Amazon AppStream 2.0 배포 모범 사례

Amazon AppStream 2.0 배포 모범 사례:

Table of Contents

Amazon AppStream 2.0 배포 모범 사례

발행일: 2022년 1월 19일 (문서 수정)

요약

이 백서에서는 Amazon AppStream 2.0 배포를 위한 일련의 모범 사례를 간략하게 설명합니다. 이 백서에서는 Amazon Virtual Private Cloud(VPC) 설계, 이미지 생성 및 관리, 플릿 사용자 지정, 플릿 Auto Scaling 전략을 다룹니다. 여기에는 사용자 연결 방법, 인증 및 Microsoft Active Directory와의 통합이 포함됩니다. 이 백서에는 AppStream 2.0 보안 설계, 모니터링 및 비용 최적화를 위한 권장 사항도 포함되어 있습니다.

이 백서는 관련 정보에 빠르게 액세스할 수 있도록 작성되었습니다. 네트워크 엔지니어, 애플리케이션 제공 전문가, 디렉토리 엔지니어 또는 보안 엔지니어를 대상으로 합니다.

소개

Amazon AppStream 2.0은 사용자가 어디서나 데스크톱 애플리케이션에 즉시 액세스할 수 있도록 하는 완전관리형 애플리케이션 스트리밍 서비스입니다. AppStream 2.0은 애플리케이션을 호스팅하고 실행하는 데 필요한 AWS 리소스를 관리합니다. 자동으로 규모를 조정하며 필요에 따라 사용자에게 액세스를 제공합니다. AppStream 2.0을 사용하면 최종 사용자가 기본적으로 설치된 애플리케이션과 구분할 수 없는 반응형 사용자 환경을 통해 원하는 디바이스에서 필요한 애플리케이션에 액세스할 수 있습니다.

다음 섹션에서는 Amazon AppStream 2.0에 대한 세부 정보를 제공하고, 서비스 작동 방식을 설명하고, 서비스를 시작하는 데 필요한 사항을 설명하고, 사용할 수 있는 옵션 및 기능에 대해 설명합니다. 최종 사용자를 위해 AppStream 2.0을 배포할 때는 우수한 사용자 경험을 제공하기 위한 모범 사례를 구현하는 것이 중요합니다. 또한 규모에 상관없이 모든 기업이 월별 운영 비용을 줄이는 비용 최적화의 혜택을 누릴 수 있습니다.

핵심 개념

AppStream 2.0을 최대한 활용하려면 다음 개념을 잘 알아두세요.

- 이미지 - 이미지는 사전 구성된 인스턴스 템플릿입니다. 이미지에는 사용자에게 스트리밍할 수 있는 애플리케이션과 사용자가 애플리케이션을 빠르게 시작할 수 있도록 하는 기본 Windows 및 애플리케이션 설정이 포함되어 있습니다. AWS에서 기본 이미지를 제공합니다. 기본 이미지를 사용하여 이미지 빌더를 생성한 다음 자체 애플리케이션을 포함하는 이미지를 생성할 수 있습니다. 이미지를 만든 후에는 이미지를 변경할 수 없습니다. 다른 애플리케이션을 추가하거나 기존 애플리케이션을 업데이트하거나 이미지 설정을 변경하려면 새로운 이미지를 생성해야 합니다. 이미지를 다른 AWS 리전에 복사하거나 같은 리전의 다른 AWS 계정과 공유할 수 있습니다.
- 이미지 빌더 — 이미지 빌더는 이미지를 생성하는 데 사용하는 가상 머신입니다. AppStream 2.0 콘솔을 사용하여 이미지 빌더를 시작하고 여기에 연결할 수 있습니다. 이미지 빌더에 연결한 후 애플리케이션을 설치, 추가, 테스트한 다음 이미지 빌더를 사용하여 이미지를 생성할 수 있습니다. 소유한 프라이빗 이미지를 사용하여 새 이미지 빌더를 시작할 수 있습니다.
- 플릿 — 플릿은 지정한 이미지를 실행하는 플릿 인스턴스(스트리밍 인스턴스라고도 함)로 구성되어 있습니다. 플릿에 대해 원하는 수의 스트리밍 인스턴스를 설정하고 필요에 따라 플릿을 자동으로 조정하도록 정책을 구성할 수 있습니다. 사용자 한 명당 하나의 인스턴스가 필요합니다.
- 스택 — 스택은 연결된 플릿, 사용자 액세스 정책 및 스토리지 구성으로 구성되어 있습니다. 스택을 설정하여 사용자에게 애플리케이션을 스트리밍합니다.
- 스트리밍 인스턴스 — 스트리밍 인스턴스(플릿 인스턴스라고도 함)는 단일 사용자가 애플리케이션 스트리밍에 사용할 수 있는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스입니다. 사용자 세션이 완료되면 Amazon EC2에서 인스턴스를 종료합니다.

VPC 설계

설계 지침

AppStream 2.0을 전용 VPC에 배포합니다. AppStream 2.0 VPC를 설계할 때는 예측된 증가률에 맞게 크기를 조정하세요. 새로운 사용 사례와 나중에 추가될 수 있는 추가 가용 영역(AZ)을 위해 IP 주소 용량을 예약하십시오. AppStream 2.0의 기본 설계 포인트는 한 명의 사용자만 AppStream 2.0 인스턴스를 사용할 수 있다는 것입니다. IP 공간을 할당할 때는 한 명의 사용자를 AppStream 2.0 인스턴스당 하나의 IP 주소로 생각하십시오. AppStream 2.0을 사용하면 사용자가 여러 AppStream 2.0 인스턴스를 사용할 수 있습니다. 따라서 추가 AppStream 2.0 인스턴스가 필요한 사용 사례도 고려하여 IP 공간을 계획해야 합니다.

VPC 클래스 없는 도메인 간 라우팅(CIDR)의 최대 크기는 /16이지만 AWS에서는 프라이빗 IP 주소를 과도하게 할당하지 않는 것이 좋습니다. 추가 CIDR을 통해 VPC의 크기를 확장할 수 있지만 여기에는 한계가 있으므로 처음부터 필요한 만큼 할당해야 합니다.

AppStream 2.0 배포를 Active Directory 도메인에 조인하는 경우 VPC에 설정된 DHCP 옵션에는 도메인 DNS가 구성되어 있어야 합니다. 도메인 이름 서버는 Active Directory 도메인에 대한 권한이 있는 DNS IP 주소를 지정해야 합니다. 그렇지 않으면 DNS가 Active Directory 도메인의 신뢰할 수 있는 DNS 인스턴스로 DNS 요청을 전달해야 합니다. 또한 VPC에 `enableDnsHostnames` 및 `EnableDnsSupport`가 구성되어 있어야 합니다.

가용 영역

가용 영역(AZ)은 AWS 리전에 중복 전원, 네트워킹 및 연결이 있는 하나 이상의 개별 데이터 센터입니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

Amazon AppStream 2.0에서는 하나의 서브넷만 있으면 플릿을 시작할 수 있습니다. 모범 사례는 고유한 가용 영역당 하나의 서브넷으로 최소 2개의 가용 영역을 구성하는 것입니다. 플릿 Auto Scaling을 최적화하려면 두 개 이상의 가용 영역을 사용하십시오. 수평적 규모 조정은 증가를 대비해서 서브넷에 IP 공간을 추가할 수 있다는 추가적인 이점이 있습니다. 이에 대해서는 이 문서의 다음 서브넷 크기 조정 섹션에서 다룹니다. AWS Management Console에서는 플릿 생성 시 두 개의 서브넷만 지정할 수 있습니다. AWS Command Line Interface(AWS CLI) 또는 AWS CloudFormation를 사용하거나 세 개 이상의 서브넷 ID를 허용하십시오.

서브넷 크기

AppStream 2.0 플릿 전용 서브넷을 통해 라우팅 정책 및 네트워크 액세스 제어 목록의 유연성을 확보할 수 있습니다. 스택에는 별도의 리소스 요구 사항이 있을 수 있습니다. 예를 들어 AppStream 2.0 스택에는 별도의 규칙 세트를 제공하는 격리 요구 사항이 있을 수 있습니다. 여러 Amazon AppStream 2.0 플릿이 동일한 서브넷을 사용하는 경우 모든 플릿의 최대 용량 합계가 사용 가능한 총 IP 주소 수를 초과하지 않도록 하십시오.

동일한 서브넷에 있는 모든 플릿의 최대 용량이 사용 가능한 총 IP 주소 수를 초과할 수 있거나 초과한 경우 플릿을 전용 서브넷으로 마이그레이션하십시오. 이렇게 하면 자동 조정 이벤트로 인해 할당된 IP 공간이 소진되는 것을 방지할 수 있습니다. 플릿의 총 용량이 할당된 서브넷의 할당된 IP 공간을 초과하는 경우 API 또는 AWS CLI "update fleet"을 사용하여 더 많은 서브넷을 할당하십시오. 자세한 내용은 Amazon VPC 할당량 및 할당량 증가 방법을 참조하세요.

VPC에서 용량을 확장할 수 있도록 서브넷 수를 스케일 아웃하고 그에 따라 서브넷 크기를 조정하는 것이 가장 좋습니다. 또한 AppStream 2.0 플릿 최대값이 서브넷에서 할당한 총 IP 공간을 초과하지 않도록 해야 합니다. 총 IP 공간을 계산할 때 AWS의 각 서브넷에 대해 5개의 IP 주소가 예약됩니다. 두 개 이상의 서브넷을 사용하고 수평으로 규모를 조정하면 다음과 같은 여러 가지 이점이 있습니다.

- 가용 영역 장애 발생 시 복원력 향상
- 플릿 인스턴스 Auto Scaling 시 처리량 증가
- 프라이빗 IP 주소의 더 효율적인 사용, IP 소모 방지

Amazon AppStream 2.0의 서브넷 크기를 조정할 때는 총 서브넷 수와 사용률이 최고조에 달할 때 예상되는 최대 동시 사용률을 고려하십시오. 플릿의 (`InUseCapacity`)와 예약 용량 (`AvailableCapacity`)을 사용하여 이를 모니터링할 수 있습니다. Amazon AppStream 2.0에서는 사용한 AppStream 2.0 플릿 인스턴스와 사용 가능한 AppStream 2.0 플릿 인스턴스의 합계에 `ActualCapacity` 레이블이 지정됩니다. 총 IP 공간의 크기를 적절하게 조정하려면 필요한 `ActualCapacity` 공간을 예측하고 플릿에 할당된 서브넷 수(복원력을 위한 서브넷 1개를 뺀 값)로 나누십시오.

예를 들어 최대 예상 플릿 인스턴스 수가 1000개이고 비즈니스 요구 사항이 한 번의 가용 영역 장애에도 복원력이 있어야 하는 경우 3개의 x/23 서브넷이 기술 및 비즈니스 요구 사항을 충족합니다.

- /23 = 호스트 512개 — 예약 5개 = 서브넷당 플릿 인스턴스 507개
- 서브넷 3개 — 서브넷 1개 = 서브넷 2개
- 서브넷 2개 x 서브넷당 플릿 인스턴스 507개 = 피크 시 플릿 인스턴스 1,014개

서브넷 크기 조정 예제

2 x /22 서브넷도 복원력을 충족하지만 다음 사항을 고려하십시오.

- 1,536개의 IP 주소를 예약하는 대신 두 개의 AZ를 사용하면 2,048개의 IP 주소가 예약되어 다른 기능에 사용될 수 있는 IP 주소를 낭비하게 됩니다.
- 한 AZ에 액세스할 수 없게 되면 플릿 인스턴스를 스케일 아웃할 수 있는 기능이 AZ의 처리량에 따라 제한됩니다. 이로 인해 `PendingCapacity`의 기간이 연장될 수 있습니다.

서브넷 라우팅

AppStream 2.0 인스턴스용 프라이빗 서브넷을 생성하여 아웃바운드 트래픽을 위한 중앙 집중식 VPC를 통해 퍼블릭 인터넷으로 라우팅하는 것이 가장 좋습니다. AppStream 2.0 세션 스트리밍을 위한 인바운드 트래픽은 스트리밍 게이트웨이를 통해 Amazon AppStream 2.0 서비스를 통해 처리되므로 이를 위해 퍼블릭 서브넷을 구성할 필요가 없습니다.

