
  bucket = "my-s3-bucket"
```

```
}

resource "aws_s3_bucket_server_side_encryption_configuration" "bucketencryption" {
  bucket = aws_s3_bucket.myS3Bucket.id
  rule {
    apply_server_side_encryption_by_default {
      sse_algorithm = "AES256"
    }
  }
}

resource "aws_s3_bucket_public_access_block" "publicaccess" {
  bucket                  = aws_s3_bucket.myS3Bucket.id
  block_public_acls       = true
  block_public_policy     = true
  ignore_public_acls      = true
  restrict_public_buckets = true
}

resource "aws_s3_bucket_versioning" "versioning" {
  bucket = aws_s3_bucket.myS3Bucket.id
  versioning_configuration {
    status = "Enabled"
  }
}
```

Terraform의 경우 공급자는 리소스를 정의한 다음 개발자는 해당 리소스를 선언하고 구성합니다. 공급자는이 가이드에서 다음 섹션에서 설명하는 개념입니다. Terraform 예제에서는 여러 S3 버킷의 설정에 대해 완전히 별도의 리소스를 생성합니다. 설정을 위한 별도의 리소스를 생성하는 것이 Terraform AWS 공급자가 AWS 리소스를 처리하는 방식에 반드시 일반적인 것은 아닙니다. 그러나이 예제는 중요한 차이점을 보여줍니다. CloudFormation 리소스는 CloudFormation 리소스 사양에 따라 엄격하게 정의되지만 Terraform에는 이러한 요구 사항이 없습니다. Terraform에서 리소스의 개념은 약간 더 모호합니다.

단일 리소스가 무엇인지 정의하는 정확한 가드레일과 관련하여 도구가 다를 수 있지만 일반적으로 클라우드 리소스는 클라우드에 존재하고 생성, 업데이트 또는 삭제할 수 있는 모든 특정 엔터티입니다. 따라서 관련된 리소스 수에 관계없이 이전 두 예제 모두 내에서 정확히 동일한 설정을 사용하여 정확히 동일한 사물을 생성합니다 AWS 계정.

테라폼 제공자에 대한 이해

Terraform에서 공급자는 클라우드 제공업체, 타사 도구 및 기타 API와 상호 작용하는 플러그인입니다. Terraform을 함께 AWS사용하려면 리소스와 상호 작용하는 AWS 공급자를 사용해야 합니다. AWS

AWS CloudFormation 레지스트리를 사용하여 타사 확장을 배포 스택에 통합한 적이 없다면 Terraform 공급자가 익숙해지는 데 시간이 걸릴 수 있습니다. CloudFormation 가 기본으로 제공되기 때문에 기본적으로 AWS 리소스 공급자가 이미 있습니다. AWS반면 Terraform에는 단일 기본 공급자가 없으므로 주어진 리소스의 출처에 대해 아무 것도 가정할 수 없습니다. 즉, Terraform 구성 파일에서 가장 먼저 선언해야 할 것은 리소스가 정확히 어디로 가고 어떻게 전달되는지입니다.

이러한 구분은 Terraform에는 존재하지 않는 복잡성을 한층 더 가중시킵니다. CloudFormation 하지만 이러한 복잡성으로 인해 유연성이 향상됩니다. 단일 Terraform 모듈 내에서 여러 공급자를 선언할 수 있으며, 그러면 생성된 기본 리소스가 동일한 배포 계층의 일부로 서로 상호 작용할 수 있습니다.

이는 다양한 방식으로 유용할 수 있습니다. 제공업체가 반드시 별도의 클라우드 공급자를 위한 것은 아닙니다. 공급자는 클라우드 리소스의 모든 소스를 대표할 수 있습니다. 아마존 엘라스틱 쿠버네티스 서비스 (Amazon EKS) 를 예로 들어 보겠습니다. Amazon EKS 클러스터를 프로비저닝할 때 Helm 차트를 사용하여 타사 확장을 관리하고 Kubernetes 자체를 사용하여 포드 리소스를 관리하는 것이 좋습니다. Helm과 Kubernetes에는 모두 자체 Terraform 공급자가 있으므로 AWS이러한 리소스를 모두 동시에 프로비저닝 및 통합한 다음 이들 간에 값을 전달할 수 있습니다.

Terraform의 다음 코드 예제에서 AWS 제공자는 Amazon EKS 클러스터를 생성한 다음 결과 쿠버네티스 구성 정보가 헬름 및 쿠버네티스 제공자 모두에게 전달됩니다.

```
terraform {
  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = ">= 4.33.0"
    }

    helm = {
      source  = "hashicorp/helm"
      version = "2.12.1"
    }

    kubernetes = {
      source  = "hashicorp/kubernetes"
      version = "2.26.0"
```

```
    }
  }
  required_version = ">= 1.2.0"
}

provider "aws" {
  region = "us-west-2"
}

resource "aws_eks_cluster" "example_0" {
  name     = "example_0"
  role_arn = aws_iam_role.cluster_role.arn
  vpc_config {
    endpoint_private_access = true
    endpoint_public_access  = true
    subnet_ids              = var.subnet_ids
  }
}

locals {
  host        = aws_eks_cluster.example_0.endpoint
  certificate = base64decode(aws_eks_cluster.example_0.certificate_authority.data)
}

provider "helm" {
  kubernetes {
    host                   = local.host
    cluster_ca_certificate = local.certificate
    # exec allows for an authentication command to be run to obtain user
    # credentials rather than having them stored directly in the file
    exec {
      api_version = "client.authentication.k8s.io/v1beta1"
      args        = ["eks", "get-token", "--cluster-name",
 aws_eks_cluster.example_0.name]
      command     = "aws"
    }
  }
}

provider "kubernetes" {
  host                   = local.host
  cluster_ca_certificate = local.certificate
  exec {
    api_version = "client.authentication.k8s.io/v1beta1"
```

```
    args        = ["eks", "get-token", "--cluster-name",
 aws_eks_cluster.example_0.name]
    command     = "aws"
  }
}
```

두 IaC 도구의 경우 공급자와 관련하여 절충점이 있습니다. Terraform은 배포를 주도하는 엔진인 외부에 위치한 공급자 패키지에 전적으로 의존합니다. CloudFormation 모든 주요 AWS 프로세스를 내부적으로 지원합니다. 를 사용하면 타사 확장 프로그램을 통합하려는 경우에만 타사 공급자에 대해 걱정할 필요가 있습니다. CloudFormation 각 접근 방식에는 장단점이 있습니다. 어느 것이 적합한지는 이 가이드의 범위를 벗어나지만, 두 도구를 모두 평가할 때는 차이점을 기억하는 것이 중요합니다.

Terraform 별칭 사용

Terraform에서는 사용자 지정 구성을 각 공급자에게 전달할 수 있습니다. 그렇다면 동일한 모듈 내에서 여러 공급자 구성을 사용하려면 어떻게 해야 할까요? 이 경우 별칭을 사용해야 합니다. 별칭은 리소스별 또는 모듈별 수준에서 사용할 제공자를 선택하는 데 도움이 됩니다. 동일한 제공자의 인스턴스가 두 개 이상 있는 경우 별칭을 사용하여 기본이 아닌 인스턴스를 정의합니다. 예를 들어 기본 제공자 인스턴스는 특정 AWS 리전제공자 인스턴스일 수 있지만 별칭을 사용하여 대체 지역을 정의할 수 있습니다.

다음 Terraform 예제는 별칭을 사용하여 다양한 버킷을 프로비저닝하는 방법을 보여줍니다. AWS 리전 공급자의 기본 지역은 이지만`us-west-2`, east 별칭을 사용하여 리소스를 프로비저닝할 수 있습니다. `us-east-2`

```
provider "aws" {
  region = "us-west-2"
}

provider "aws" {
  alias  = "east"
  region = "us-east-2"
}

resource "aws_s3_bucket" "myWestS3Bucket" {
  bucket = "my-west-s3-bucket"
}

resource "aws_s3_bucket" "myEastS3Bucket" {
  provider = aws.east
  bucket   = "my-east-s3-bucket"
```

```
}
```

이전 예제에서 볼 수 있듯이 `provider` 메타 인수와 `alias` 함께 를 사용하면 특정 리소스에 대해 다른 제공자 구성을 지정할 수 있습니다. 단일 스택에 여러 리소스를 프로비저닝하는 것은 AWS 리전 시작에 불과합니다. 앨리어싱 공급자는 여러 면에서 매우 편리합니다.

예를 들어, 한 번에 여러 Kubernetes 클러스터를 프로비저닝하는 것은 매우 일반적입니다. 별칭은 Helm 및 Kubernetes 공급자를 추가로 구성하는 데 도움이 되므로 Amazon EKS 리소스별로 이러한 타사 도구를 다르게 사용할 수 있습니다. 다음 Terraform 코드 예제는 별칭을 사용하여 이 작업을 수행하는 방법을 보여줍니다.

```
resource "aws_eks_cluster" "example_0" {
  name     = "example_0"
  role_arn = aws_iam_role.cluster_role.arn
  vpc_config {
    endpoint_private_access = true
    endpoint_public_access  = true
    subnet_ids              = var.subnet_ids[0]
  }
}

resource "aws_eks_cluster" "example_1" {
  name     = "example_1"
  role_arn = aws_iam_role.cluster_role.arn
  vpc_config {
    endpoint_private_access = true
    endpoint_public_access  = true
    subnet_ids              = var.subnet_ids[1]
  }
}

locals {
  host         = aws_eks_cluster.example_0.endpoint
  certificate  = base64decode(aws_eks_cluster.example_0.certificate_authority.data)
  host1        = aws_eks_cluster.example_1.endpoint
  certificate1 = base64decode(aws_eks_cluster.example_1.certificate_authority.data)
}

provider "helm" {
  kubernetes {
    host                   = local.host
    cluster_ca_certificate = local.certificate
    exec {
```

```
      api_version = "client.authentication.k8s.io/v1beta1"
      args        = ["eks", "get-token", "--cluster-name",
 aws_eks_cluster.example_0.name]
      command     = "aws"
    }
  }
}

provider "helm" {
  alias = "helm1"
  kubernetes {
    host                   = local.host1
    cluster_ca_certificate = local.certificate1
    exec {
      api_version = "client.authentication.k8s.io/v1beta1"
      args        = ["eks", "get-token", "--cluster-name",
 aws_eks_cluster.example_1.name]
      command     = "aws"
    }
  }
}

provider "kubernetes" {
  host                   = local.host
  cluster_ca_certificate = local.certificate
  exec {
    api_version = "client.authentication.k8s.io/v1beta1"
    args        = ["eks", "get-token", "--cluster-name",
 aws_eks_cluster.example_0.name]
    command     = "aws"
  }
}

provider "kubernetes" {
  alias                  = "kubernetes1"
  host                   = local.host1
  cluster_ca_certificate = local.certificate1
  exec {
    api_version = "client.authentication.k8s.io/v1beta1"
    args        = ["eks", "get-token", "--cluster-name",
 aws_eks_cluster.example_1.name]
    command     = "aws"
  }
```

```
}
```

테라폼 모듈에 대한 이해

코드형 인프라 (IaC) 영역에서 모듈은 재사용을 위해 격리되고 함께 패키징되는 독립형 코드 블록입니다. 모듈의 개념은 Terraform 개발에서 피할 수 없는 부분입니다. 자세한 내용은 Terraform 설명서의 모듈을 참조하십시오. AWS CloudFormation 모듈도 지원합니다. 자세한 내용은 AWS 클라우드 운영 및 마이그레이션 블로그의 AWS CloudFormation 모듈 소개를 참조하십시오.

Terraform의 모듈 간의 주요 차이점은 특수 리소스 유형 () 을 사용하여 CloudFormation 모듈을 가져온다는 것입니다. CloudFormation `AWS::CloudFormation::ModuleVersion` Terraform의 모든 구성에는 루트 모듈이라는 모듈이 하나 이상 있습니다. 기본.tf 파일에 있는 테라폼 리소스 또는 Terraform 구성 파일의 파일은 루트 모듈에 있는 것으로 간주됩니다. 그러면 루트 모듈이 다른 모듈을 호출하여 스택에 포함할 수 있습니다. 다음 예제는 오픈 소스 eks 모듈을 사용하여 Amazon Elastic Kubernetes Service (Amazon EKS) 클러스터를 프로비저닝하는 루트 모듈을 보여줍니다.

```
terraform {
  required_providers {
    helm = {
      source  = "hashicorp/helm"
      version = "2.12.1"
    }
  }
  required_version = ">= 1.2.0"
}

module "eks" {
  source  = "terraform-aws-modules/eks/aws"
  version = "20.2.1"
  vpc_id  = var.vpc_id
}

provider "helm" {
  kubernetes {
    host                   = module.eks.cluster_endpoint
    cluster_ca_certificate =
 base64decode(module.eks.cluster_certificate_authority_data)
  }
}
```

위의 구성 파일에 공급자가 포함되어 있지 않다는 사실을 눈치채셨을 것입니다. AWS 모듈은 독립적이며 자체 제공자를 포함할 수 있기 때문입니다. Terraform 공급자는 전 세계적이므로 하위 모듈의 공급

자를 루트 모듈에서 사용할 수 있습니다. 하지만 모든 모듈 값에 적용되는 것은 아닙니다. 모듈 내의 다른 내부 값은 기본적으로 해당 모듈로만 범위가 지정되며 루트 모듈에서 액세스할 수 있으려면 출력으로 선언해야 합니다. 오픈소스 모듈을 활용하여 스택 내 리소스 생성을 단순화할 수 있습니다. 예를 들어, eks 모듈은 EKS 클러스터를 프로비저닝하는 데 그치지 않고 완벽하게 작동하는 Kubernetes 환경을 프로비저닝합니다. eks 모듈 구성이 요구 사항에 맞으면 이를 사용하면 수십 줄의 코드를 추가로 작성하지 않아도 됩니다.

모듈 호출

Terraform 배포 중에 실행하는 두 가지 기본 Terraform CLI 명령은 테라폼 초기화와 테라폼 적용입니다. 이 `terraform init` 명령이 수행하는 기본 단계 중 하나는 모든 하위 모듈을 찾아 종속 항목으로 디렉터리로 가져오는 것입니다. `.terraform/modules` 개발 중에 외부 소스 모듈을 새로 추가할 때마다 명령을 사용하기 전에 다시 초기화해야 합니다. `apply` Terraform 모듈에 대한 참조를 들으면 이 디렉터리의 패키지를 참조하는 것입니다. 엄밀히 말하면 코드에서 선언하는 모듈은 호출 모듈이므로 실제로는 module 키워드가 실제 모듈을 호출하며, 이 모듈은 종속성으로 저장됩니다.

이런 식으로 호출 모듈은 배포 시 교체될 전체 모듈을 보다 간결하게 나타내는 역할을 합니다. 원하는 기준을 사용하여 스택 내에 자체 모듈을 만들어 리소스를 논리적으로 분리함으로써 이 아이디어를 활용할 수 있습니다. 단, 이 작업의 최종 목표는 스택 복잡성을 줄이는 것이어야 한다는 점만 기억하세요. 모듈 간에 데이터를 공유하려면 모듈 내에서 해당 데이터를 출력해야 하기 때문에 모듈에 너무 많이 의존하면 상황이 지나치게 복잡해질 수 있습니다.

루트 모듈

모든 Terraform 구성에는 적어도 하나의 모듈이 있으므로 가장 많이 다루게 될 모듈인 루트 모듈의 모듈 속성을 검사하는 데 도움이 될 수 있습니다. Terraform 프로젝트를 작업할 때마다 루트 모듈은 최상위 디렉터리의 모든 `.tf` (또는`.tf.json`) 파일로 구성됩니다. 최상위 `terraform apply` 디렉토리에서 실행하면 Terraform은 해당 디렉토리에서 찾은 모든 파일을 실행하려고 시도합니다. `.tf` 하위 디렉터리의 모든 파일은 이러한 최상위 구성 파일 중 하나에서 호출되지 않는 한 무시됩니다.

이렇게 하면 코드를 어느 정도 유연하게 구성할 수 있습니다. 단일 프로세스에 여러 파일이 포함될 수 있기 때문에 Terraform 배포를 파일보다 모듈이라고 부르는 것이 더 정확한 이유이기도 합니다. Terraform이 모범 사례로 권장하는 표준 모듈 구조가 있습니다. 하지만 최상위 디렉터리에 `.tf` 파일을 넣으면 나머지 파일과 함께 실행됩니다. 실제로 모듈을 실행하면 모듈의 모든 최상위 `.tf` 파일이 배포됩니다. `terraform apply` 그렇다면 Terraform은 어떤 파일을 가장 먼저 실행할까요? 이 질문에 대한 답은 매우 중요합니다.

Terraform은 초기화 후와 스택 배포 전에 수행하는 일련의 단계가 있습니다. 먼저 기존 구성을 분석한 다음 종속성 그래프를 생성합니다. 종속성 그래프는 어떤 리소스가 필요하고 어떤 순서로 처리해야 하는지를 결정합니다. 예를 들어 다른 리소스에서 참조되는 속성을 포함하는 리소스는 종속 리소스보다 먼저 처리됩니다. 마찬가지로 depends_on 파라미터를 사용하여 명시적으로 종속성을 선언한 리소스는 지정한 리소스보다 먼저 처리됩니다. 가능한 경우 Terraform은 병렬 처리를 구현하고 비종속 리소스를 동시에 처리할 수 있습니다. 배포하기 전에 terraform graph 명령을 사용하여 종속성 그래프를 볼 수 있습니다.

종속성 그래프가 생성된 후 Terraform은 배포 중에 수행해야 할 작업을 결정합니다. 종속성 그래프를 최신 상태 파일과 비교합니다. 이 프로세스의 결과를 계획이라고 하며 이는 CloudFormation 변경 세트와 매우 비슷합니다. terraform plan 명령을 사용하면 현재 계획을 볼 수 있습니다.

가장 좋은 방법은 표준 모듈 구조에 최대한 가깝게 유지하는 것이 좋습니다. 구성 파일이 너무 길어서 효율적으로 관리할 수 없고 논리적 분리가 관리를 단순화할 수 있는 경우 코드를 여러 파일에 분산할 수 있습니다. 스택을 최대한 효율적으로 실행하기 위해 종속성 그래프 및 계획 프로세스가 어떻게 작동하는지 염두에 두세요.

Terraform 상태 및 백엔드 이해

코드형 인프라(IaC)에서 가장 중요한 개념 중 하나는 상태 개념입니다. IaC 서비스는 상태를 유지하므로 배포할 때마다 리소스를 다시 생성하지 않고도 IaC 파일에 리소스를 선언할 수 있습니다. IaC 파일은 배포가 끝날 때 모든 리소스의 상태를 문서화하므로 다음 배포에서 선언된 대로 해당 상태를 대상 상태와 비교할 수 있습니다. 따라서 현재 상태에 라는 Amazon Simple Storage Service(Amazon S3) 버킷이 포함되어 `my-s3-bucket` 있고 수신되는 변경 사항에 동일한 버킷도 포함되어 있는 경우, 새 프로세스는 모든 새 버킷을 생성하려고 하지 않고 기존 버킷에 발견된 모든 변경 사항을 적용합니다.

다음 표에는 일반적인 IaC 상태 프로세스의 예가 나와 있습니다.

현재 상태	대상 상태	작업
이름이 인 S3 버킷 없음 `my-s3-bucket`	이름이 인 S3 버킷 `my-s3-bucket`	라는 S3 버킷 생성 `my-s3-bucket`
`my-s3-bucket` 버킷 버전 관리가 구성되지 않은 경우	`my-s3-bucket` 버킷 버전 관리가 구성되지 않은 경우	작업 없음
`my-s3-bucket` 버킷 버전 관리가 구성되지 않은 경우	`my-s3-bucket` 버킷 버전 관리가 구성된	버킷 버전 관리를 `my-s3-bucket` 사용하도록 구성
`my-s3-bucket` 버킷 버전 관리가 구성된	이름이 인 S3 버킷 없음 `my-s3-bucket`	삭제 시도 `my-s3-bucket`

AWS CloudFormation 및 Terraform 트랙 상태의 다양한 방법을 이해하려면 두 도구 간의 첫 번째 기본 차이점을 기억해야 합니다. CloudFormation은 내부에서 호스팅 AWS 클라우드되고 Terraform은 기본적으로 원격입니다. 이 사실을 통해 CloudFormation은 내부적으로 상태를 유지할 수 있습니다. CloudFormation 콘솔로 이동하여 지정된 스택의 이벤트 기록을 볼 수 있지만 CloudFormation 서비스 자체가 상태 규칙을 적용합니다.

지정된 리소스에 대해 CloudFormation이 작동하는 세 가지 모드는 `Create`, `Update`및 입니다`Delete`. 현재 모드는 마지막 배포에서 발생한 일을 기반으로 결정되며, 그렇지 않으면 영향을 받을 수 없습니다. 결정된 모드에 영향을 미치기 위해 CloudFormation 리소스를 수동으로 업데이트할 수 있지만 "이 리소스의 경우 `Create` 모드에서 운영"이라는 명령을 CloudFormation에 전달할 수 없습니다.

Terraform은에서 호스팅되지 않으므로 상태를 유지하는 AWS 클라우드프로세스를 더 구성할 수 있어야 합니다. 이러한 이유로 Terraform 상태는 자동으로 생성된 상태 파일 내에서 유지됩니다. Terraform

개발자는 CloudFormation보다 훨씬 더 직접적으로 상태를 처리해야 합니다. 기억해야 할 중요한 점은 추적 상태가 두 도구 모두에 동일하게 중요하다는 것입니다.

기본적으로 Terraform 상태 파일은 Terraform 스택을 실행하는 기본 디렉터리의 최상위에 로컬로 저장됩니다. 로컬 개발 환경에서 `terraform apply` 명령을 실행하면 Terraform이 실시간으로 상태를 유지하는 데 사용하는 terraform.tfstate 파일을 생성하는 것을 볼 수 있습니다. 더 좋거나 더 나쁘면 CloudFormation보다 Terraform의 상태를 훨씬 더 잘 제어할 수 있습니다. 상태 파일을 직접 업데이트해서는 안 되지만 배포 간에 상태를 업데이트하는 몇 가지 Terraform CLI 명령을 실행할 수 있습니다. 예를 들어, terraform 가져오기를 사용하면 Terraform 외부에서 생성된 리소스를 배포 스택에 추가할 수 있습니다. 반대로 terraform state rm을 실행하여 상태에서 리소스를 제거할 수 있습니다.

Terraform이 상태를 어딘가에 저장해야 한다는 사실은 CloudFormation에 적용되지 않는 또 다른 개념인 백엔드를 초래합니다. Terraform 백엔드는 배포 후 Terraform 스택이 상태 파일을 저장하는 곳입니다. 새 배포가 시작될 때 상태 파일을 찾을 것으로 예상되는 위치이기도 합니다. 위에서 설명한 대로 로컬에서 스택을 실행할 때 최상위 로컬 디렉터리에 Terraform 상태 사본을 보관할 수 있습니다. 이를 로컬 백엔드라고 합니다.

지속적 통합 및 지속적 배포(CI/CD) 환경을 위해 개발할 때 로컬 상태 파일은 일반적으로 버전 제어에서 벗어나도록 .gitignore 파일에 포함됩니다. 그러면 파이프라인 내에 로컬 상태 파일이 없습니다. 제대로 작동하려면 파이프라인 단계가 어딘가에서 올바른 상태 파일을 찾아야 합니다. 이러한 이유로 Terraform 구성 파일에는 종종 백엔드 블록이 포함됩니다. 백엔드 블록은 Terraform 스택에 상태 파일을 찾기 위해 자체 최상위 디렉터리 이외의 위치를 찾아야 함을 나타냅니다.

Terraform 백엔드는 Amazon S3 버킷, API 엔드포인트 또는 원격 Terraform 워크스페이스 등 거의 모든 곳에 위치할 수 있습니다. 다음은 Amazon S3 버킷에 저장된 Terraform 백엔드의 예입니다.