리전 내 연결

Active Directory 도메인에 연결된 AppStream 2.0 플릿 인스턴스의 경우 각 AWS 리전의 공유 서비스 VPC에서 Active Directory 도메인 컨트롤러를 구성합니다. Active Directory의 소스는 Amazon EC2 기반 도메인 컨트롤러 또는 AWSMicrosoft Managed AD일 수 있습니다. 공유 서비스와 AppStream 2.0 VPC 간의 라우팅은 VPC 피어링 연결 또는 트랜짓 게이트웨이를 통해 이루어질 수 있습니다. 트랜짓 게이트웨이는 대규모 라우팅의 복잡성을 해결하지만 대부분의 설정에서 VPC 피어링을 선호하는 데에는 여러 가지 이유가 있습니다.

- VPC 피어링은 두 VPC 간의 직접 연결입니다(추가 홉 없음).
- 시간당 요금은 없으며 가용 영역 간 표준 데이터 전송 요금만 부과됩니다.
- 대역폭에는 제한이 없습니다.
- VPC 간 보안 그룹 액세스를 지원합니다.

AppStream 2.0 인스턴스가 공유 서비스 VPC에서 대규모 데이터 세트를 포함하는 애플리케이션 인프라 및/또는 파일 서버에 연결되는 경우 특히 그렇습니다. 일반적으로 액세스하는 이러한 리소스에 대한 경로를 최적화하면 다른 모든 VPC 및 인터넷 라우팅이 트랜짓 게이트웨이를 통해 수행되는 설계에서도 VPC 피어링 연결이 선호됩니다.

아웃바운드 인터넷 트래픽

공유 서비스로의 직접 라우팅은 대부분 피어링 연결을 통해 최적화되지만, AWS 트랜짓 게이트웨이를 사용하여 여러 VPC에서 단일 인터넷 출구 지점을 생성하여 AppStream 2.0의 아웃바운드 트래픽을 설계할 수 있습니다. 다중 VPC 설계에서는 나가는 모든 인터넷 트래픽을 제어하는 전용 VPC를 사용하는 것이 표준 관행입니다. 이 구성을 사용하면 트랜짓 게이트웨이의 유연성이 향상되고 서브넷에 연결된 표준 라우팅 테이블을 통한 라우팅을 제어할 수 있습니다. 또한 이 설계는 추가 복잡성 없이 전이적 라우팅을 지원하므로 각 VPC에 중복 NAT(네트워크 주소 변환) 게이트웨이 또는 NAT 인스턴스가 필요하지 않습니다.

모든 아웃바운드 인터넷 트래픽이 단일 VPC로 중앙 집중화되면 NAT 게이트웨이 또는 NAT 인스턴스가 일반적인 설계 선택입니다. 어떤 것이 조직에 가장 적합한지 결정하려면 NAT 게이트웨이와 NAT 인스턴스를 비교하기 위한 관리 가이드를 참조하세요. AWS Network Firewall은 경로 수준에서 보호하고 OSI 모델의 계층 3에서 7까지의 상태 비저장 및 상태 저장 규칙을 제공하여 보안 그룹 및 네트워크 액세스 제어 수준 이상으로 보호를 확장할 수 있습니다. 자세한 내용은 AWS Network Firewall의 배포 모델을 참조하세요. 조직에서 URL 필터링과 같은 고급 기능을 수행하는 타사 제품을 선택한 경우 아웃바운드 인터넷 VPC에 서비스를 배포하십시오. 이는 NAT 게이트웨이 또는 NAT 인스턴스를 대체할 수 있습니다. 타사 공급업체가 제공하는 지침을 따르십시오.

온프레미스

온프레미스 리소스에 대한 연결이 필요한 경우, 특히 Active Directory에 연결된 AppStream 2.0 인스턴스의 경우 AWS Direct Connect을 통해 복원력이 매우 뛰어난 연결을 설정하십시오.

VPC 엔드포인트

Amazon S3 VPC 엔드포인트

많은 Amazon AppStream 2.0 배포에는 홈 폴더 및 애플리케이션 설정을 통한 사용자 상태 지속성이 필요합니다. 이러한 Amazon Simple Storage Service(Amazon S3) 위치와의 프라이빗 통신을 활성화하면 퍼블릭 인터넷을 사용하지 않아도 됩니다. VPC 엔드포인트 게이트웨이를 통해 이를 달성할 수 있습니다. VPC 엔드포인트 게이트웨이가 AWS PrivateLink for Amazon S3보다 선호되는 이유는 다음과 같습니다.

- AppStream 2.0 네트워크 액세스 요구 사항에 대해 비용 최적화되었습니다.
- 온프레미스 리소스에서는 Amazon S3 버킷에 액세스할 필요가 없습니다.
- 사용자 지정 정책 문서를 사용하여 AppStream 2.0 인스턴스에서만 액세스를 제한할 수 있습니다.

VPC 엔드포인트 게이트웨이를 만든 후에는 사용자 지정 정책을 생성하여 프라이빗 연결을 보호하는 것이 가장 좋습니다. 사용자 지정 정책은 AppStream 2.0 서비스 Identity and Access Management 역할의 Amazon 리소스 이름(ARN)으로 시작됩니다. 사용자 상태 지속성에 필요한 S3 작업을 명시적으로 지정하십시오.

> **Note**
>
> `Resources` 섹션의 다음 예에서는 상태 홈 폴더 경로를 먼저 지정하고 애플리케이션 설정 경로를 두 번째로 지정합니다.

Example

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

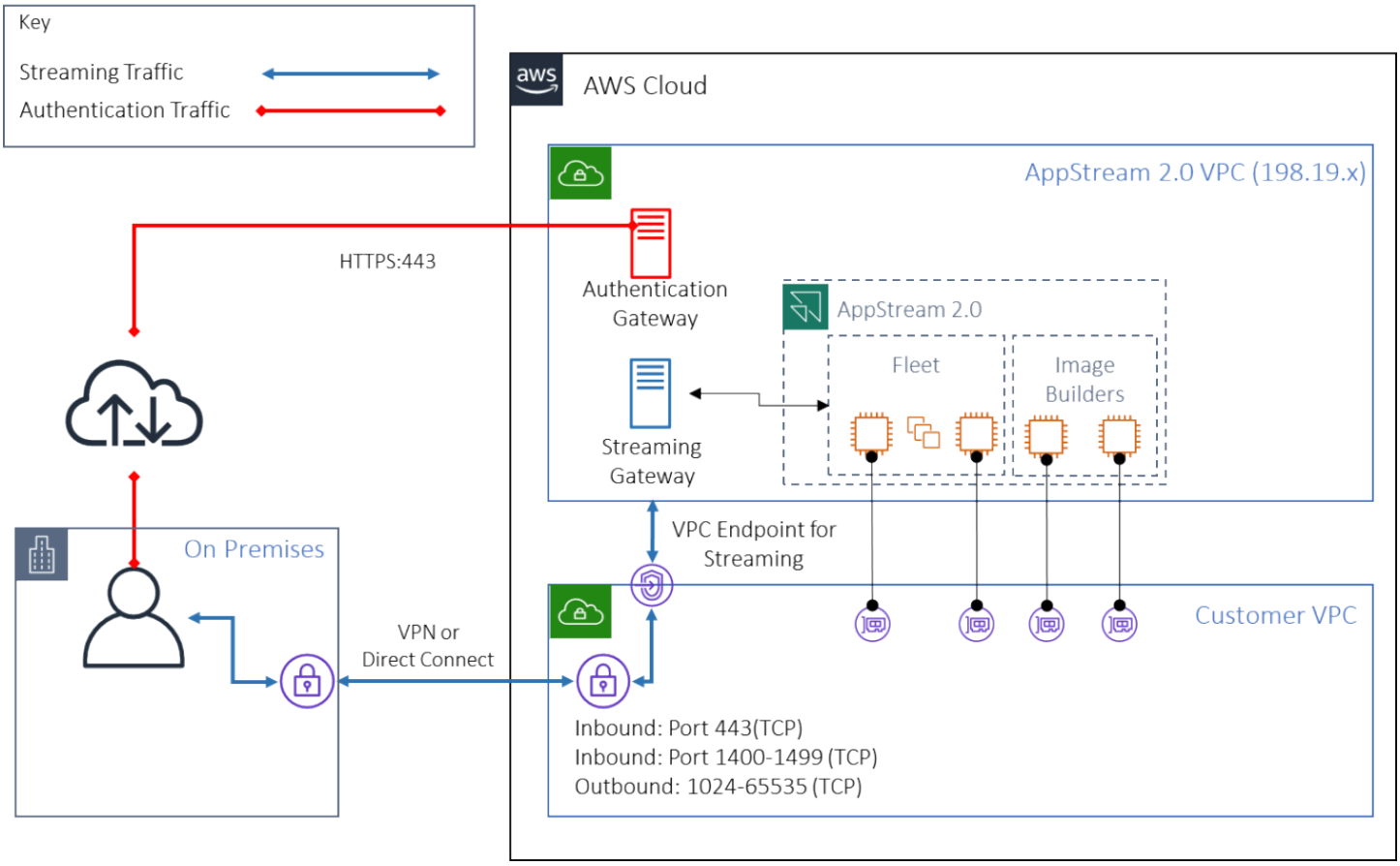
```
      "Sid": "Allow-AppStream-to-access-home-folder-and-
application-settings",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:sts::account-id-without-hyphens:assumed-
role/AmazonAppStreamServiceAccess/AppStream2.0"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*"
      ]
    }
  ]
}
```

Amazon AppStream 2.0 API 인터페이스 VPC 엔드포인트

Amazon AppStream 2.0에 대한 API 및 CLI 명령이 VPC에서 시작되는 설계 시나리오에서는 인터페이스 VPC 엔드포인트를 통해 이러한 프로그래밍 방식 호출을 사유화십시오.

Amazon AppStream 2.0 스트리밍 VPC 엔드포인트

인터페이스 VPC 엔드포인트를 통해 Amazon AppStream 2.0 스트리밍 트래픽을 라우팅할 수 있지만 이 구성을 사용할 때는 주의해야 합니다. 퍼블릭 인터넷을 통한 기본 스트리밍 동작은 Amazon AppStream 2.0 스트리밍 트래픽의 가장 효율적이고 성능이 우수한 전송 방법입니다.



Amazon AppStream 2.0 스트리밍 인터페이스 VPC 엔드포인트

이전 그림에서 볼 수 있듯이 퍼블릭 인터넷은 Amazon AppStream 2.0 스트리밍 게이트웨이로 가는 가장 효율적인 경로입니다. 고객 관리형 VPC와 네트워킹을 통한 라우팅은 복잡성과 지연 시간을 증가시킵니다. 또한 Direct Connect를 통한 데이터 전송 요금도 추가됩니다.

> **Note**
>
> VPC 엔드포인트는 스트리밍만 지원하며 인증은 여전히 퍼블릭 인터넷을 통해 이루어져야 합니다. SAML SSO(Single Sign-On) ID 공급자(IdP)와 같은 필수 액세스는 여전히 퍼블릭 인터넷을 통해서만 액세스할 수 있는 요구 사항입니다.

이미지 생성 및 관리

AppStream 2.0에서 플릿 또는 이미지 빌더를 시작할 때는 AppStream 2.0 기본 이미지 중 하나를 선택해야 합니다. 그러면 관리자는 기본 이미지를 기반으로 자체 애플리케이션 및 구성 설정을 추가할 수 있습니다.

이미지를 구축할 때는 애플리케이션이 정확하고 안전하게 작동하도록 하기 위한 주요 고려 사항이 있습니다. 또한 이미지 유지 관리 방법에 대한 디자인 고려 사항도 있습니다.

AppStream 2.0 이미지 만들기

새 이미지를 만들 때는 다음 사항을 고려해야 합니다.

- 운영 체제
- 애플리케이션
- 사용자 프로필
- 보안
- 성능
- 에이전트 버전
- Image Assistant CLI

AppStream 2.0 이미지 만들기

2021년 11월, AppStream 2.0은 Amazon Linux 2에 대한 지원을 시작했습니다. 이번 발표를 통해 AppStream 2.0은 이제 네 가지 플랫폼 유형을 지원합니다.