```
terraform {
  backend "s3" {
    bucket = "my-s3-bucket"
    key    = "state-file-folder"
    region = "us-east-1"
  }
}
```

Terraform 구성 파일 내에 민감한 정보가 저장되지 않도록 백엔드는 부분 구성도 지원합니다. 이전 예제에서는 버킷에 액세스하는 데 필요한 자격 증명이 구성에 없습니다. 자격 증명은 환경 변수 또는와 같은 다른 수단을 사용하여 얻을 수 있습니다 AWS Secrets Manager. 자세한 내용은 AWS Secrets Manager 및 HashiCorp Terraform을 사용하여 민감한 데이터 보안을 참조하세요.

일반적인 백엔드 시나리오는 로컬 환경에서 테스트 목적으로 사용되는 로컬 백엔드입니다. terraform.tfstate 파일은 원격 리포지토리로 푸시되지 않도록 .gitignore 파일에 포함됩니다. 그런 다음 CI/CD 파이프라인 내의 각 환경은 자체 백엔드를 유지합니다. 이 시나리오에서는 여러 개발자가이 원격 상태에 액세스할 수 있으므로 상태 파일의 무결성을 보호해야 합니다. 여러 배포가 동시에 실행되고 상태를 업데이트하는 경우 상태 파일이 손상될 수 있습니다. 따라서 로컬이 아닌 백엔드가 있는 상황에서는 일반적으로 배포 중에 상태 파일이 잠깁니다.

테라폼 데이터 소스 이해

배포 스택이 기존 리소스의 데이터에 의존하는 것은 매우 일반적입니다. 대부분의 IaC 도구에는 다른 프로세스에서 만든 리소스를 가져오는 방법이 있습니다. 이렇게 가져온 리소스는 대개 읽기 전용이며 (IAM 역할은 예외임) 스택 내 리소스에 필요한 데이터에 액세스하는 데 사용됩니다. AWS CloudFormation 리소스를 가져올 수 있지만, 를 보면 이 아이디어를 더 잘 설명할 수 있습니다. AWS 클라우드 개발 키트 (AWS CDK)

개발자가 기존 프로그래밍 언어를 사용하여 CloudFormation 템플릿을 생성하는 AWS CDK 데 도움이 됩니다. AWS CDK 작업의 최종 결과는 가져온 리소스입니다 CloudFormation. 그러나 와 함께 사용되는 구문을 AWS CDK 사용하면 Terraform과 더 쉽게 비교할 수 있습니다. 다음은 를 사용하여 리소스를 가져오는 예제입니다. AWS CDK

```
const importedBucket: IBucket = Bucket.fromBucketAttributes(
    scope,
    "imported-bucket",
    {
        bucketName: "My_S3_Bucket"
    }
);
```

가져온 리소스는 일반적으로 같은 종류의 새 리소스를 만들 때 사용하는 것과 동일한 클래스에서 정적 메서드를 호출하여 만들어집니다. 를 `new Bucket(...` 호출하면 새 리소스가 생성되고, 호출하면 기존 리소스를 `Bucket.fromBucketAttributes(...` 가져옵니다. 올바른 버킷을 찾을 AWS CDK 수 있도록 버킷 속성의 하위 집합을 함수에 전달합니다. 하지만 또 다른 차이점은 새 버킷을 만들면 모든 속성과 메서드를 사용할 수 있는 `Bucket` 클래스의 전체 인스턴스가 반환된다는 것입니다. 리소스를 가져오면 `Bucket` 반드시 있어야 하는 속성만 포함하는 `IBucket` 유형인 an이 반환됩니다. 외부 스택에서 리소스를 가져올 수는 있지만 리소스로 수행할 수 있는 작업은 제한적입니다.

Terraform에서는 데이터 소스를 사용하여 유사한 목표를 달성합니다. 대부분의 정의된 Terraform 리소스에는 함께 사용할 수 있는 데이터 소스가 함께 제공됩니다. 다음은 Terraform S3 버킷 리소스와 해당 데이터 소스의 예입니다.

```
# S3 Bucket resource:
resource "aws_s3_bucket" "My_S3_Bucket" {
  bucket = "My_S3_Bucket"
}

# S3 Bucket data source:
```

```
data "aws_s3_bucket" "My_S3_Bucket" {
  bucket = "My_S3_Bucket"
}
```

이 두 항목의 유일한 차이점은 이름 접두사입니다. 데이터 원본 설명서에서 볼 수 있듯이 데이터 원본에 전달할 수 있는 매개 변수는 리소스보다 적습니다. 이는 리소스가 이러한 파라미터를 사용하여 새 S3 버킷의 모든 속성을 선언하는 반면, 데이터 원본에는 기존 리소스의 데이터를 고유하게 식별하고 가져오기에 충분한 정보만 필요하기 때문입니다.

Terraform 리소스와 데이터 소스 구문 간의 유사성은 편리할 수 있지만 문제가 될 수도 있습니다. 초보 Terraform 개발자는 구성에서 실수로 리소스 대신 데이터 소스를 사용하는 경우가 많습니다. Terraform 데이터 소스는 항상 읽기 전용입니다. 읽기 작업 (예: 다른 리소스에 ID 이름 제공) 에 해당 리소스 대신 사용할 수 있습니다. 하지만 기본 리소스의 일부 측면을 근본적으로 변경하는 쓰기 작업에는 사용할 수 없습니다. 이러한 이유로 Terraform 데이터 소스는 기본 리소스의 복제된 버전이라고 생각할 수 있습니다.

이전 AWS CDK iBucket 예제와 마찬가지로 데이터 소스는 읽기 전용 시나리오에 유용합니다. 기존 리소스에서 데이터를 가져와야 하지만 해당 리소스를 스택 내에 유지할 필요가 없는 경우 데이터 소스를 사용하십시오. 계정의 기본 VPC를 사용하는 Amazon EC2 인스턴스를 생성하는 경우를 좋은 예로 들 수 있습니다. VPC는 이미 존재하므로 데이터를 가져오기만 하면 됩니다. 다음 코드 샘플은 데이터를 사용하여 대상 VPC를 식별하는 방법을 보여줍니다.