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Amazon Linux 2

애플리케이션에 필요한 사항에 따라 특정 플랫폼을 선택해야 할 수도 있습니다(예를 들어, 애플리케이션에 Windows가 필요한 경우 Amazon Linux 2는 옵션이 아닙니다). 애플리케이션 요구 사항 외에도 다음 비교 매트릭스를 참조하여 사용 사례와 환경에 가장 적합한 플랫폼 유형을 선택할 수 있습니다.

표 1 — 플랫폼 유형, 사용 시기, 가격

플랫폼 유형	사용해야 하는 경우	플릿 요금*
Windows Server(2012 R2, 2016 또는 2019)	애플리케이션은 Windows에서만 실행할 수 있습니다(Amazon Linux 2는 지원하지 않음). 스트리밍 인스턴스를 도메인으로 가입하고 싶습니다. AppStream 2.0 스트리밍 인스턴스에서 기존 그룹 정책을 사용하려고 합니다(Linux는 그룹 정책을 준수하지 않지만 세션 스크립트를 사용하여 세션 시작 시 구성을 자동화할 수 있습니다). 데스크톱 보기를 사용하며 사용자는 Windows 데스크톱 환경을 선호합니다. 애플리케이션 카탈로그와 이미지를 만들려면 단계별 마법사를 제공하는 Image Assistant 애플리케이션을 사용하는 것이 좋습니다. 현재는 터미널 명령을 사용하여 Amazon Linux 2 이미지를 생성해야 합니다(자세한 내용은 이 자습서 참조). 애플리케이션 설정 지속성을 사용하고 싶습니다. 애플리케이션 설정 지속성 활성화는 현재 Linux 기반 스택에서 지원되지 않습니다.	각 고유 사용자에 대해 월 4.19 달러의 RDS SAL(Microsoft 원격 데스크톱 서비스 구독자 액세스 라이선스) 요금**에 다음 요금이 추가됩니다. 1. 상시 작동, 온디맨드 플릿의 경우 시간당 0.10 달러 2. 탄력적 플릿의 경우 시간당 0.15 달러
Amazon Linux 2	저렴한 스트리밍 인스턴스를 활용하고 RDS SAL 라이선스 요금을 피하고 싶을 것입니다. 애플리케이션은 Amazon Linux 2와 호환됩니다.	Linux 인스턴스는 Window 인스턴스에 비해 비용이 저렴합니다. Linux에서는 RDS SAL 요금과 다음과 같은 시간당 요금을 지불하지 않습니다.

플랫폼 유형	사용해야 하는 경우	플릿 요금*
		1. 상시 작동, 온디맨드 플릿의 경우 시간당 0.084 달러 2. 탄력적 플릿의 경우 시간당 0.112달러

* 버지니아 북부 지역의 stream.standard.medium 기준

** 자격을 갖춘 고객은 자체 라이선스를 가져와 AWS RDS SAL 수수료를 면제받을 수 있습니다. 자세한 내용은 AppStream 2.0 요금 페이지를 참조하세요. 교육 기관 고객도 특별 혜택을 받을 수 있습니다. 학교, 대학교 및 특정 공공 기관은 사용자당 Microsoft RDS SAL 사용자 요금 감면 혜택을 받을 수 있습니다.

애플리케이션

애플리케이션을 설치하기 전에 애플릴케이션 종속성 및 하드웨어 요구 사항과 같은 애플리케이션 요구 사항을 검토하는 것이 중요합니다. Image Builder 인스턴스에 애플리케이션을 성공적으로 설치한 후에는 테스트 사용자 컨텍스트에서 사용자를 전환하고 애플리케이션을 테스트해야 합니다.

애플리케이션 배포를 계획할 때는 서비스 엔드포인트와 할당량을 염두에 두세요. 또한 이미지를 생성하기 전에 설치 프로그램 및 도우미 파일을 정리하여 전체 C 드라이브 공간을 최적화하세요. 다시 말씀드리지만, AppStream 2.0 인스턴스에는 200GB의 고정 크기 볼륨이 하나 있습니다. 고정 크기 볼륨을 초과하지 않도록 하려면 설치 후 디스크 공간을 최적화하는 것이 가장 좋습니다.

사용자가 실시간으로 액세스할 수 있는 애플리케이션 카탈로그를 수정하려는 경우 동적 애플리케이션 프레임워크가 API 작업을 제공합니다. 동적 앱 공급자에서 관리하는 애플리케이션은 이미지에 포함되거나, 혹은 Windows 파일 공유 또는 애플리케이션 가상화 기술에서처럼 오프인스턴스가 될 수 있습니다. 이 기능을 사용하려면 Microsoft Active Directory 도메인에 조인되는 플릿이 필요합니다. 자세한 내용은 AppStream 2.0과 함께 Active Directory 사용을 참조하세요.

앱 블록

앱 블록은 사용자가 사용할 애플리케이션을 시작하는 데 필요한 설치 스크립트와 애플리케이션 파일을 나타냅니다. 가상 하드 디스크(VHD)는 Amazon S3의 모든 객체가 될 수 있습니다. 이 객체는 완전히 다운로드해야 사용자가 애플리케이션에 액세스할 수 있으므로 1.5GB 미만으로 설정하는 것이 좋습니다.

앱 블록 최적화

Windows 기반 플릿의 경우 애플리케이션을 포함할 VHDX 파일을 만드는 것이 좋습니다. Linux 기반 플릿의 경우 이미지(IMG)를 만드는 것이 좋습니다. 애플리케이션 파일을 호스팅하려면 이러한 가상 디스크를 가능한 한 작게 만들어야 합니다. 가상 디스크를 압축하여 크기를 더 줄일 수 있습니다. 설치 스크립트에서 마운트하기 전에 디스크의 압축을 풀어야 합니다. Windows PowerShell 설치 스크립트 예제에는 압축 해제 기능이 포함되어 있습니다. 아카이브 확장(zip)과 다운로드 속도 사이에는 절충점이 있습니다. 가장 빠른 애플리케이션 실행 시간을 제공하는 밸런스를 찾기 위해 몇 가지 테스트가 필요할 수 있습니다.

애플리케이션 업데이트

애플리케이션에는 사소한 변경 사항과 주요 변경 사항이 모두 있을 수 있습니다. 사소한 업데이트의 경우 앱 블록 파일을 호스팅하는 Amazon S3 버킷에서 버전 관리를 활성화하십시오. 이 설정을 통해 관리자는 앱 블록 구성을 변경하지 않고도 해당 애플리케이션 VHD 객체의 버전을 변경하여 특정 애플리케이션의 이전 버전으로 롤백할 수 있습니다. 주요 업데이트를 통해 업데이트된 VHD를 위한 새 앱 블록을 만드십시오. 이를 통해 관리자는 버전 관리 수준이 아닌 앱 블록 수준에서 주요 애플리케이션 변경 내용을 구분할 수 있어 관리 애플릴케이션 관리를 위한 보다 체계적인 접근 방식을 제공합니다.

사용자 프로필 사용자 지정

Amazon AppStream 2.0은 기본적으로 비지속 애플리케이션 및 데스크톱 솔루션입니다. 사용자 세션이 종료되면 시스템 및 사용자 변경도 모두 종료됩니다. 필요한 경우에만 애플리케이션 설정 지속성을 활성화하십시오. 이로 인해 로그온 프로세스에 오버헤드가 추가되고 필요한 S3 스토리지에 대한 비용 고려 사항이 추가될 수 있습니다.

애플리케이션 설정 지속성이 필요한 상황에서는 AWS는 사용자 지정 정책 및 S3 VPC 게이트웨이 엔드포인트를 통해 연결을 보호할 것을 권장합니다. 전체 애플리케이션 설정 크기를 평가하고 애플리케이션 설정 지속성에 저장된 설정을 최소화하여 비용과 성능을 최적화합니다.

사용자 프로필 사용자 지정은 AppStream 2.0 Image Builder 인스턴스에서 구성할 수 있습니다. 여기에는 레지스트리 키 추가 및 수정, 파일 추가 및 기타 사용자별 구성이 포함됩니다. AppStream 2.0 Image Assistant에서 사용자 프로필을 생성할 수 있는 옵션이 있습니다. 그러면 템플릿 사용자 프로필이 기본 사용자 프로필에 복사됩니다. 이미지가 플릿에 배포된 후 플릿에서 세션을 스트리밍하는 최종 사용자는 기본 사용자 프로필에서 사용자 프로필을 생성하게 됩니다. 특히 애플리케이션 설정 지속성이 활성화된 경우 사용자 프로필 크기를 최소화하는 것을 고려해야 합니다. 기본적으로 사용자 프로필의 최대 vHDX 크기는 1GB입니다. 스트리밍 세션이 시작될 때마다 사용자 프로필 vHDX 파일이 S3 버킷에서 다운로드됩니다. 이렇게 하면 스트리밍 세션 준비 시간이 늘어나고 제한을 초과할 위험이 생겨 vHDX 파일을 사용한 사용자 프로필 마운트가 실패하게 됩니다.

1GB보다 큰 사용자 프로필이 필요한 사용 사례의 경우 AWS는 프로필을 저장하는 다른 방법을 사용할 것을 권장합니다. Windows File Server용 Amazon FSx와 같은 공유 스토리지에서 로밍 프로필 또는 FSLogix 프로필 컨테이너를 사용하는 경우를 예로 들 수 있습니다. Windows File Server용 Amazon FSx 및 FSLogix를 사용하여 Amazon AppStream 2.0에서 애플리케이션 설정 지속성 최적화를 참조하세요.

보안

개발자가 고려해야 하는 보안 측정에는 여러 가지가 있습니다. Windows 운영 체제, 애플리케이션 및 종속 항목에 대한 업데이트를 설치하고 유지 관리할 책임은 AppStream 사용자에게 있습니다. 기본 이미지를 최신 상태로 유지하는 방법에 대한 추가 지침은 AppStream 2.0 이미지를 최신으로 유지하기를 참조하여 기본 이미지를 최신 상태로 유지하는 방법에 대한 추가 지침을 참조하세요.

기본적으로 AppStream 2.0에서는 사용자 또는 애플리케이션이 이미지 애플리케이션 카탈로그에 지정된 것 이외의 모든 프로그램을 인스턴스에서 시작할 수 있습니다. 이는 애플리케이션이 워크플로의 일부로 다른 애플리케이션을 사용하지만 사용자가 종속 애플리케이션을 직접 시작하지 못하게 하려는 경우에 유용합니다. 예를 들어 애플리케이션은 애플리케이션 공급업체의 웹 사이트의 도움말 지침을 제공하기 위해 브라우저를 시작하지만 사용자가 브라우저를 직접 시작하지는 않도록 해야 합니다. 경우에 따라 스트리밍 인스턴스에서 실행할 수 있는 애플리케이션을 제어해야 할 수 있습니다. Microsoft AppLocker는 명시적 제어 정책을 사용하여 사용자가 실행할 수 있는 애플리케이션을 활성화하거나 비활성화하는 애플리케이션 제어 소프트웨어입니다.

바이러스 백신 소프트웨어는 스트리밍 세션 및 이미지 빌더 인스턴스에 부정적인 영향을 미칠 수 있습니다. AWS는 바이러스 백신 소프트웨어의 자동 업데이트를 활성화하지 않도록 권장합니다. Windows Defender에 대한 자세한 내용은 바이러스 백신 소프트웨어를 참조하세요.

성능

새 이미지를 만들기 전에 테스트 사용자로 애플리케이션을 테스트하는 것이 중요합니다. 테스트 사용자로 테스트하면 관리자가 아닌 사용자 컨텍스트에서도 애플리케이션을 실행할 수 있는지 확인할 수 있습니다. 또한 작업 관리자 및 성능 모니터와 같은 기본 제공 도구를 사용하여 애플리케이션 성능과 사용자 경험을 확인할 수 있습니다. CPU, 메모리, GPU 메모리와 같은 리소스 사용률을 모니터링하는 것이 가장 좋습니다. CPU, 메모리 또는 GPU 메모리 리소스 제약이 있는 경우 인스턴스 유형을 업그레이드해 보십시오. 성능을 확장하려면:

- 브라우저 팝업 창 비활성화
- 향상된 IE 보안 비활성화

AppStream 2.0 에이전트 버전 선택

새 이미지를 생성할 때 최신 AppStream 2.0 에이전트 소프트웨어를 사용하거나 업데이트하지 않도록 선택할 수 있습니다. AppStream 2.0 에이전트 소프트웨어의 각 버전에는 버그 수정 및 기능 향상이 포함되어 있습니다. 최신 소프트웨어를 사용해 이미지를 유지하세요. 이 문서의 이미지 업데이트 섹션에서 이에 대한 메커니즘을 검토하십시오.

최신 에이전트 사용 옵션을 선택할 수 있습니다. 이 옵션을 사용하면 시작 시 항상 최신 AppStream 2.0 에이전트가 설치됩니다. 하지만 예상치 못한 변경은 사용자 환경에 영향을 미칠 수 있으며 에이전트 업데이트로 인해 인스턴스 시작 시간이 늘어날 수 있습니다. 기본 이미지를 업데이트하려면 이미지를 다시 만들어야 합니다. 업데이트된 이미지를 프로덕션에 배포하기 전에 테스트를 수행하여 시작 시간을 최소화하는 것도 중요합니다.

Image Assistant 명령줄 인터페이스(CLI)

AppStream 2.0 이미지를 자동화하거나 프로그래밍 방식으로 생성하려는 개발자의 경우 Image Assistant CLI를 사용하십시오. 이 기능은 2019년 7월 26일 또는 그 이후에 출시된 AppStream 2.0 에이전트 소프트웨어가 설치된 이미지 빌더에서 사용할 수 있습니다. 다음의 대략적 개요에서는 프로그래밍 방식으로 AppStream 2.0 이미지를 생성하는 프로세스를 설명합니다.

1. 애플리케이션 설치 자동화를 사용하여 이미지 빌더에 필요한 애플리케이션을 설치합니다. 이 설치는 최종 사용자가 시작할 애플리케이션, 모든 종속성 및 백그라운드 애플리케이션을 포함할 수 있습니다.
2. 최적화할 파일 및 폴더를 결정합니다.
3. 해당될 경우, Image Assistant `add-application` CLI 작업을 사용하여 AppStream 2.0 이미지에 대한 애플리케이션 메타데이터 및 최적화 매니페스트를 지정합니다.
4. AppStream 2.0 이미지를 위한 추가 애플리케이션을 지정하려면 필요한 각 애플리케이션에 1~3단계를 반복합니다.
5. 해당될 경우, Image Assistant `update-default-profile` CLI 작업을 사용하여 기본 Windows 프로필을 덮어쓰고 최종 사용자용 기본 애플리케이션 및 Windows 설정을 생성합니다.
6. Image Assistant `create-image` CLI 작업을 사용하여 이미지를 생성합니다.

자세한 내용은 Image Assistant CLI 작업을 사용하여 프로그래밍 방식으로 AppStream 2.0 이미지 생성을 참조하세요.

사용자 스트리밍 환경 관리

세션 스크립트를 사용한 사용자 지정

AppStream 2.0은 인스턴스상 세션 스크립트를 제공합니다. 이러한 스크립트를 사용하여 사용자의 스트리밍 세션에서 특정 이벤트가 발생했을 때 자체 사용자 지정 스크립트를 실행할 수 있습니다. 예를 들어 사용자 지정 스크립트를 사용하여 사용자의 스트리밍 세션이 시작되기 전에 AppStream 2.0 환경을 준비할 수 있습니다. 또한 사용자 지정 스크립트를 사용하여 사용자가 스트리밍 세션을 완료한 후 스트리밍 인스턴스를 정리할 수도 있습니다.

AppStream 2.0 이미지 내에 세션 스크립트를 지정됩니다. 세션 스크립트 구성에 대한 자세한 내용은 세션 스크립트를 사용하여 사용자 환경 관리에 대한 관리 가이드 섹션을 참조하세요. 네트워크 공유 또는 AWS Identity and Access Management(IAM) 프로필과 함께 사용하면 세션 스크립트를 사용하여 스토리지 위치에서 추가 스크립팅을 검색할 수 있습니다. 이 추가 스크립팅을 사용하여 추가 사용자 경험 최적화를 실행할 수 있습니다. 이렇게 하면 사용자에게 애플리케이션 환경을 제공하는 데 필요한 이미지와 플릿의 수를 최소화할 수 있습니다.

Active Directory 그룹 정책 사용

Active Directory 도메인에서 AppStream 2.0 플릿을 사용하려는 경우 그룹 정책 객체(GPO)를 사용하여 사용자 환경을 관리할 수 있습니다. AppStream 2.0 인스턴스가 생성되는 조직 단위(OU)에 GPO를 할당할 수 있습니다. 이미지 생성을 단순화하려면 상속을 차단하는 OU에서 기본 AppStream 2.0 이미지를 시작하십시오. 이렇게 하면 AppStream 2.0 사용자 경험에 영향을 미치는 다른 도메인 정책이 방지됩니다. 고유한 GPO를 사용하여 각 플릿을 전용 OU에 배포하면 AppStream 2.0 이미지 관리의 일대다 통합 이점을 누릴 수 있는 환경을 구축할 수 있습니다.

그룹 정책을 사용하는 예로는 각 AppStream 2.0 플릿에 대해 서로 다른 Internet Explorer 홈 페이지의 이미지 세트를 지정하는 경우를 들 수 있습니다.

이미지 업데이트

소프트웨어 패치는 컴퓨팅 리소스의 보안 및 성능에 매우 중요합니다. Well-Architected 프레임워크의 보안 원칙에는 잦은 패치 적용이 모범 사례로 나열되어 있습니다.

이미지를 빌드하고 배포할 때 AppStream 2.0 이미지에 패치가 필요한 네 가지 범주의 소프트웨어가 있습니다.

- 애플리케이션 및 종속성 — 이미지의 애플리케이션 및 종속 항목에 대한 패치는 사용자의 책임입니다.

- Microsoft Windows 운영 체제 — Windows 업데이트를 설치하고 유지 관리하는 것은 사용자의 책임입니다.
- 소프트웨어 구성 요소 — AppStream 2.0 작업에 필요한 드라이버, 에이전트 및 기타 소프트웨어(예: Amazon CloudWatch 에이전트)입니다. AppStream 2.0은 새 에이전트와 드라이버가 포함된 새 기본 이미지를 정기적으로 릴리스합니다. 최신 베이스를 사용하여 이미지를 재빌드하여 이미지의 소프트웨어 구성 요소를 최신 베이스라인으로 가져올 수 있습니다. 애플리케이션이 많거나 애플리케이션 설치가 복잡한 경우 최신 기반으로 이미지를 재구축하는 프로세스는 시간이 많이 걸리고 번거로울 수 있습니다.
- AppStream 2.0 에이전트 - Image Assistant에서 항상 최신 에이전트 버전 사용을 선택할 수 있습니다. 이 옵션을 사용하면 이미지에서 시작되는 스트리밍 인스턴스가 자동으로 최신 버전의 에이전트를 사용합니다.

다음 중 하나를 수행하여 AppStream 2.0 이미지를 최신 상태로 유지할 수 있습니다.

- 관리형 AppStream 2.0 이미지 업데이트를 사용하여 이미지 업데이트 – 이 업데이트 방법은 최신 Windows 운영 체제 업데이트 및 드라이버 업데이트와 최신 AppStream 2.0 에이전트 소프트웨어를 제공합니다. 이 관리형 방법은 서비스 및 Microsoft 운영 체제 구성 요소를 업데이트하지만 애플리케이션 구성 요소를 업데이트할 수는 없습니다. 애플리케이션 설치가 복잡하거나 수동 구성이 필요한 경우에는 이 방법을 사용하는 것이 가장 좋습니다.
- 관리형 AppStream 2.0 이미지 버전을 사용하여 AppStream 2.0 에이전트 소프트웨어 업데이트 - 이 업데이트 방법은 최신 AppStream 2.0 에이전트 소프트웨어를 제공합니다. 이 방법을 사용하면 애플리케이션 구성 요소를 업데이트할 수 있습니다.

플릿 사용자 지정

플릿 유형

플릿을 생성할 때 고객은 플릿 유형을 선택해야 합니다. 각 플릿 유형은 사용자 경험, 비용 및 유지 관리 오버헤드에 대해 서로 다른 이점을 제공합니다. 선택한 플릿 유형에 관계없이 각 옵션은 Windows 및 Linux 플랫폼 유형과 데스크톱 보기 또는 애플리케이션 보기를 모두 지원합니다.

고객은 이제 다음 플릿 유형 중에서 선택할 수 있습니다.

- 상시 작동 — 이 플릿 유형은 사용자에게 앱에 대한 즉각적인 액세스 권한을 제공합니다. 사용자가 앱을 스트리밍하지 않아도 플릿에서 실행 중인 모든 인스턴스에 대해 요금이 청구됩니다.
- 온디맨드 — 스트리밍 비용을 최적화하려면 이 플릿 유형을 선택하십시오. 온디맨드 플릿을 사용하면 사용자는 세션 시작 시간이 약 1~2분 정도 걸립니다. 하지만 스트리밍 인스턴스 요금은 사용자가 연결된 경우에만 부과되며, 스트리밍 앱이 아닌 플릿의 각 인스턴스에 대해서는 소액의 시간당 요금이 부과됩니다.
- 탄력적 — 탄력적 플릿은 설치가 필요하지 않고 가상 하드 디스크(VHD)에서 실행할 수 있는 애플리케이션에 사용할 수 있습니다. 탄력적 플릿은 AppStream 2.0 이미지를 지원하지 않으며 규모 조정 정책도 필요하지 않습니다. 스트리밍 세션 기간에 대해서만 청구됩니다.