```
data "aws_vpc" "default" {
  default = true
}

resource "aws_instance" "instance1" {
  ami           = "ami-123456"
  instance_type = "t2.micro"
  subnet_id     = data.aws_vpc.default.main_route_table_id
}
```

테라폼 변수, 로컬 값 및 출력에 대한 이해

변수는 코드 블록 내에 자리 표시자를 허용하여 코드 유연성을 향상시킵니다. 코드가 재사용될 때마다 변수가 다른 값을 나타낼 수 있습니다. Terraform은 모듈식 범위로 변수 유형을 구분합니다. 입력 변수는 모듈에 삽입할 수 있는 외부 값이고, 출력 값은 외부에서 공유할 수 있는 내부 값이며, 로컬 값은 항상 원래 범위 내에 있습니다.

Variables

AWS CloudFormation 매개 변수를 사용하여 한 스택 배포에서 다음 스택 배포로 설정 및 재설정할 수 있는 사용자 지정 값을 나타냅니다. 마찬가지로 Terraform은 입력 변수 또는 변수를 사용합니다. 변수는 Terraform 구성 파일의 어느 곳에서나 선언할 수 있으며 일반적으로 필수 데이터 유형 또는 기본값으로 선언됩니다. 다음 세 표현식은 모두 유효한 Terraform 변수 선언입니다.

```
variable "thing_i_made_up" {
  type = string
}

variable "random_number" {
  default = 5
}

variable "dogs" {
  type = list(object({
    name  = string
    breed = string
  }))

  default = [
    {
      name  = "Sparky",
      breed = "poodle"
    }
  ]
}
```

구성 내에서 Sparky의 품종에 액세스하려면 변수를 사용합니다. `var.dogs[0].breed` 변수에 기본값이 없고 nullable 변수로 분류되지 않은 경우 각 배포마다 변수 값을 설정해야 합니다. 그렇지 않으면 변수에 새 값을 설정하는 것은 선택 사항입니다. 루트 모듈에서는 명령줄, 환경 변수 또는

terraform.tfvars 파일에서 현재 변수 값을 설정할 수 있습니다. 다음 예제는 모듈의 최상위 디렉토리에 저장되어 있는 terraform.tfvars 파일에 변수 값을 입력하는 방법을 보여줍니다.

```
# terraform.tfvars
dogs = [
   {
      name  = "Sparky",
      breed = "poodle"
   },
   {
      name  = "Fluffy",
      breed = "chihuahua"
   }
]

random_number = 7

thing_i_made_up = "Kabibble"
```

이 예제에서 terraform.tfvars 파일의 값은 변수 dogs 선언의 기본값을 재정의합니다. 자식 모듈 내에서 변수를 선언하는 경우 다음 예제와 같이 모듈 선언 블록 내에서 직접 변수 값을 설정할 수 있습니다.

```
module "my_custom_module" {
  source        = "modulesource/custom"
  version       = "0.0.1"
  random_number = 8
}
```

변수를 선언할 때 사용할 수 있는 다른 인수에는 다음이 포함됩니다.

- `sensitive`— Terraform 프로세스 출력에 변수 값이 노출되지 `true` 않도록 설정합니다.
- `nullable`— 이 값을 로 `true` 설정하면 변수에 값이 없을 수 있습니다. 이는 기본값이 설정되지 않은 변수에 편리합니다.
- `description`— 스택의 메타데이터에 변수 설명을 추가합니다.
- `validation`— 변수에 대한 검증 규칙을 설정합니다.

Terraform 변수의 가장 편리한 기능 중 하나는 변수 선언 내에 하나 이상의 유효성 검사 개체를 추가할 수 있다는 것입니다. 유효성 검사 개체를 사용하여 변수가 통과해야 하는 조건을 추가할 수 있습니다.

그렇지 않으면 배포가 실패합니다. 조건을 위반할 때마다 표시되도록 사용자 지정 오류 메시지를 설정할 수도 있습니다.

예를 들어 팀 구성원이 실행할 Terraform 구성 파일을 설정하는 경우를 예로 들 수 있습니다. 스택을 배포하기 전에 팀 구성원은 terraform.tfvars 파일을 만들어 중요한 구성 값을 설정해야 합니다. 이를 상기시키기 위해 다음과 같이 할 수 있습니다.

```
variable "important_config_setting" {
  type = string

  validation {
    condition     = length(var.important_config_setting) > 0
    error_message = "Don't forget to create the terraform.tfvars file!"
  }

  validation {
    condition     = substr(var.important_config_setting, 0, 7) == "prefix-"
    error_message = "Remember that the value always needs to start with 'prefix-'"
  }
}
```

이 예제에서 볼 수 있듯이 단일 변수 내에 여러 조건을 설정할 수 있습니다. Terraform은 실패한 조건에 대한 오류 메시지만 표시합니다. 이러한 방식으로 변수 값에 모든 종류의 규칙을 적용할 수 있습니다. 변수 값으로 인해 파이프라인 장애가 발생하는 경우 그 이유를 정확히 알 수 있습니다.

로컬 값

모듈 내에 별칭을 지정하려는 값이 있는 경우 절대 업데이트되지 않는 기본 변수를 선언하는 대신 `locals` 키워드를 사용하십시오. 이름에서 알 수 있듯이 `locals` 블록에는 내부적으로 해당 특정 모듈로 범위가 지정된 용어가 포함됩니다. 리소스 이름에 사용할 변수 값에 접두사를 추가하는 등 문자열 값을 변환하려는 경우에는 로컬 값을 사용하는 것이 좋습니다. 다음 예제와 같이 단일 `locals` 블록으로 모듈의 모든 로컬 값을 선언할 수 있습니다.

```
locals {
  moduleName    = "My Module"
  localConfigId = concat("prefix-", var.important_config_setting)
}
```

단, 값에 접근할 때 `locals` 키워드는 다음과 같이 단수형이 된다는 점을 기억하세요. `local.LocalConfigId`

출력 값

Terraform 입력 변수가 CloudFormation 매개 변수와 같으면 Terraform 출력 값이 출력과 같다고 말할 수 있습니다. CloudFormation 둘 다 배포 스택 내에서 값을 노출하는 데 사용됩니다. 그러나 Terraform 모듈은 도구 구조에 더 깊이 뿌리내리고 있기 때문에 Terraform 출력 값은 모듈 내의 값을 상위 모듈이나 다른 하위 모듈에 노출하는 데에도 사용됩니다. 이는 해당 모듈이 모두 동일한 배포 스택 내에 있더라도 마찬가지입니다. 두 개의 사용자 지정 모듈을 빌드하고 있고 첫 번째 모듈이 두 번째 모듈의 ID 값에 액세스해야 하는 경우 두 번째 모듈에 다음 블록을 추가해야 합니다. `output`

```
output "module_id" {
  value = local.module_id
}
Then in the first module you could use it like this:
module "first_module" {
  source = "path/to/first/module"
}

resource "example_resource" "example_resource_name" {
  module_id = module.first_module.module_id
}
```

Terraform 출력 값은 동일한 스택 내에서 사용할 수 있으므로 `output` 블록의 `sensitive` 속성을 사용하여 스택 출력에 값이 표시되지 않도록 할 수도 있습니다. 또한 변수가 `precondition` 블록을 사용하는 것과 같은 방식으로 블록도 블록을 사용할 수 있습니다. 즉, 변수가 특정 규칙 세트를 따르도록 하기 위해서입니다. `output` `validation` 이렇게 하면 배포를 진행하기 전에 모듈 내의 모든 값이 예상대로 존재하는지 확인할 수 있습니다.

```
output "important_config_setting" {
  value = var.important_config_setting

  precondition {
    condition     = length(var.important_config_setting) > 0
    error_message = "You forgot to create the terraform.tfvars file again."
  }
}
```

Terraform 함수, 표현식 및 메타 인수 이해

일반적인 프로그래밍 언어가 아닌 선언적 구성 파일을 사용하는 IaC 도구에 대한 한 가지 비판은 사용자 지정 프로그래밍 로직을 구현하기가 더 어렵다는 것입니다. Terraform 구성에서이 문제는 함수, 표현식 및 메타 인수를 사용하여 해결됩니다.

함수

코드를 사용하여 인프라를 프로비저닝할 때의 큰 이점 중 하나는 공통 워크플로를 저장하고 반복적으로 재사용하여 매번 다른 인수를 전달하는 기능입니다. Terraform 함수는 AWS CloudFormation 내장 함수와 유사하지만 구문은 함수가 프로그래밍 방식으로 호출되는 방식과 더 유사합니다. 이 가이드의 예제에서 하위 문자열, concat,length 및 base64decode와 같은 일부 Terraform 함수를 이미 발견했을 수 있습니다. 내장 함수가 있는 CloudFormation과 마찬가지로 Terraform에는 구성에 사용할 수 있는 일련의 내장 함수가 있습니다. 예를 들어 특정 리소스 속성이 파일에 직접 붙여넣는 데 비효율적인 매우 큰 JSON 객체를 사용하는 경우 객체를 .json 파일에 넣고 Terraform 함수를 사용하여 액세스할 수 있습니다. 다음 예제에서 `file` 함수는 파일의 내용을 문자열 형식으로 반환한 다음 `jsondecode` 이를 객체 유형으로 변환합니다.

```
resource "example_resource" "example_resource_name" {
  json_object = jsondecode(file("/path/to/file.json"))
}
```

Expressions

또한 Terraform은 보다 전통적인 삼원 연산자 구문을 사용한다는 점을 제외하면 CloudFormation `condition` 함수와 유사한 조건식도 허용합니다. 다음 예제에서는 두 표현식이 정확히 동일한 결과를 반환합니다. 두 번째 예는 Terraform이 스플랫 표현식을 호출하는 것입니다. 별표로 인해 Terraform은 각 항목의 `id` 속성만 사용하여 목록을 반복하고 새 목록을 생성합니다.

```
resource "example_resource" "example_resource_name" {
  boolean_value  = var.value ? true : false
  numeric_value  = var.value > 0 ? 1 : 0
  string_value   = var.value == "change_me" ? "New value" : var.value
  string_value_2 = var.value != "change_me" ? var.value : "New value"
}
There are two ways to express for loops in a Terraform configuration:
resource "example_resource" "example_resource_name" {
```

```
  list_value   = [for object in var.ids : object.id]
  list_value_2 = var.ids[*].id
}
```

메타 인수

이전 코드 예제에서 `list_value` 및 `list_value_2`를 인수라고 합니다. 이러한 메타 인수 중 일부에 이미 익숙할 수 있습니다. 또한 Terraform에는 인수처럼 작동하지만 몇 가지 추가 기능이 있는 몇 가지 메타 인수가 있습니다.

- 메타 인수의 depends_on은 CloudFormation DependsOn 속성과 매우 유사합니다.
- 공급자 메타 인수를 사용하면 여러 공급자 구성을 한 번에 사용할 수 있습니다.
- 수명 주기 메타 인수를 사용하면 CloudFormation의 제거 및 삭제 정책과 유사한 리소스 설정을 사용자 지정할 수 있습니다.

다른 메타 인수를 사용하면 함수 및 표현식 기능을 리소스에 직접 추가할 수 있습니다. 예를 들어 개수 메타 인수는 여러 유사한 리소스를 동시에 생성하는 데 유용한 메커니즘입니다. 다음 예제에서는 `count`메타 인수를 사용하지 않고 두 개의 Amazon Elastic Container Service(Amazon EKS) 클러스터를 생성하는 방법을 보여줍니다.

```
resource "aws_eks_cluster" "example_0" {
  name     = "example_0"
  role_arn = aws_iam_role.cluster_role.arn
  vpc_config {
    endpoint_private_access = true
    endpoint_public_access  = true
    subnet_ids              = var.subnet_ids[0]
  }
}

resource "aws_eks_cluster" "example_1" {
  name     = "example_1"
  role_arn = aws_iam_role.cluster_role.arn
  vpc_config {
    endpoint_private_access = true
    endpoint_public_access  = true
    subnet_ids              = var.subnet_ids[1]
  }
}
```

다음 예제에서는 count메타 인수를 사용하여 두 개의 Amazon EKS 클러스터를 생성하는 방법을 보여줍니다.

```
resource "aws_eks_cluster" "clusters" {
  count    = 2
  name     = "cluster_${count.index}"
  role_arn = aws_iam_role.cluster_role.arn
  vpc_config {
    endpoint_private_access = true
    endpoint_public_access  = true
    subnet_ids              = var.subnet_ids[count.index]
  }
}
```

각 단위 이름을 지정하려면의 리소스 블록 내에서 목록 인덱스에 액세스할 수 있습니다count.index. 하지만 좀 더 복잡한 유사한 리소스를 여러 개 생성하려면 어떻게 해야 할까요? 여기에서 for_each meta-argument가 들어옵니다. for_each 메타 인수는 숫자 대신 목록이나 객체를 전달하는 점을 count제외하면와 매우 유사합니다. Terraform은 목록 또는 객체의 각 멤버에 대해 새 리소스를 생성합니다. 루프 인덱스가 아닌 목록의 내용에 액세스할 수 있다는 count = length(list)점을 제외하면를 설정하는 경우와 유사합니다.

이는 항목 목록 또는 단일 객체 모두에 적용됩니다. 다음 예제에서는 IDid-1로 id-0 및가 있는 두 개의 리소스를 생성합니다 IDs.

```
variable "ids" {
  default = [
    { id = "id-0" },
    { id = "id-1" },
  ]
}

resource "example_resource" "example_resource_name" {
  # If your list fails, you might have to call "toset" on it to convert it to a set
  for_each = toset(var.ids)
  id       = each.value
}
```

다음 예제에서는 Sparky용 리소스 1개와 chihuahua용 리소스 1개도 생성합니다.

```
variable "dogs" {
  default = {
```

```
    poodle    = "Sparky"
    chihuahua = "Fluffy"
  }
}

resource "example_resource" "example_resource_name" {
  for_each = var.dogs
  breed    = each.key
  name     = each.value
}
```

count.index를 사용하여 개수의 루프 인덱스에 액세스할 수 있는 것과 마찬가지로 각 객체를 사용하여 for_each 루프에 있는 각 항목의 키와 값에 액세스할 수 있습니다. for_each는 목록과 객체를 모두 반복하기 때문에 각 키와 값은 추적하기가 약간 혼란스러울 수 있습니다. 다음 표에는 for_each meta-argument를 사용할 수 있는 다양한 방법과 각 반복 시 값을 참조하는 방법이 나와 있습니다.

예제	**for_each** 유형	첫 번째 반복	두 번째 반복
A	`["poodle", "chihuahua"]`	`each.key = "poodle"` `each.value = null`	`each.key = "chihuahua"` `each.value = null`

B	`[`
	`{`
	`type = "poodle",`
	`name = "Sparky"`
	`},`
	`{`
	`type = "chihuahua",`
	`name = "Fluffy"`
		`each.key = {`
		`type = "poodle",`
		`name = "Sparky"`
		`}`
		`each.value = null`
			`each.key = {`
			`type = "chihuahua",`
			`name = "Fluffy"`
			`}`
			`each.value = null`

예제	**for_each** 유형	첫 번째 반복	두 번째 반복
	}]		

C	{
	
	poodle =
	"Sparky",
	
	chihuahua =
	"Fluffy"
	
	}
		each.key =
		"poodle"
		
		each.value =
		"Sparky"
			each.key =
			"chihuahua"
			
			each.value =
			"Fluffy"

D	{
	
	dogs = {
	
	poodle =
	"Sparky",
	
	chihuahua =
	"Fluffy"
	
	},
	
	cats = {
	
	persian =
	"Felix",
	
	burmese =
	"Morris"
	
	}
	
	}
		each.key = "dogs"
		
		each.value = {
		
		poodle =
		"Sparky",
		
		chihuahua =
		"Fluffy"
		
		}
			each.key = "cats"
			
			each.value = {
			
			persian =
			"Felix",
			
			burmese =
			"Morris"
			
			}

예제	**for_each** 유형	첫 번째 반복	두 번째 반복

E	{
	
	dogs = [
	
	{
	
	type = "poodle",
	
	name = "Sparky"
	
	},
	
	{
	
	type = "chihuahua",
	
	name = "Fluffy"
	
	}
	
	],
	
	cats = [
	
	{
	
	type = "persian",
	
	name = "Felix"
	
	},
	
	{
	
	type = "burmese",
	
	name = "Morris"
		each.key = "dogs"
		
		each.value = [
		
		{
		
		type = "poodle",
		
		name = "Sparky"
		
		},
		
		{
		
		type = "chihuahua",
		
		name = "Fluffy"
		
		}
		
		]
			each.key = "cats"
			
			each.value = [
			
			{
			
			type = "persian",
			
			name = "Felix"
			
			},
			
			{
			
			type = "burmese",
			
			name = "Morris"
			
			}
			
			]

예제	**for_each** 유형	첫 번째 반복	두 번째 반복
	}] }		

따라서 var.animals가 E행과 같으면 다음 코드를 사용하여 동물당 하나의 리소스를 생성할 수 있습니다.

```
resource "example_resource" "example_resource_name" {
  for_each = var.animals
  type     = each.key
  breeds   = each.value[*].type
  names    = each.value[*].name
}
```

또는 다음 코드를 사용하여 동물당 두 개의 리소스를 생성할 수 있습니다.