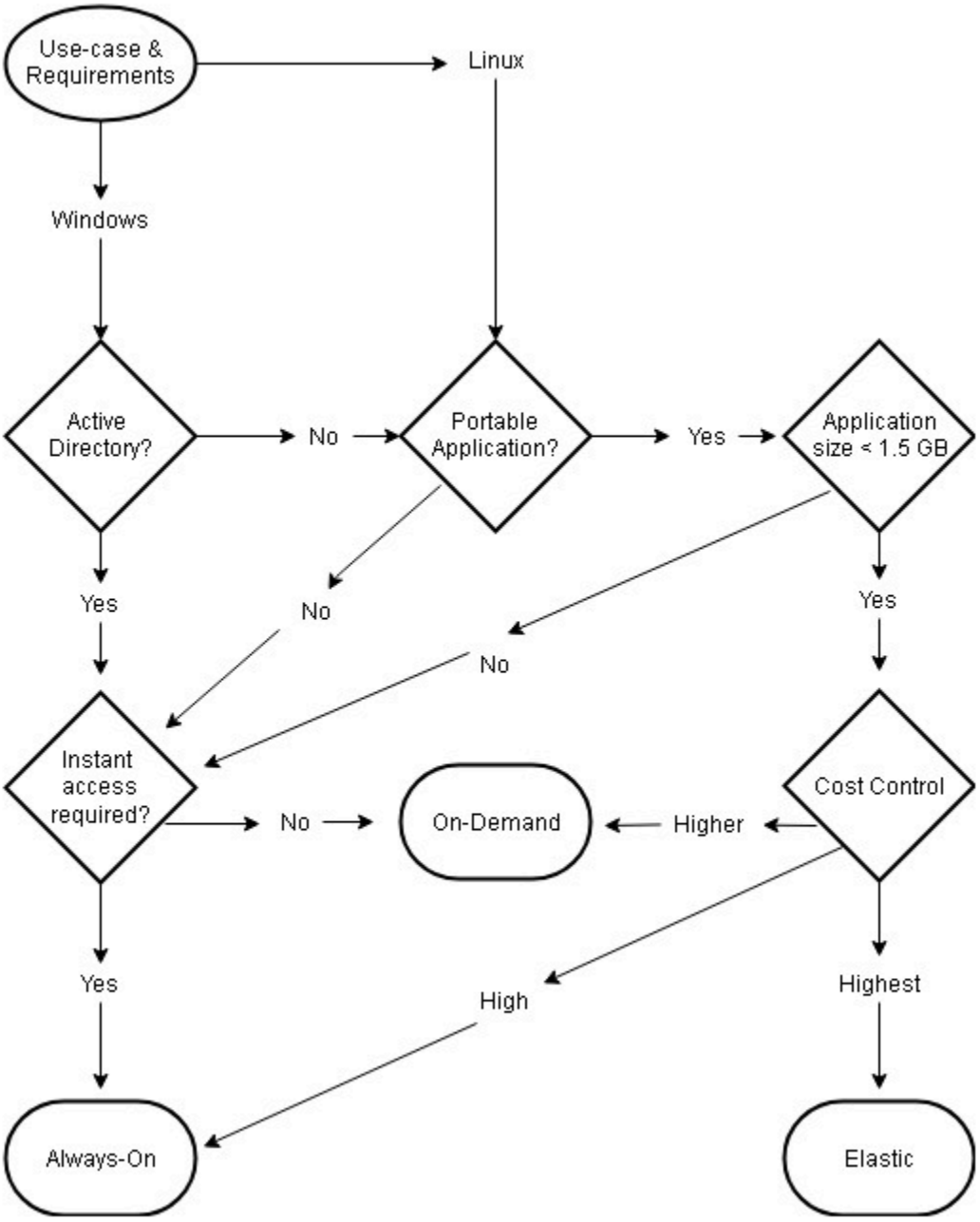
표 2 - Amazon AppStream 2.0 플릿 유형

플릿 유형	사용해야 하는 경우	사용자 경험	요금 모델	주의
상시 작동	사용자는 세션을 시작할 때 애플리케이션에 즉시 액세스할 수 있어야 합니다. 사용 패턴을 예측할 수 있고 규모 조정 정책을 통해 비용을 안정적으로 제어할 수 있기 때	애플리케이션에 대한 즉각적인 액세스	플릿에서 사용 가능한 모든 인스턴스에 대해 전체 요금을 지불합니다(세션에 사용되는지 여부와 관계없음).	사용자 지정 이미지 및 규모 조정 정책을 지원합니다.

플릿 유형	사용해야 하는 경우	사용자 경험	요금 모델	주의
	문에 플릿에 상당한 초과 용량이 없을 것입니다.			
온디맨드	플릿에 상당한 초과 용량을 유지해야 합니다. 가장 비용 최적화된 환경을 원하며 사용하지 않은 용량에 대해 정가를 지불하고 싶지 않습니다. 사용자는 세션을 시작한 후 1~2분 정도 기다려서 애플리케이션에 액세스할 수 있습니다. 더 큰 인스턴스 유형을 사용하고 있습니다. 실행 중인 인스턴스의 시간당 비용은 중지된 인스턴스 요금보다 훨씬 비쌉니다.	사용자는 세션을 시작한 후 애플리케이션에 액세스할 때까지 1~2분 정도 기다립니다.	활성 세션이 있는 스트리밍 인스턴스의 경우에만 정가를 지불하고, 유휴 인스턴스의 경우 소액의 시간당 요금을 지불합니다.	사용자 지정 이미지 및 규모 조정 정책을 지원합니다.

플릿 유형	사용해야 하는 경우	사용자 경험	요금 모델	주의
탄력적	애플리케이션과 해당 종속 항목이 최대 1.5GB보다 작습니다. 사용자가 탄력적 플릿에서 세션을 시작할 때마다 Amazon S3에서 세션으로 가상 하드 디스크(VHD) 파일을 다운로드해야 합니다. 따라서 VHD 파일이 커지면(예: 1.5GB 초과) 최종 사용자 경험이 저하됩니다. 애플리케이션은 이식 가능합니다. 즉, 애플리케이션과 모든 종속 항목을 VHD에 배치하고 VHD에서 시작할 수 있습니다. 도메인에 조인된 스트리밍 인스턴스는 필요하지 않습니다(현재 탄력적 플릿에서는 도메인 가입을 사용할 수 없습니다). 활성 세션에 대해서만 비용을 지불하고 싶습니다(즉, 플릿	사용자는 세션을 시작한 후 애플리케이션에 액세스할 때까지 45초에서 3분 정도 기다립니다(대기 시간은 가상 하드 디스크 크기에 따라 다름).	스트리밍 세션 기간에 대해서만 청구됩니다. 탄력적 플릿에는 유휴 인스턴스라는 개념이 없으므로 사용하지 않은 인스턴스에 대해서는 요금이 부과되지 않습니다.	사용자 지정 이미지(고객이 애플리케이션과 함께 VHD를 제공) 또는 규모 조정 정책을 지원하지 않습니다. 현재 `stream.standard.small` 및 `stream.standard.medium` 인스턴스를 지원합니다. 사용 사례에 다른 인스턴스 유형이 필요한 경우 AWS 계정 팀에 문의하세요.

플릿 유형	사용해야 하는 경우	사용자 경험	요금 모델	주의
	에서 사용하지 않은 용량에 대해서는 비용을 지불하지 않음). 사용자는 세션을 시작한 후 애플리케이션에 액세스하는 데 45초 이상 기다릴 수 있습니다. AWS에서 규모 조정을 관리하기를 원합니다(관리할 규모 조정 정책 없음).			



플릿 유형 사용 사례 및 요구 사항

플릿 크기 조정

최소 용량 및 예약된 규모 조정

AppStream 2.0 플릿의 크기를 조정할 때는 사용자 경험과 비용으로 바로 이어지는 몇 가지 고려 사항이 있습니다. 최소 용량에 입력한 값을 사용하면 AppStream 2.0 인스턴스 수가 이 값보다 적은 경우가

거의 없습니다. AppStream 2.0 세션이 종료된 후 총 AppStream 2.0 인스턴스가 최소 용량 값보다 작으면 새 플릿 인스턴스가 시작됩니다. 항상 그렇듯이 하나의 AppStream 2.0 인스턴스가 하나의 사용자 세션에 직접 매핑되어 최소 용량 값에 직접적인 영향을 미친다는 점을 기억해야 합니다.

예상되는 동시 항목을 초과하는 최소 용량 값을 입력하면 사용자 환경에는 영향을 미치지 않지만 비용이 증가하게 됩니다. 값이 너무 낮으면 비용이 절감되지만 총 요청이 가용 용량을 초과할 경우 사용자 경험에 영향을 미칩니다. 이러한 유형의 상황에서 관리자에게 "용량 부족" 오류가 표시됩니다. 예를 들어, `PendingCapacity`가 `AvailableCapacity`가 될 때까지 기다리는 경우 하루 시작 시 예상 연결 수가 예측 가능한 일관된 값일 때 사용자의 시간을 비효율적으로 사용하게 됩니다.

일반적으로 사용량이 적은 시간을 수용할 수 있는 최소 용량으로 시작한 다음 예약된 규모 조정 정책을 사용하여 근무일이 시작되기 전에 최소 용량을 효과적으로 재설정하십시오. 최소 용량을 사용량이 적은 시간으로 되돌리려면 또 다른 예약된 조정 정책을 만들어야 합니다. 규모 조정 정책 및 구현 방법에 대한 자세한 내용은 이 문서의 플릿 Auto Scaling 전략 섹션을 참조하세요.

최대 용량 및 서비스 할당량

최대 용량을 설정하는 경우 임의의 값처럼 보일 수 있지만 적절하게 예측하고 설정하면 총 리소스 소비량과 비용을 최적화할 수 있습니다. 입력한 값이 AppStream 2.0 플릿의 서비스 할당량보다 높을 경우 AWS 계정이 유효한 것으로 보이지만, Auto Scaling 이벤트가 리소스를 최대 용량으로 확대하려고 시도하면 최대 용량 값이 사용 가능한 서비스 할당량을 초과하므로 이벤트가 시작되지 않습니다. 조직에서 예상한 대로 자동 규모 조정 기능을 사용할 수 있도록 하려면 원하는 최대 용량에 대한 서비스 할당량 요청을 제출해야 합니다.

최대 용량 값을 설정할 때 고려해야 할 또 다른 중요한 사항은 비용입니다. 자세한 내용은 이 문서의 플릿 유형 선택을 통한 비용 최적화 섹션을 참조하세요.

데스크톱 뷰 또는 애플리케이션 뷰 선택

애플리케이션 뷰 또는 데스크톱 뷰 선택 여부는 성능이나 비용에 영향을 미치지 않습니다. AppStream 2.0 플릿당 언제든지 하나의 뷰에만 액세스할 수 있습니다. 스트림 뷰 옵션을 변경할 수 있습니다. 스트림 뷰를 변경하려면 플릿을 다시 시작해야 하므로 사용량이 적은 업무 시간에 이 변경을 계획하세요.

스트림 뷰에 대한 단일 모범 사례는 없습니다. 스트림 뷰 옵션의 영향은 다음을 통해 요약됩니다.

- 관리자를 위한 사용량 보고서 기능을 통해 애플리케이션 사용에 대한 세부 보고
- 최종 사용자를 위한 전반적인 경험 및 워크플로(예: 전체 데스크톱이 사용 사례의 요구 사항을 해결하는지 아니면 애플리케이션을 보는 것만으로 충분할까요?).

데스크톱 뷰

모든 사용자 워크플로가 세션에서 수행되는 사용 사례의 경우 데스크톱 뷰는 모든 애플리케이션이 하나의 환경에 집중되도록 하여 사용자 환경을 단순화합니다. 데스크톱 뷰는 운영 체제 (OS)와의 통합이 필요한 3~5개 이상의 애플리케이션을 배포할 때 보다 일관된 사용자 환경을 제공할 수 있습니다. 데스크톱 뷰는 분리되고 서로 다른 두 환경을 유지 관리할 때 효과적입니다. 예를 들어 사용자는 프로덕션 데스크톱 환경과 사전 프로덕션 데스크톱 환경 모두에 동시에 액세스하여 레이아웃, 구성 및 애플리케이션 액세스에 대한 변경 사항을 검증할 수 있습니다.

AppStream 2.0 사용 보고서는 데스크톱 뷰에 대한 일일 애플리케이션 보고서를 생성합니다. 애플리케이션의 결과 출력은 단순히 AppStream 2.0 세션에 직접 매핑되는 '데스크톱'입니다. 자세한 내용은 이 문서의 사용자 사용 모니터링 섹션을 참조하세요.

애플리케이션 전용 뷰

애플리케이션 전용 뷰는 AppStream 2.0 스택이 간헐적으로 필요한 몇 가지 애플리케이션을 제공하기 위한 경우에도 효과적입니다. 키오스크 환경에서는 애플리케이션 뷰를 통해 안전하게 잠긴 애플리케이션 전송을 제공합니다. 애플리케이션 뷰를 사용하면 AppStream 2.0이 기본 Windows 셸을 사용자 지정 셸로 대체합니다. 이 사용자 지정 셸은 실행 중인 애플리케이션만 표시하므로 OS의 공격 범위를 최소화합니다.

AppStream 2.0을 사용하여 기존 조직의 데스크톱 환경을 보강하는 사용 사례의 경우 애플리케이션 전용 뷰가 선호됩니다. AppStream 2.0 Windows 클라이언트를 기본 애플리케이션 모드에서 배포하여 키보드 단축키를 모두 사용할 수 있도록 하여 사용자 혼란을 최소화합니다.

Amazon 2.0 사용 보고서는 데스크톱 뷰에 대한 일일 애플리케이션 보고서를 생성합니다. 애플리케이션 및 실행 사용에 대한 보다 세밀한 보고를 원하면 운영 체제 수준에서 보고하는 타사 솔루션을 고려해 보세요. 보고 모드에서 Microsoft AppLocker를 사용하거나 Liquidware의 Stratusphere UX와 같이 AWS Marketplace에서 사용할 수 있는 솔루션을 고려할 수 있습니다.

AWS Identity and Access Management 역할 구성

워크로드에서 AppStream 2.0 최종 사용자가 세션 내에서 다른 AWS 서비스에 액세스해야 하는 경우 AWS Identity and Access Management (IAM) 역할)을 사용하여 액세스를 위임하는 것이 좋습니다. 플릿 수준의 할당을 통해 IAM 역할을 최종 사용자 세션에 직접 연결할 수 있습니다. AppStream 2.0에서 IAM 역할을 사용할 때의 추가 모범 사례는 관리자 안내서의 이 섹션을 참조하세요.