```
resource "example_resource" "example_resource_name" {
  for_each = var.animals.dogs
  type     = "dogs"
  breeds   = each.value.type
  names    = each.value.name
}

resource "example_resource" "example_resource_name" {
  for_each = var.animals.cats
  type     = "cats"
  breeds   = each.value.type
  names    = each.value.name
}
```

FAQ

언제 대신 Terraform을 사용해야 하나요? CloudFormation

일반적으로 워크로드가 주로 기반인 경우 Terraform이 따라올 수 없는 수준의 기본 지원을 AWS CloudFormation 제공합니다. AWS하지만 워크로드에 타사 프로세스가 상당히 많이 포함되어 있거나 여러 클라우드 제공업체에 분산되어 있는 경우 Terraform을 고려해 볼 수 있는 도구입니다.

대신 언제 사용해야 하나요? AWS CDK CloudFormation

를 AWS 클라우드 개발 키트 (AWS CDK)사용하면 당신도 함께 사용하고 CloudFormation 있습니다. AWS CDK 이를 통해 공통 프로그래밍 언어를 사용하여 CloudFormation 템플릿을 생성할 수 있습니다. AWS CDK 지원하는 프로그래밍 언어에 익숙하다면 CloudFormation 템플릿을 생성하는 데 필요한 시간을 줄일 AWS CDK 수 있습니다.

Terraform 구성을 AWS CDK 생성하는 것과 같은 도구가 있습니까?

와 비교하여 CDK for Terraform (CDKTF) 은 동일한 구성 라이브러리를 사용하여 리소스를 프로비저닝하고 동일한 jsii 엔진을 사용하여 여러 프로그래밍 언어를 지원합니다. AWS CDK템플릿을 생성할 때와 동일한 방식으로 Terraform 구성을 생성하는 데 사용할 수 있습니다. AWS CDK CloudFormation

Terraform에 대해 자세히 알아보려면 어떻게 해야 하나요?

고급 테라폼 개념에 대한 자세한 내용은 Terraform 설명서를 참조하십시오. 또한 모든 주요 제공업체 및 오픈 소스 모듈의 구성 요소에 대해서도 설명합니다.

관련 리소스

AWS 설명서

- AWS CDK 설명서
- AWS CloudFormation 설명서
- 테라폼: 비욘드 더 베이직 위드 AWS (AWS 블로그 포스트)

기타 리소스

- 테라폼용 CDK 문서
- Terraform 설명서

부록: 테라폼 속성 액세스 예제

Resource

```
resource "aws_s3_bucket" "myS3Bucket" {
     bucket = "my-s3-bucket"
}

bucketName = aws_s3_bucket.myS3Bucket.bucket
```

데이터 소스

```
data "aws_s3_bucket" "myS3Bucket" {
     bucket = "my-s3-bucket"
}

bucketName = data.aws_s3_bucket.myS3Bucket.bucket
```

모듈

```
module "eks" {
    source = "terraform-aws-modules/eks/aws"
    version = "20.2.1"
}

vpc_id = module.eks.vpc_id
```

변수

```
variable "my_variable" = {
   default = "dog"
}

animalType = var.my_variable
```

로컬

```
locals {
  type = "dog"
}

animalType = local.type
```

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2024년 3월 29일

AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

숫자

7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 버전으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예:에서 온프레미스 Oracle 데이터베이스를 Oracle용 Amazon Relational Database Service(RDS)로 마이그레이션합니다 AWS 클라우드.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예:의 EC2 인스턴스에서 온프레미스 Oracle 데이터베이스를 Oracle로 마이그레이션합니다 AWS 클라우드.
- 재배치(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: Microsoft Hyper-V 애플리케이션을 로 마이그레이션합니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중으로 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

A

ABAC

속성 기반 액세스 제어를 참조하세요.

추상화된 서비스

관리형 서비스를 참조하세요.

ACID

원자성, 일관성, 격리, 내구성을 참조하세요.

능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. 더 유연하지만 액티브-패시브 마이그레이션보다 더 많은 작업이 필요합니다.

능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 데이터가 대상 데이터베이스에 복제되는 동안 소스 데이터베이스만 애플리케이션 연결의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

집계 함수

행 그룹에서 작동하고 그룹에 대한 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로는 `SUM` 및가 있습니다`MAX`.

AI

인공 지능을 참조하세요.

AIOps

인공 지능 작업을 참조하세요.

익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

애플리케이션 제어

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용할 수 있는 보안 접근 방식입니다.

애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 포트폴리오 검색 및 분석 프로세스의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 What is Artificial Intelligence?를 참조하십시오.

인공 지능 운영(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AWS 마이그레이션 전략에서 AIOps가 사용되는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

원자성, 일관성, 격리성, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

ABAC(속성 기반 액세스 제어)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management (IAM) 설명서의 용 ABAC AWS를 참조하세요.

신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

가용 영역

다른 가용 영역의 장애로부터 격리 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내의 고유한 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환 AWS 하기 위한 효율적이고 효과적인 계획을 개발하는 데 도움이 되는의 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이러한 관점에서 AWS CAF는 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 AWS CAF 웹 사이트와 AWS CAF 백서를 참조하십시오.

AWS 워크로드 검증 프레임워크(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 권장하고, 작업 견적을 제공하는 도구입니다. AWS WQF는 AWS Schema Conversion Tool (AWS SCT)에 포함되어 있습니다. 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

B

잘못된 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

BCP

비즈니스 연속성 계획을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 Data in a behavior graph를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. Endianness도 참조하세요.

바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 “이 이메일이 스팸인가요, 스팸이 아닌가요?”, '이 제품은 책인가요, 자동차인가요?' 등의 문제를 예측해야 할 수 있습니다.

블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

블루/그린(Blue/Green) 배포

두 개의 별개이지만 동일한 환경을 생성하는 배포 전략입니다. 현재 애플리케이션 버전은 한 환경(파란색)에서 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 빠르게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 작업을 실행하고 인적 활동 또는 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같은 일부 봇은 유용하거나 유용합니다. 잘못된 봇이라고 하는 일부 다른 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 것입니다.

봇넷

맬웨어에 감염되고 봇 셰이더 또는 봇 운영자라고 하는 단일 당사자에 의해 제어되는 봇 네트워크입니다. Botnet은 봇과 봇의 영향을 확장하는 가장 잘 알려진 메커니즘입니다.

브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 About branches(GitHub 설명서)를 참조하십시오.

브레이크 글래스 액세스

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 Well-Architected 지침의 깨진 절차 구현 표시기를 AWS 참조하세요.

브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

C

CAF

AWS 클라우드 채택 프레임워크를 참조하세요.

canary 배포

최종 사용자에게 버전의 느린 증분 릴리스입니다. 확신이 드는 경우 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

Cloud Center of Excellence를 참조하세요.

CDC

변경 데이터 캡처를 참조하세요.

변경 데이터 캡처(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 내용을 감사하거나 복제하여 동기화를 유지하는 등의 다양한 용도로 CDC를 사용할 수 있습니다.

카오스 엔지니어링

시스템의 복원력을 테스트하기 위해 의도적으로 장애 또는 중단 이벤트를 도입합니다. AWS Fault Injection Service (AWS FIS)를 사용하여 AWS 워크로드에 스트레스를 주고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전달을 참조하세요.

분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

클라이언트측 암호화

대상이 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 암호화합니다.

클라우드 혁신 센터(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 CCoE 게시물을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 엣지 컴퓨팅 기술과 연결됩니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 클라우드 운영 모델 구축을 참조하십시오.

클라우드 채택 단계

조직이 로 마이그레이션할 때 일반적으로 거치는 4단계: AWS 클라우드

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 기반 – 클라우드 채택 확장을 위한 기초 투자(예: 랜딩 존 생성, CCoE 정의, 운영 모델 구축)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 블로그 게시물 The Journey Toward Cloud-First and the Stages of Adoption on the AWS 클라우드 Enterprise Strategy 블로그에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 마이그레이션 준비 가이드를 참조하세요.

CMDB

구성 관리 데이터베이스를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리에는 GitHub 또는가 포함됩니다Bitbucket Cloud. 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

컴퓨터 비전(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 AI 필드입니다. 예를 들어 Amazon SageMaker AI는 CV에 대한 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상 상태에서 변경됩니다. 이로 인해 워크로드가 규정을 준수하지 않을 수 있으며 일반적으로 점진적이고 의도하지 않은 것입니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 검색 및 분석 단계에서 CMDB의 데이터를 사용합니다.

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다. YAML 템플릿을 사용하여 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 적합성 팩을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 지속적 전달의 이점을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 참조하십시오.

CV

컴퓨터 비전을 참조하세요.

D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework에서 보안 원칙의 구성 요소입니다. 자세한 내용은 데이터 분류를 참조하십시오.

데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

데이터 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 분산된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 개인 정보 보호 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 데이터 경계 구축을 참조하세요 AWS.

데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

데이터 주체

데이터를 수집 및 처리하는 개인입니다.

데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템입니다. 데이터 웨어하우스에는 일반적으로 많은 양의 기록 데이터가 포함되며 일반적으로 쿼리 및 분석에 사용됩니다.

데이터 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

DDL

데이터베이스 정의 언어를 참조하세요.

딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

심층 방어

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 이 전략을 채택하면 AWS Organizations 구조의 여러 계층에 여러 컨트롤을 AWS추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고 합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 AWS Organizations와 함께 사용할 수 있는 AWS 서비스를 참조하십시오.

배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

개발 환경

환경을 참조하세요.

탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Detective controls를 참조하십시오.

개발 가치 흐름 매핑 (DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM은 원래 린 제조 방식을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

차원 테이블

스타 스키마에서는 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블입니다. 차원 테이블 속성은 일반적으로 텍스트 필드 또는 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 일반적으로 쿼리 제약, 필터링 및 결과 집합 레이블 지정에 사용됩니다.

재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

재해 복구(DR)

재해로 인한 가동 중지 시간과 데이터 손실을 최소화하는 데 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 Disaster Recovery of Workloads on AWS: Recovery in the Cloud를 참조하세요.

DML

데이터베이스 조작 언어를 참조하세요.

도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. Strangler Fig 패턴과 함께 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

DR

재해 복구를 참조하세요.

드리프트 감지

기준 구성과의 편차 추적. 예를 들어 AWS CloudFormation 를 사용하여 시스템 리소스의 드리프트를 감지하거나를 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 랜딩 존의 변경 사항을 감지할 수 있습니다.

DVSM

개발 값 스트림 매핑을 참조하세요.

E

EDA

탐색 데이터 분석을 참조하세요.

EDI

전자 데이터 교환을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 클라우드 컴퓨팅과 비교할 때 엣지 컴퓨팅은 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간의 비즈니스 문서 자동 교환. 자세한 내용은 전자 데이터 교환이란 무엇입니까?를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이퍼텍스트로 변환하는 컴퓨팅 프로세스입니다.

암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

엔드포인트

서비스 엔드포인트를 참조하세요.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 엔드포인트 서비스 생성을 참조하십시오.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, MES, 프로젝트 관리)를 자동화하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 봉투 암호화를 참조하세요.

환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어, AWS CAF 보안 에픽에는 ID 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획을 참조하세요.

탐색 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

F

팩트 테이블

별표 스키마의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블에는 측정값이 포함된 열과 차원 테이블에 대한 외래 키가 포함된 열의 두 가지 유형이 포함됩니다.

빠른 실패

자주 증분 테스트를 사용하여 개발 수명 주기를 줄이는 철학입니다. 애자일 접근 방식의 중요한 부분입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 컨트롤 플레인 또는 데이터 플레인과 같은 AWS 클라우드경계입니다. 자세한 내용은 AWS 장애 격리 경계를 참조하세요.

기능 브랜치

브랜치를 참조하세요.

기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 SHAP(Shapley Additive Descriptions) 및 통합 그레디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용

할 수 있습니다. 예를 들어, 날짜 '2021-05-27 00:15:37'을 '2021년', '5월', '목', '15일'로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

몇 장의 샷 프롬프트

유사한 작업을 수행하도록 요청하기 전에 LLM에 작업과 원하는 출력을 보여주는 몇 가지 예제를 제공합니다. 이 기법은 컨텍스트 내 학습을 적용하여 모델이 프롬프트에 포함된 예제(샷)에서 학습합니다. 퓨샷 프롬프트는 특정 형식 지정, 추론 또는 도메인 지식이 필요한 작업에 효과적일 수 있습니다. 제로샷 프롬프트도 참조하세요.

FGAC

세분화된 액세스 제어를 참조하세요.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 변경 데이터 캡처를 통해 연속 데이터 복제를 사용하여 최대한 짧은 시간 내에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

파운데이션 모델을 참조하세요.

파운데이션 모델(FM)

일반화 및 레이블 지정되지 않은 데이터의 대규모 데이터 세트에 대해 훈련된 대규모 딥 러닝 신경망입니다. FMs은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 작업을 수행할 수 있습니다. 자세한 내용은 파운데이션 모델이란 무엇입니까?를 참조하세요.

G

생성형 AI

대량의 데이터에 대해 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트 및 오디오와 같은 새로운 콘텐츠 및 아티팩트를 생성할 수 있는 AI 모델의 하위 집합입니다. 자세한 내용은 생성형 AI란 무엇입니까?를 참조하세요.

지리적 차단

지리적 제한을 참조하세요.

지리적 제한(지리적 차단)

Amazon CloudFront에서 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하십시오.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 트렁크 기반 워크플로는 현대적이고 선호하는 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조업에서는 골든 이미지를 사용하여 여러 디바이스에 소프트웨어를 프로비저닝할 수 있으며 디바이스 제조 작업의 속도, 확장성 및 생산성을 개선하는 데 도움이 됩니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 브라운필드라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이는 AWS Config Amazon GuardDuty AWS Security Hub, , AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

H

HA

고가용성을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스

키마를 변환하는 것은 복잡한 작업일 수 있습니다.AWS 는 스키마 변환에 도움이 되는 AWS SCT를 제공합니다.

높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

홀드아웃 데이터

기계 학습 모델을 훈련하는 데 사용되는 데이터 세트에서 보류된 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교하여 모델 성능을 평가할 수 있습니다.

동종 데이터베이스 마이그레이션

동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로) 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫포밍 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 핫픽스는 긴급하기 때문에 일반적인 DevOps 릴리스 워크플로 외부에서 실행됩니다.

하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

정보

IaC

코드형 인프라를 참조하세요.

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

IIoT

산업용 사물 인터넷을 참조하십시오.

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드를 위한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 변경 가능한 인프라보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 변경 불가능한 인프라를 사용한 배포 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

증분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스 또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통해 제조 프로세스의 현대화를 참조하기 위해 2016년에 Klaus Schwab에서 도입한 용어입니다.

인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 산업용 사물 인터넷(IoT) 디지털 트랜스포메이션 전략 구축을 참조하십시오.

검사 VPC

AWS 다중 계정 아키텍처에서는 VPC(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPCs. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 IoT란?을 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

IoT

사물 인터넷을 참조하세요.

IT 정보 라이브러리(TIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL은 ITSM의 기반을 제공합니다.

IT 서비스 관리(TSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

ITIL

IT 정보 라이브러리를 참조하세요.

ITSM

IT 서비스 관리를 참조하세요.

L

레이블 기반 액세스 제어(LBAC)

사용자 및 데이터 자체에 각각 보안 레이블 값을 명시적으로 할당하는 필수 액세스 제어(MAC)를 구현한 것입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

랜딩 존

랜딩 존은 확장 가능하고 안전한 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 안전하고 확장 가능한 다중 계정 AWS 환경 설정을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터를 기반으로 사전 훈련된 딥 러닝 AI 모델입니다. LLM은 질문 답변, 문서 요약, 텍스트를 다른 언어로 번역, 문장 완성과 같은 여러 작업을 수행할 수 있습니다. 자세한 내용은 LLMs 참조하십시오.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어를 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 최소 권한 적용을 참조하십시오.

리프트 앤드 시프트

7R을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. Endianness도 참조하세요.

LLM

대규모 언어 모델을 참조하세요.

하위 환경

환경을 참조하세요.

M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 참조하십시오.

기본 브랜치

브랜치를 참조하세요.

맬웨어