정적 보안 인증 사용

일부 워크로드의 경우 IAM 액세스 키를 연결된 역할에서 상속하는 대신 정적 입력이 필요할 수 있습니다. 이러한 자격 증명을 받는 방법은 두 가지입니다. 첫 번째 방법은 액세스 키를 AWS 서비스 내에 저장한 다음 최종 사용자에게 서비스에서 해당 특정 값을 가져올 수 있는 명시적인 IAM 액세스 권한을 부여하는 것입니다. 액세스 키 저장 메커니즘의 두 가지 예로는 AWS Secrets Manager 또는 AWS SSM 파라미터 스토어를 사용하는 경우를 들 수 있습니다. 두 번째 방법은 AppStream 2.0 자격 증명 공급자를 사용하여 연결된 역할의 액세스 키에 액세스하는 것입니다. 자격 증명 공급자를 호출하고 액세스 키와 비밀 키의 출력을 파싱하여 이 작업을 수행할 수 있습니다. PowerShell 내에서 이 작업을 수행하는 방법의 예는 다음과 같습니다.

```
$CMD = 'C:\Program Files\Amazon\Photon\PhotonRoleCredentialProvider
\PhotonRoleCredentialProvider.exe'
$role = 'Machine'

$output = & $CMD --role=$role
$parsed = $output | ConvertFrom-Json

$access_key = $parsed.AccessKeyId
$secret_key = $parsed.SecretAccessKey
$session_token = $parsed.SessionToken
```

AppStream 2.0 S3 버킷 보호

AppStream 2.0 워크로드가 홈 폴더 및/또는 애플리케이션 지속성으로 구성된 경우 영구 데이터가 저장되는 Amazon S3 버킷이 무단으로 액세스되거나 실수로 삭제되지 않도록 보호하는 것이 가장 좋습니다. 첫 번째 보호 계층은 Amazon S3 버킷 정책을 추가하여 실수로 버킷을 삭제하지 않도록 하는 것입

니다. 두 번째 보호 계층은 최소 권한 원칙에 부합하는 버킷 정책을 추가하는 것입니다. 필요한 당사자에게만 버킷 액세스를 허용함으로써 원칙을 준수할 수 있습니다.

플릿 Auto Scaling 전략

AppStream 2.0 인스턴스에 대한 이해

AppStream 2.0 플릿 인스턴스의 사용자 대 플릿 인스턴스 비율은 1:1 입니다. 즉, 각 사용자가 고유한 스트리밍 인스턴스를 갖게 됩니다. 동시에 연결하는 사용자 수에 따라 플릿 규모가 결정됩니다.

조정 정책

Application Auto Scaling 그룹에서 AppStream 2.0 플릿을 시작합니다. 이를 통해 사용량에 따라 플릿을 규모 조정하여 수요를 충족할 수 있습니다. 사용량이 증가하면 플릿이 스케일 아웃되고 사용자가 연결을 끊으면 플릿이 다시 스케일 인됩니다. 이는 규모 조정 정책을 설정하여 제어합니다. 예약된 규모 조정 정책, 단계적 규모 조정 정책 및 대상 추적 규모 조정 정책을 설정할 수 있습니다. 이러한 규모 조정 정책에 대한 자세한 내용은 Amazon AppStream 2.0용 플릿 Auto Scaling을 참조하세요.

단계적 조정

이러한 정책은 현재 플릿 크기 또는 특정 인스턴스 수의 백분율만큼 플릿 용량을 늘리거나 줄입니다. 단계적 규모 조정 정책은 `Capacity Utilization`, `Available Capacity` 또는 `Insufficient Capacity Errors`의 AppStream 2.0 CloudWatch 지표에 의해 트리거됩니다.

단계적 규모 조정 정책을 사용할 때는 AWS는 고정된 인스턴스 수가 아닌 일정 비율의 용량을 추가하도록 권장합니다. 이렇게 하면 규모 조정 작업이 플릿 크기에 비례하도록 할 수 있습니다. 플릿 크기에 비해 인스턴스 수가 적기 때문에 너무 느리게 스케일 아웃하거나 플릿 규모가 작을 때 인스턴스를 너무 많이 추가하는 상황을 방지하는 데 도움이 됩니다.

대상 추적

이 정책에서는 플릿의 용량 사용률 수준을 지정합니다. Application Auto Scaling은 규모 조정 정책을 트리거하는 CloudWatch 경보를 생성 및 관리합니다. 이렇게 하면 용량이 추가하거나 제거하여 플릿을 지정한 목표 값으로 또는 목표 값에 가깝게 유지합니다. 애플리케이션 가용성을 보장하기 위해 플릿은 가능한 한 빨리 지표에 비례하여 스케일 아웃되고 더 서서히 스케일 인됩니다. 목표 추적을 구성할 때는 규모 조정 쿨다운 고려하여 스케일 아웃 및 스케일 인이 원하는 간격으로 이루어지도록 하십시오.

목표 추적은 이탈률이 높은 상황에 효과적입니다. 이탈은 많은 사용자가 짧은 시간 내에 세션을 시작하고 종료할 때 발생합니다. 플릿의 CloudWatch 지표를 검토하여 이탈을 식별할 수 있습니다. 원하는 용량의 변경 없이 (또는 거의 변동이 없는) 플릿의 보류 용량이 0이 아닌 기간이면 이탈률이 높을 가능성

이 높습니다. 이탈률이 높은 상황에서는 15분 기간의 이탈률(100 — 목표 사용률)을 초과하는 목표 추적 정책을 구성하십시오. 예를 들어 사용자 이직으로 인해 플릿의 10%가 15분 내에 중단될 경우 높은 이탈률을 상쇄하기 위해 용량 사용률 목표를 90% 이하로 설정하세요.

예약된 규모 조정

이러한 정책을 통해 시간 기반 일정에 따라 원하는 플릿 용량을 설정할 수 있습니다. 이 정책은 로그인 동작을 이해하고 수요 변화를 예측할 수 있을 때 효과적입니다.

예를 들어, 영업일이 시작될 때 오전 9시에 동시에 스트리밍 연결을 요청하는 사용자가 100명 있다고 예상할 수 있습니다. 오전 8시 40분에 최소 플릿 크기를 100으로 설정하도록 스케줄 기반 규모 조정 정책을 구성할 수 있습니다. 이렇게 하면 플릿 인스턴스를 생성하여 근무일 시작 시 사용할 수 있으며 100명의 사용자가 동시에 연결할 수 있습니다. 그런 다음 다른 예정된 정책을 설정하여 오후 5시에 플릿을 최소 10개로 스케일 인할 수 있습니다. 이렇게 하면 근무 시간 이후 세션에 대한 수요가 근무일 중보다 적기 때문에 비용을 절약할 수 있습니다.

프로덕션 환경에서의 규모 조정 정책

다양한 유형의 규모 조정 정책을 단일 플릿에 결합하여 사용자 행동에 맞는 정확한 규모 조정 정책을 정의할 수 있습니다. 이전 예시에서는 예약된 규모 조정 정책을 대상 추적 또는 단계별 규모 조정 정책과 결합하여 특정 수준의 사용률을 유지할 수 있습니다. 예약된 규모 조정과 대상 추적 규모 조정을 함께 사용하면 용량이 즉시 필요할 때 사용률 수준이 급격히 증가하는 영향을 줄일 수 있습니다.

규모 조정 정책으로 인해 원하는 인스턴스 수가 변경될 때 스트리밍 세션에 연결된 사용자는 스케일 인 또는 스케일 아웃의 영향을 받지 않습니다. 규모 조정 정책으로 인해 기존 스트리밍 세션이 종료되지는 않습니다. 기존 세션은 사용자 또는 플릿 타임아웃 정책에 따라 세션이 종료될 때까지 중단 없이 계속됩니다.

CloudWatch 지표로 AppStream 2.0 사용을 모니터링하면 시간이 지남에 따라 규모 조정 정책을 최적화하는 데 도움이 될 수 있습니다. 예를 들어 초기 설정 중에 리소스를 과도하게 프로비저닝하는 것이 일반적이며 장기간 사용률이 낮아질 수 있습니다. 또는 플릿이 충분히 프로비저닝되지 않은 경우 용량 사용률이 높고 “용량이 충분하지 않음” 오류가 발생할 수 있습니다. CloudWatch 지표를 검토하면 규모 조정 정책을 조정하여 이러한 오류를 완화하는 데 도움이 될 수 있습니다. 자세한 내용과 사용할 수 있는 AppStream 2.0 규모 조정 정책의 예는 Amazon AppStream 2.0 플릿 규모 조정을 참조하세요.

조정 정책 설계 모범 사례

조정 정책 결합

많은 고객이 AppStream 2.0에서 Auto Scaling의 성능과 유연성을 높이기 위해 다양한 유형의 조정 정책을 단일 플릿으로 결합하기로 선택합니다. 예를 들어, 사용자가 근무일을 시작할 것으로 예상하여 오전 6시에 플릿 최소값을 늘리고, 사용자가 작업을 중단하기 전인 오후 4시에 플릿 최소값을 낮추도록 예약된 조정 정책을 구성할 수 있습니다. 이 예약된 규모 조정 정책을 대상 추적 또는 단계별 규모 조정 정책과 결합하여 하루 중 특정 수준의 사용률을 유지하고 사용량을 스케일 인하거나 스케일 아웃하여 급증하는 사용량을 처리할 수 있습니다. 예약된 규모 조정과 대상 추적 규모 조정을 함께 사용하면 용량이 즉시 필요할 때 사용률 수준이 급격히 증가하는 영향을 줄일 수 있습니다.

조정 이탈 방지

사용 사례로 인해 플릿에 높은 이탈이 발생할 수 있는지 생각해 보세요. 이탈은 많은 사용자가 짧은 시간 내에 세션을 시작하고 종료할 때 발생합니다. 이는 많은 사용자가 로그오프하기 전에 단 몇 분 동안 플릿의 애플리케이션에 동시에 액세스하는 경우 발생할 수 있습니다.

이러한 상황에서는 사용자가 세션을 종료하면 인스턴스가 종료되므로 플릿 크기가 원하는 용량보다 훨씬 아래로 떨어질 수 있습니다. 단계별 조정 정책으로 인해 이탈을 상쇄할 만큼 빠르게 인스턴스를 추가하지 못할 수 있으며, 그 결과 플릿이 특정 크기로 정체될 수 있습니다.

플릿의 CloudWatch 지표를 검토하여 이탈을 식별할 수 있습니다. 원하는 용량의 변경 없이 (또는 거의 변동이 없는) 플릿의 보류 용량이 0이 아닌 기간이면 이탈률이 높을 가능성이 높습니다. 이탈률이 높은 상황을 고려하려면 목표 추적 조정 정책을 사용하고 15분 동안 (100 — 목표 사용률)이 이탈률을 초과하도록 목표 사용률을 선택하세요. 예를 들어 사용자 이직으로 인해 플릿의 10%가 15분 내에 중단될 경우 높은 이탈률을 상쇄하기 위해 용량 사용률 목표를 90% 이하로 설정하세요.

최대 프로비저닝 속도 이해

사용자 수가 많은 AppStream 2.0 플릿을 관리하는 고객은 프로비저닝 속도 제한을 고려해야 합니다. 이 한도는 플릿 또는 AWS 계정 내 모든 플릿에 인스턴스를 추가할 수 있는 속도에 영향을 줍니다.

고려해야 할 한도는 두 가지입니다.

- 단일 플릿의 경우 AppStream 2.0은 분당 최대 20개의 인스턴스를 프로비저닝합니다.

- 단일 AWS 계정의 경우 AppStream 2.0은 분당 60개 인스턴스 (분당 100개 인스턴스 버스트)의 속도로 프로비저닝합니다.

3개 이상의 플릿을 병렬로 스케일 아웃할 경우 계정 프로비저닝 속도 제한은 이러한 플릿 전체에 공유됩니다. 예를 들어, 병렬로 스케일 인되는 6개의 플릿은 각각 분당 최대 10개의 인스턴스를 프로비저닝할 수 있습니다. 또한 조정 이벤트에 대한 응답으로 특정 스트리밍 인스턴스가 프로비저닝을 완료하는 데 걸리는 시간도 고려하세요. Active Directory 도메인에 가입되지 않은 플릿의 경우 이 시간은 일반적으로 15분입니다. Active Directory 도메인에 가입된 플릿의 경우 최대 25분이 소요될 수 있습니다.

이러한 제약 조건이 있는 경우 다음 예제를 고려해 보세요.

- 단일 플릿을 0개에서 1000개 인스턴스로 규모 조정하려는 경우 프로비저닝이 완료되는 데 50분(인스턴스 1000개/분당 인스턴스 20개)이 걸리고, 최종 사용자가 모든 인스턴스를 사용할 수 있게 되려면 15~25분이 추가로 소요되며 총 65~75분이 소요됩니다.
- 단일 플릿을 0개에서 333개 인스턴스로 규모 조정하려는 경우(AWS 계정에서 총 999개 인스턴스의 경우) 프로비저닝이 완료되는 데 17분(인스턴스 999개/분당 인스턴스 60개)이 걸리고, 최종 사용자가 모든 인스턴스를 사용할 수 있게 되려면 15분이 추가로 소요되며 총 32~42분이 소요됩니다.

복수 가용 영역 활용

플릿 배포를 위해 리전에서 여러 AZ를 선택하세요. 플릿에 대해 여러 AZ를 선택하면 조정 이벤트에 대한 응답으로 플릿이 인스턴스를 추가할 수 있는 가능성이 높아집니다. CloudWatch 지표 PendingCapacity는 대규모 플릿 배포에서 플릿 AZ 설계가 얼마나 최적화되었는지 평가하는 출발점입니다. PendingCapacity 값이 지속적으로 높다는 것은 수평(AZ 간) 확장을 확장해야 한다는 의미일 수 있습니다. 자세한 내용은 Amazon AppStream 2.0 리소스 모니터링을 참조하세요.

예를 들어 Auto Scaling에서 플릿 크기를 늘리기 위해 인스턴스를 프로비저닝하려고 하는데 선택한 AZ의 용량이 충분하지 않은 경우 Auto Scaling은 대신 플릿에 지정한 다른 AZ에 인스턴스를 추가합니다. 가용 영역 및 AppStream 2.0 설계에 대한 자세한 내용은 이 문서의 가용 영역을 참조하세요.

용량 부족 오류 지표 모니터링

“용량 부족 오류”는 AppStream 2.0 플릿에 대한 CloudWatch 지표입니다. 이 지표는 용량 부족으로 인해 거부된 세션 요청 수를 지정합니다.

조정 정책을 변경할 때 용량 부족 오류가 발생할 경우 알려주는 CloudWatch 경보를 생성하면 도움이 됩니다. 이를 통해 조정 정책을 신속하게 조정하여 사용자의 가용성을 최적화할 수 있습니다. 관리 가이드에서는 AppStream 2.0 리소스를 모니터링하는 자세한 단계를 제공합니다.

연결 메서드

AppStream 2.0에서 세션을 스트리밍할 때 사용자는 다음 두 가지 연결 방법을 사용할 수 있습니다.

- 웹 브라우저 액세스 - 모든 HTML5 지원 브라우저가 지원됩니다. 플러그인이나 다운로드가 필요하지 않습니다.
- AppStream 2.0 Windows 클라이언트

가장 좋은 방법은 사용자 사용 사례에 맞는 기능 및 디바이스 요구 사항을 고려하여 요구 사항을 가장 잘 지원하는 브라우저 또는 디바이스를 조정하는 것입니다.

> **Note**
>
> AppStream 2.0은 화면 해상도가 1,024x768 픽셀보다 낮은 디바이스에서는 지원되지 않습니다.

기능 및 디바이스 지원 요약

표 3 — 기능 및 디바이스 지원 요약

	웹 브라우저 액세스	AppStream 2.0 Windows 클라이언트
다중 모니터(최대 2K 해상도)	지원	지원
다중 모니터(최대 4K 해상도)	해당 사항 없음	지원
드로잉 태블릿 지원	지원*	지원
터치스크린 디바이스 지원	지원	해당 사항 없음
USB 패스스루 디바이스 지원	해당 사항 없음	지원
키보드 바로 가기	지원	지원
상대 마우스 오프셋	지원	지원

	웹 브라우저 액세스	AppStream 2.0 Windows 클라이언트
파일 전송	지원	지원
로컬 프린터 리디렉션	해당 사항 없음	지원
로컬 드라이브 리디렉션	해당 사항 없음	지원
웹 캠 지원	지원	지원

*Google Chrome 및 Mozilla Firefox만 해당

웹 브라우저 액세스

AppStream 2.0 웹 브라우저 액세스를 통해 전용 클라이언트를 설치할 필요 없이 애플리케이션에 액세스할 수 있습니다. 사용자는 지원되는 HTML5 지원 브라우저를 사용하여 연결할 수 있습니다. 브라우저 플러그인이나 확장 프로그램은 필요하지 않습니다.

웹 브라우저 액세스를 통해 다양한 최종 디바이스 운영 체제 및 유형을 선택할 수 있습니다.

Windows용 AppStream 2.0 클라이언트

Windows용 AppStream 2.0 클라이언트는 Windows PC에 설치하는 애플리케이션입니다. 이 애플리케이션은 웹 브라우저로 AppStream 2.0에 액세스할 때 사용할 수 없는 추가 기능을 제공합니다. 예를 들어 AppStream 클라이언트는 다음을 지원합니다.

- 3대 이상의 모니터 또는 4K 해상도 사용
- AppStream 2.0을 통해 스트리밍되는 애플리케이션에 USB 디바이스 사용
- 스트리밍 세션 중에 로컬 드라이브 및 폴더 액세스
- 스트리밍 애플리케이션에서 로컬 컴퓨터에 연결된 프린터로 인쇄 작업 리디렉션
- 스트리밍 세션 내에서 화상 및 음성 회의에 로컬 웹캠 사용
- 스트리밍 세션 중에 액세스하는 애플리케이션의 키보드 단축키 사용
- 로컬에 설치된 애플리케이션과 거의 동일한 방식으로 원격 스트리밍 애플리케이션 사용

AppStream 2.0 클라이언트 연결 모드

AppStream 2.0 클라이언트는 네이티브 애플리케이션 모드와 클래식 모드의 두 가지 연결 모드를 제공합니다. 선택한 연결 모드에 따라 애플리케이션 스트리밍 중에 사용할 수 있는 옵션과 스트리밍 애플리케이션의 작동 및 표시 방법이 결정됩니다. 관리자는 사용자가 네이티브 애플리케이션 모드와 클래식 모드 사이를 전환할 수 있도록 제어할 수 있습니다.

- 클래식 모드는 AppStream 2.0 세션 창에서 애플리케이션을 스트리밍합니다. 이는 최종 사용자가 웹 브라우저에서 애플리케이션을 스트리밍하는 방식과 유사합니다. 최종 사용자가 브라우저와 동일한 방식으로 애플리케이션을 스트리밍하고 로컬 파일 연결 및 프린터 리디렉션과 같은 추가 기능을 사용하려는 경우 클래식 모드를 사용하십시오. 권장되는 기본 연결 모드는 클래식 모드입니다. 클래식 모드는 데스크톱 뷰에서 지원되는 유일한 모드입니다.
- 네이티브 애플리케이션 모드를 사용하면 최종 사용자가 로컬에 설치된 다른 애플리케이션과 비슷한 방식으로 원격 스트리밍 애플리케이션을 사용할 수 있습니다. 최종 사용자가 로컬에 설치된 애플리케이션을 사용하는 데 익숙하다면 네이티브 애플리케이션 모드를 사용하면 원활한 환경을 제공할 수 있습니다. 원격 스트리밍 애플리케이션은 로컬에 설치된 애플리케이션과 거의 동일한 방식으로 작동합니다. 로컬 애플리케이션의 아이콘과 마찬가지로 원격 스트리밍 애플리케이션 아이콘이 로컬 PC의 작업 표시줄에 표시됩니다. 로컬 애플리케이션의 아이콘과 달리 네이티브 애플리케이션 모드의 스트리밍 애플리케이션 아이콘에는 AppStream 2.0 로고가 포함됩니다. 네이티브 애플리케이션 모드는 사용자가 애플리케이션 키보드 단축키를 사용하고, 키보드 단축키를 사용하여 개별 로컬 애플리케이션과 개별 원격 애플리케이션 간에 쉽게 전환하려는 경우 권장되는 연결 모드입니다.

클라이언트 배포 및 관리

사용자가 직접 AppStream 2.0 클라이언트를 설치하거나 관리자가 PowerShell 스크립트를 원격으로 실행하거나 AppStream 2.0 클라이언트를 사용자 지정 설정으로 다시 패키징하여 AppStream 2.0 클라이언트를 대신 설치할 수 있습니다.

사용자가 스트리밍 세션에서 사용할 수 있도록 하려는 USB 디바이스를 정규화해야 합니다. 자격이 부여되지 않은 USB 디바이스는 AppStream 2.0에서 감지되지 않으며 세션과 공유할 수 없습니다. 디바이스에 자격이 부여된 후 사용자는 새 스트리밍 세션을 시작할 때마다 AppStream 2.0과 디바이스를 공유해야 합니다.

AppStream 2.0 클라이언트를 대규모로 배포할 때 AWS는 엔터프라이즈 배포 도구를 사용할 것을 권장합니다. 엔터프라이즈 배포 도구에는 AppStream 클라이언트 설치 파일 및 그룹 정책 관리 템플릿이 포함되어 있습니다.

사용자 지정 도메인

프로그래밍 방식으로 AppStream 2.0을 배포하는 경우 사용자에게 스트리밍 세션에 대한 친숙한 환경을 제공할 수 있는 사용자 지정 도메인을 만들 수 있습니다. AppStream 2.0의 SAML 2.0 IdP 배포에서는 사용자 액세스가 AppStream 2.0이 아니라 IdP에서 시작된다는 점을 강조하는 것이 중요합니다. AppStream 2.0 URL은 인증 후 IdP에서 제공되므로 사용자는 AppStream 2.0 URL을 필요로 하지 않습니다. 따라서 SAML 2.0 IdP 배포에는 사용자 지정 도메인 이름이 필요하지 않습니다.

인증

AppStream 2.0에서는 Amazon 2.0 외부에서 또는 AppStream AppStream 2.0 서비스의 일부로 인증을 수행할 수 있습니다. AppStream 2.0 배포에 대한 인증 방식을 선택하는 것은 설계의 기본 고려 사항입니다. 조직에서 다양한 사용 사례에 따라 AppStream 2.0을 여러 번 배포하는 경우는 드문 일이 아닙니다. 사용 사례마다 인증 방법이 다를 수 있습니다.

2.0에는 세 가지 유형의 인증 방법이 있습니다. AppStream

- SAML 2.0
- 사용자 풀
- 프로그래밍 방식

최적화된 방법 결정

Amazon AppStream 2.0은 대부분의 조직 설계 요구 사항에 유연하게 적용할 수 있도록 설계되었습니다. 최적화된 인증 방법을 결정할 때는 서비스를 사용하는 사용자의 목적과 목적, 조직 정책 및 절차를 고려하는 것이 가장 좋습니다.

다음은 사용 사례와 조직 목표를 결합한 몇 가지 예입니다.