컴퓨터 보안 또는 개인 정보 보호를 손상하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 방해하거나, 민감한 정보를 유출하거나, 무단 액세스를 가져올 수 있습니다. 맬웨어의 예로는 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스 는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB는 관리형 서비스의 예입니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원재료를 작업 현장의 완성된 제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

마이그레이션 가속화 프로그램을 참조하세요.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 결과를 검사하여 조정하는 전체 프로세스입니다. 메커니즘은 작동 시 자체를 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 메커니즘 구축을 참조하세요.

멤버 계정

조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정. AWS Organizations하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

제조 실행 시스템을 참조하세요.

메시지 대기열 원격 측정 전송(MQTT)

리소스가 제한된 IoT 디바이스에 대한 게시/구독 패턴을 기반으로 하는 경량 M2M(machine-to-machine) 통신 프로토콜입니다.

마이크로서비스

잘 정의된 API를 통해 통신하고 일반적으로 소규모 자체 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 AWS 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하세요.

마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 에서 마이크로서비스 구현을 참조하세요 AWS.

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 컨설팅 지원, 교육 및 서비스를 제공하는 AWS 프로그램입니다. MAP에는 레거시 마이그레이션을 체계적인 방식으로 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하는 도구 세트가 포함되어 있습니다.

대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 AWS 마이그레이션 전략의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 일하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 클라우드 마이그레이션 팩토리 가이드와 마이그레이션 팩토리에 대한 설명을 참조하십시오.

마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예: AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

Migration Portfolio Assessment(MPA)

로 마이그레이션하기 위한 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다 AWS 클라우드. MPA는 상세한 포트폴리오 평가(서버 적정 규모 조정, 가격 책정, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선순위 지정, 웨이브 계획)을 제공합니다. MPA 도구(로그인 필요)는 모든 AWS 컨설턴트와 APN 파트너 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 실행 계획을 수립하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오. MRA는 AWS 마이그레이션 전략의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 로 마이그레이션하는 데 사용되는 접근 방식입니다 AWS 클라우드. 자세한 내용은이 용어집의 7R 항목을 참조하고 대규모 마이그레이션을 가속화하기 위해 조직 동원을 참조하세요.

ML

기계 학습을 참조하세요.

현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 의 애플리케이션 현대화 전략을 참조하세요 AWS 클라우드.

현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는 로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 의 애플리케이션에 대한 현대화 준비 상태 평가를 참조하세요 AWS 클라우드.

모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 마이크로서비스로 모놀리식 유형 분해를 참조하십시오.

MPA

마이그레이션 포트폴리오 평가를 참조하세요.

MQTT

메시지 대기열 원격 측정 전송을 참조하세요.

멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

변경 가능한 인프라

프로덕션 워크로드를 위해 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework는 변경 불가능한 인프라를 모범 사례로 사용할 것을 권장합니다.

O

OAC

오리진 액세스 제어를 참조하세요.

OAI

오리진 액세스 ID를 참조하세요.

OCM

조직 변경 관리를 참조하세요.

오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

OI

작업 통합을 참조하세요.

OLA

운영 수준 계약을 참조하세요.

온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

OPC-UA

Open Process Communications - Unified Architecture를 참조하세요.

Open Process Communications - 통합 아키텍처(OPC-UA)

산업 자동화를 위한 M2M(Machinemachine-to-machine) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계와 상호 운용성 표준을 제공합니다.

운영 수준 협약(OLA)

서비스 수준에 관한 계약(SLA)을 지원하기 위해 직무 IT 그룹이 서로에게 제공하기로 약속한 내용을 명확히 하는 계약입니다.

운영 준비 상태 검토(ORR)

인시던트 및 가능한 장애의 범위를 이해, 평가, 예방 또는 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 운영 준비 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경과 함께 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조에서 OT 및 정보 기술(IT) 시스템의 통합은 Industry 4.0 혁신의 핵심 초점입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 운영 통합 가이드를 참조하십시오.

조직 트레일

조직 AWS 계정 내 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 Creating a trail for an organization을 참조하십시오.

조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM은 변화 채택을 가속화하고, 과도기적 문제를 해결하고, 문화 및 조직적 변화를 주도함으로써 조직이 새로운 시스템 및 전략을 준비하고 전환할 수 있도록 지원합니다. AWS 마이그레이션 전략에서는 클라우드 채택 프로젝트에 필요한 변경 속도 때문에이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 사용 가이드를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서 Amazon Simple Storage Service(S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 고급 옵션입니다. OAC는 AWS KMS (SSE-KMS)를 사용한 모든 서버 측 암호화 AWS 리전와 S3 버킷에 대한 동적 PUT 및 DELETE 요청에서 모든 S3 버킷을 지원합니다.

오리진 액세스 ID(OAI)

CloudFront에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 CloudFront는 Amazon S3가 인증할 수 있는 보안 주체를 생성합니다. 인증된 보안 주체는 특

정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더 세분화되고 향상된 액세스 제어를 제공하는 OAC도 참조하십시오.

ORR

운영 준비 상태 검토를 참조하세요.

OT

운영 기술을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 처리하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

P

권한 경계

사용자나 역할이 가질 수 있는 최대 권한을 설정하기 위해 IAM 보안 주체에 연결되는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 권한 경계를 참조하십시오.

개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. PII의 예로는 이름, 주소, 연락처 정보 등이 있습니다.

PII

개인 식별 정보를 참조하세요.

플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

PLC

프로그래밍 가능한 로직 컨트롤러를 참조하세요.

PLM

제품 수명 주기 관리를 참조하세요.

정책

권한을 정의하거나(자격 증명 기반 정책 참조), 액세스 조건을 지정하거나(리소스 기반 정책 참조), 조직의 모든 계정에 대한 최대 권한을 정의할 수 있는 객체 AWS Organizations 입니다(서비스 제어 정책 참조).

다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 스토어를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다. 자세한 내용은 마이크로서비스에서 데이터 지속성 활성화를 참조하십시오.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 참조하십시오.

조건자

`false`일반적으로 `WHERE` 절에 있는 `true` 또는를 반환하는 쿼리 조건입니다.

조건자 푸시다운

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄어들고 쿼리 성능이 향상됩니다.

예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Preventative controls를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 AWS 있는의 엔터티입니다. 이 엔터티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 역할 용어 및 개념의 보안 주체를 참조하십시오.

설계에 따른 개인 정보 보호

전체 개발 프로세스를 통해 개인 정보를 고려하는 시스템 엔지니어링 접근 방식입니다.

프라이빗 호스팅 영역

Amazon Route 53에서 하나 이상의 VPC 내 도메인과 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보가 담긴 컨테이너입니다. 자세한 내용은 Route 53 설명서의 프라이빗 호스팅 영역 작업을 참조하십시오.

사전 예방적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스가 프로비저닝되기 전에 리소스를 스캔합니다. 리소스가 컨트롤을 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 제어 참조 가이드를 참조하고 보안 제어 구현의 사전 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도, 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리.

프로덕션 환경

환경을 참조하세요.

프로그래밍 가능한 로직 컨트롤러(PLC)

제조 분야에서는 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

프롬프트 체인

한 LLM 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 작업을 하위 작업으로 나누거나 예비 응답을 반복적으로 구체화하거나 확장하는 데 사용됩니다. 이를 통해 모델 응답의 정확성과 관련성을 개선하고 보다 세분화되고 개인화된 결과를 얻을 수 있습니다.

가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

게시/구독(pub/sub)

마이크로서비스 간의 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 MES에서 마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 지침과 같은 일련의 단계입니다.

쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

R

RACI 매트릭스

책임, 책임, 상담, 정보 제공(RACI)을 참조하세요.

RAG

Retrieval Augmented Generation을 참조하세요.

랜섬웨어

결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

RASCI 매트릭스

책임, 책임, 상담, 정보 제공(RACI)을 참조하세요.

RCAC

행 및 열 액세스 제어를 참조하세요.

읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의 로드를 줄일 수 있습니다.

재설계

7R을 참조하세요.

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터링

7R을 참조하세요.

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전 는 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 계정에서 사용할 수 있는 지정을 참조 AWS 리전 하세요.

회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

리호스팅

7R을 참조하세요.

release

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7R을 참조하세요.

리플랫포밍

7R을 참조하세요.

재구매

7R을 참조하세요.

복원력

중단에 저항하거나 복구할 수 있는 애플리케이션의 기능입니다. 에서 복원력을 계획할 때 고가용성 및 재해 복구가 일반적인 고려 사항입니다 AWS 클라우드. 자세한 내용은 AWS 클라우드 복원력을 참조하세요.

리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

RACI(Responsible, Accountable, Consulted, Informed) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다. 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조언자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 Implementing security controls on AWS의 Responsive controls를 참조하십시오.

retain

7R을 참조하세요.

사용 중지

7R을 참조하세요.

검색 증강 세대(RAG)

응답을 생성하기 전에 LLM이 훈련 데이터 소스 외부에 있는 신뢰할 수 있는 데이터 소스를 참조하는 생성형 AI 기술입니다. 예를 들어 RAG 모델은 조직의 지식 기반 또는 사용자 지정 데이터에 대한 의미 검색을 수행할 수 있습니다. 자세한 내용은 RAG란 무엇입니까?를 참조하십시오.

교체

공격자가 보안 인증 정보에 액세스하는 것을 더 어렵게 만들기 위해 보안 암호를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

액세스 규칙이 정의된 기본적이고 유연한 SQL 표현식을 사용합니다. RCAC는 행 권한과 열 마스크로 구성됩니다.

RPO

복구 시점 목표를 참조하세요.

RTO

복구 시간 목표를 참조하세요.

런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

S

SAML 2.0

많은 ID 제공업체(idP)에서 사용하는 개방형 표준입니다. 이 기능을 사용하면 연동 SSO(Single Sign-On)를 AWS Management Console 사용할 수 있으므로 사용자는 조직의 모든 사용자에 대해 IAM에서 사용자를 생성하지 않고도에 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하십시오.

SCADA

감독 제어 및 데이터 획득을 참조하세요.

SCP

서비스 제어 정책을 참조하세요.

secret

에는 암호 또는 사용자 자격 증명과 같이 암호화된 형식으로 저장하는 AWS Secrets Manager기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 Secrets Manager 설명서의 Secrets Manager 보안 암호에 무엇이 있습니까?를 참조하세요.

설계를 통한 보안

전체 개발 프로세스를 통해 보안을 고려하는 시스템 엔지니어링 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어에는 예방, 탐지, 대응 및 사전 예방의 네 가지 주요 유형이 있습니다.

보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM)와 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협과 보안 침해를 탐지하고 알림을 생성합니다.

보안 응답 자동화

보안 이벤트에 자동으로 응답하거나 해결하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지 또는 대응 AWS 보안 제어 역할을 합니다. 자동 응답 작업의 예로는 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 자격 증명 교체 등이 있습니다.

서버 측 암호화

데이터를 AWS 서비스 수신하는가 대상에서 데이터를 암호화합니다.

서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCP는 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대해 제한을 설정하거나 가드레일을 정의합니다. SCP를 허용 목록 또는 거부 목록으로 사용하여 허용하거나 금지할 서비스 또는 작업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 서비스 제어 정책을 참조하세요.

서비스 엔드포인트

에 대한 진입점의 URL입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

서비스 수준에 관한 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

서비스 수준 지표(SLI)

오류율, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정입니다.

서비스 수준 목표(SLO)

서비스 수준 지표로 측정되는 서비스의 상태를 나타내는 대상 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수를 AWS 위해와 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 담당하는 반면, 사용자는 클라우드의 보안을 담당합니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

SIEM

보안 정보 및 이벤트 관리 시스템을 참조하세요.

단일 장애 지점(SPOF)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에 장애가 발생한 경우.

SLA

서비스 수준 계약을 참조하세요.

SLI

서비스 수준 표시기를 참조하세요.

SLO

서비스 수준 목표를 참조하세요.

분할 앤 시드 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 에서 애플리케이션 현대화에 대한 단계별 접근 방식을 참조하세요 AWS 클라우드.

SPOF

단일 장애 지점을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스 또는 비즈니스 인텔리전스용으로 설계되었습니다.

Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도

하고 대체하는 것과 비슷합니다. Martin Fowler가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

서브넷

VPC의 IP 주소 범위입니다. 서브넷은 단일 가용 영역에 상주해야 합니다.

감독 제어 및 데이터 획득(SCADA)

제조에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 프로덕션 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

사용자 상호 작용을 시뮬레이션하여 잠재적 문제를 감지하거나 성능을 모니터링하는 방식으로 시스템을 테스트합니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

LLM에 컨텍스트, 지침 또는 지침을 제공하여 동작을 지시하는 기법입니다. 시스템 프롬프트는 컨텍스트를 설정하고 사용자와의 상호 작용을 위한 규칙을 설정하는 데 도움이 됩니다.

T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색 및 필터링할 수 있습니다. 자세한 내용은 AWS 리소스에 태그 지정을 참조하십시오.

대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

테스트 환경

환경을 참조하세요.

훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

전송 게이트웨이

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 전송 게이트웨이란 무엇입니까?를 참조하세요.

트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

신뢰할 수 있는 액세스

사용자를 대신하여 AWS Organizations 및 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요 AWS Organizations .

튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

피자 두 판 팀

피자 두 판이면 충분한 소규모 DevOps 팀. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

U

불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다. 자세한 내용은 Quantifying uncertainty in deep learning systems 가이드를 참조하십시오.

차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

상위 환경

환경을 참조하세요.

V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수반하는 데이터베이스 유지 관리 작업입니다.

버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있게 하는 두 VPC 간의 연결입니다. 자세한 내용은 Amazon VPC 설명서의 VPC 피어링이란?을 참조하십시오.

취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

W

웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에 대해 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대 위치를 기반으로 행 값에 액세스하는 등의 작업을 처리하는 데 유용합니다.

워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

WORM

쓰기를 한 번, 많이 읽기를 참조하세요.

WQF

AWS 워크로드 검증 프레임워크를 참조하세요.

한 번 쓰기, 많이 읽기(WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 데이터를 읽을 수 있지만 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 변경할 수 없는 것으로 간주됩니다.

Z

제로데이 익스플로잇

제로데이 취약성을 활용하는 공격, 일반적으로 맬웨어입니다.

제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

제로샷 프롬프트

LLM에 작업을 수행하기 위한 지침을 제공하지만 작업에 도움이 될 수 있는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 작업을 처리해야 합니다. 제로샷 프롬프트의 효과는 작업의 복잡성과 프롬프트의 품질에 따라 달라집니다. 스크린샷이 거의 없는 프롬프트도 참조하세요.

좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.