표 4 — 조직 목표를 포함한 사용 사례

예	설명	인증
도메인에 가입된 플릿 인스턴스가 필요합니다.	AppStream 이미지에 설치된 애플리케이션은 도메인에 가입된 리소스에만 액세스할 수 있습니다.	SAML 2.0
Microsoft 서비스와의 긴밀한 통합	Microsoft 그룹 정책 및 백엔드 인프라 개발에 대한 조직의 의존도	SAML 2.0
기존 엔터프라이즈 SSO(Single Sign-On)	모든 신규 서비스는 여러 보고 및 보안 프로세스가 설정된 엔터프라이즈 SSO 솔루션을 활용해야 합니다.	SAML 2.0

예	설명	인증
애플리케이션에 대한 스마트 카드 지원	스마트 카드 리더를 통해 스트리밍되는 애플리케이션에 대한 세션 내 인증을 위한 스마트 카드(예: 프라이빗 ID 확인 및 일반 액세스 카드).	SAML 2.0
임시 직원이 포함된 계절별 인력	1년 중 몇 달 동안 임시 근로자에게는 활동을 완료하는 데 필요한 내부 리소스가 포함되지 않은 소수의 애플리케이션이 할당됩니다.	사용자 풀
제한적 IT 지원	IdP(자격 증명 공급자) 유지 관리에 따르는 오버헤드를 없애고자 하고 사용자 수가 50명 미만이고 IT 직원이 제한된 소규모 조직	사용자 풀
ISV(독립 소프트웨어 개발 판매 회사)	조직에서 구축한 독점 솔루션에는 사용자 권한 부여 및 인증이 포함되며 솔루션의 일부로 AppStream 2.0을 확장합니다. *	프로그래밍 방식
기술 쇼케이스	사용자 정보를 저장할 필요 없이 솔루션 둘러보기의 일환으로 독점 기술을 소개하는 완전한 임시 환경입니다.	프로그래밍 방식
대화형 웹 사이트 환경	스트리밍 Windows 애플리케이션을 사용하여 대화형 웹 사이트를 만드세요. **	프로그래밍 방식

*자세한 내용은 소프트웨어 공급업체: 모든 사용자 디바이스에 애플리케이션 제공을 참조하세요.

**자세한 내용은 AppStream 2.0 스트리밍 세션 임베드을 참조하십시오.

조직에 이전에 제공된 예제에 나열되지 않은 사용 사례 또는 정책이 있는 경우 AppStream 2.0 워크플로우 사용량의 원하는 종료 상태를 예측하여 인증 솔루션이 이와 충돌하지 않도록 하는 것이 좋습니다.

자격 증명 공급자 구성

SAML 2.0

SAML(보안 어설션 마크업 언어) 2.0은 사용자가 AWS 리소스를 사용할 수 있도록 지원하는 일반적인 배포 옵션입니다. 다양한 타사 SAML 2.0 ID 공급자가 2.0을 지원합니다. AppStream AppStream 2.0 리소스가 도메인에 가입되었는지 여부에 관계없이 SAML 2.0 IdP를 사용하려면 IAM을 사용해야 합니다.

대부분은 각 SAML 애플리케이션에 대해 특정 SAML 속성을 갖는 고유한 metadata.xml 를 IdPs 생성하므로, 모든 AppStream 2.0 스택에는 SAML IdP와 신뢰할 수 있는 관계를 갖는 역할 및 2.0 스택의 SAML IdP 및 ARN 요구 사항과 일치하는 조건으로 AppStream:Stream에 대한 단일 권한을 가진 정책이 필요합니다. AppStream

AppStream 2.0 관리 가이드에서는 단일 2.0 스택 설계에 대한 예제 구성을 제공합니다. AppStream 다중 스택 배포의 경우 SAML 2.0 다중 스택 애플리케이션 카탈로그 사용을 위한 선택적 단계를 참조하세요.

사용자 풀

AppStream 2.0의 사용자 풀 탭은 간단한 개념 증명을 위한 유효한 옵션입니다. AppStream 2.0을 사용하여 프로덕션 응용 프로그램을 제공하는 모든 사용 사례 및 조직에서는 사용자 풀을 사용하지 않는 것이 가장 좋습니다.

사용자 풀에 대해 한 가지 중요한 점은 사용자의 이메일 주소는 대소문자를 구분한다는 점입니다. 따라서 사용자에게 사용자 자격 증명을 올바르게 입력하는 방법을 교육하는 것이 가장 좋습니다.

스트리밍 URL

중앙 집중식 서비스 (일반적으로 ISV) 에서 AppStream 2.0 리소스를 호출하는 배포의 경우 프로그래밍 방식 인증은 응용 프로그램을 사용하여 프로그래밍 방식으로 AWS 호출하여 정보를 동적으로 전달하고 사용자를 위한 2.0 세션을 생성합니다. AppStream URL 작업을 사용하여 스트리밍 URL을 만들 때는 API 인증 방법 (일반적으로 '프로그래밍 방식'이라고 함) 을 사용하십시오. CreateStreaming `CreateStreamingURL` 호출하는 사용자는 `appstream:CreateStreamingURL` 권한이 있는 유효한 사용자 또는 역할을 사용하고 있어야 합니다.

프로그래밍 방식 액세스에 대한 정책을 생성할 때는 리소스 섹션에서 기본 '*' 대신 정확한 AppStream 2.0 Stack ARN을 지정하여 액세스를 보호하는 것이 좋습니다. 예:

Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appstream:createStreamingURL"
            ],
            "Resource": "arn:aws:appstream:us-east-
1:031421429609:stack/BestPracticesStack"
        }
    ]
}
```

> **Note**
>
> 스택 설명 API 또는 AWS CLI를 사용하여 AppStream 2.0 스택의 ARN을 빠르게 검색할 수 있습니다.

AppStream 2.0 인스턴스는 일반 인스턴스로 시작해야 합니다. AppStream 2.0 인스턴스는 애플리케이션에서 전달된 정보를 통해 세션 컨텍스트를 사용하여 환경을 설정하여 사용자에게 동적인 환경을 제공합니다.

로컬 GPO를 사용하여 `CreateStreamingURL` 사용자 로그온 시 설정을 지정할 수 있지만 세션에서 사용할 고객 ID 또는 데이터베이스 연결 설정과 같은 주요 특성을 사용하고 전달할 때는 세션 컨텍스트가 가장 좋습니다. AppStream

애플리케이션 사용 권한

AppStream 2.0은 사용자에게 제공되는 응용 프로그램 카탈로그를 동적으로 구축할 수 있습니다. 애플리케이션 사용 AppStream 권한은 SAML 2.0 속성을 기반으로 하거나 2.0 동적 애플리케이션 프레임워크를 사용합니다.

대부분의 시나리오에서 SAML 2.0을 사용하는 속성 기반 애플리케이션 권한을 사용하는 것이 좋습니다. 애플리케이션 패키지 전송을 관리하려면 동적 애플리케이션 프레임워크를 사용하는 것이 좋습니다.

Microsoft Active Directory와의 통합

Amazon AppStream 2.0 이미지 빌더 및 플릿은 Microsoft Active Directory와 통합될 수 있습니다. 이를 통해 사용자 인증 및 권한 부여를 위한 중앙 집중식 방법을 제공하고 도메인에 가입된 AppStream 2.0 인스턴스에 Active Directory 그룹 정책을 적용할 수 있습니다. 도메인에 연결된 AppStream 플릿을 사용하면 온프레미스 환경과 동일한 관리 이점을 얻을 수 있습니다. 여기에는 네트워크 파일 공유, 사용자-앱 사용 권한, 로밍 프로필, 프린터 액세스 및 기타 정책 기반 설정에 대한 중앙 집중식 관리가 포함됩니다.

AppStream 2.0 환경을 Active Directory와 통합할 때는 AppStream 2.0 스택에 대한 초기 인증이 여전히 SAML2.0 IdP에 의해 관리된다는 점에 유의해야 합니다. 사용자가 IdP에 성공적으로 인증된 후 세션을 시작할 때 Active Directory 도메인에 대한 도메인 암호 또는 스마트 카드 인증을 입력해야 합니다.

AppStream 2.0과 함께 사용할 Active Directory Domain Services(ADDS) 환경을 설계할 때는 두 가지 서비스 옵션과 다양한 배포 시나리오를 사용할 수 있습니다. 또한 Active Directory 사이트 토폴로지 소유자와 함께 AppStream 2.0 네트워킹을 검토해야 합니다.

서비스 옵션

Active Directory는 AWS Managed Microsoft Active Directory(AD)를 사용하여 배포할 수도 있습니다. AWS Managed Microsoft AD는 Microsoft Active Directory를 실행할 수 있는 완전 관리형 서비스입니다. Microsoft Active Directory는 EC2 또는 온프레미스에서 실행되는 자체 호스팅 환경에서도 사용할 수 있습니다.

배포 시나리오

나열된 다음 배포 시나리오는 Microsoft Managed AD 또는 고객의 자체 관리형 Active Directory를 사용하는 AppStream 2.0의 일반적으로 사용되고 권장되는 통합 옵션입니다. 아래 나열된 모든 아키텍처 다이어그램은 핵심 Amazon 구조를 사용합니다.

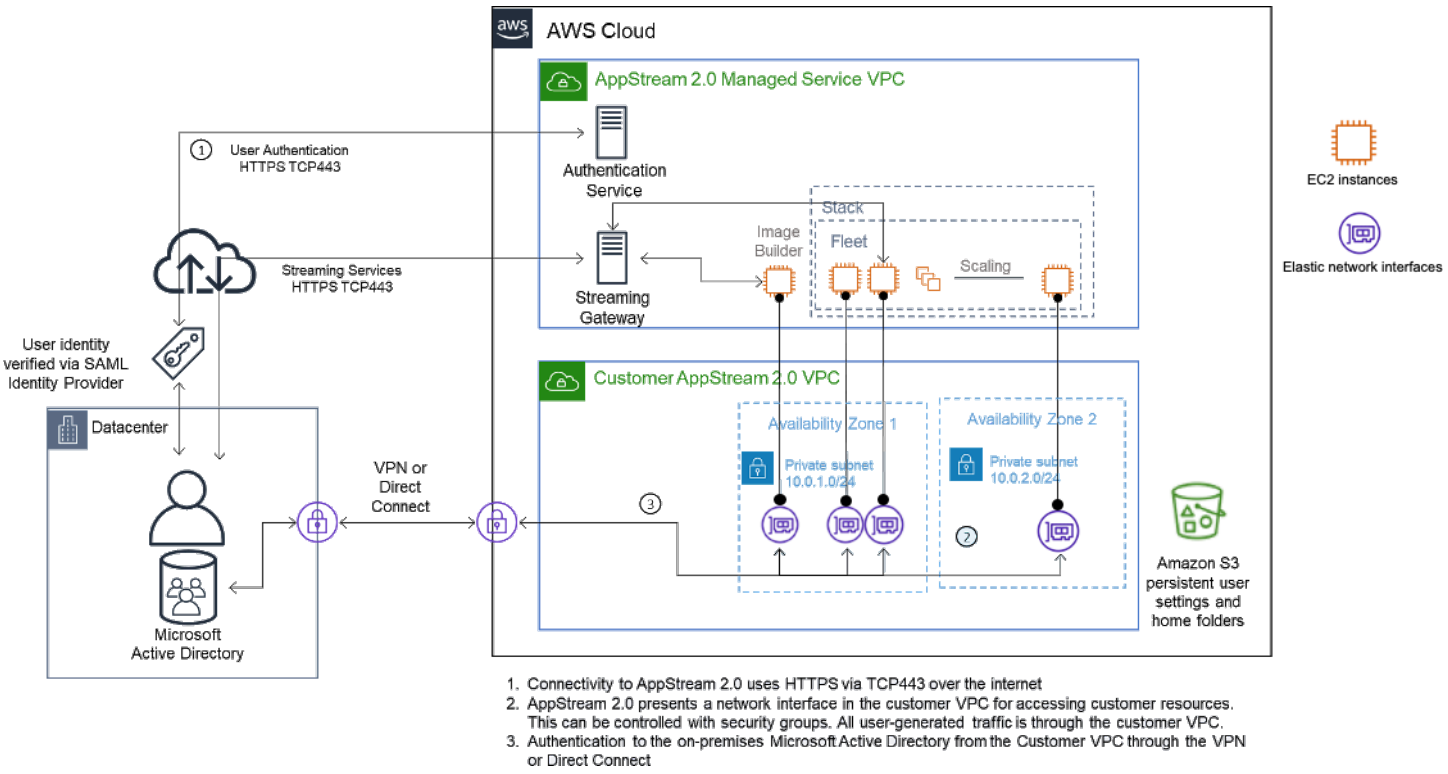
- Amazon VPC(Virtual Private Cloud) — 4개 AZ에 분산된 최소 4개의 프라이빗 서브넷이 있는 AppStream 2.0 서비스 전용 Amazon VPC를 생성합니다. 프라이빗 서브넷 중 2개는 AppStream 플릿과 이미지 빌더에 사용됩니다. 나머지 두 서브넷은 EC2 또는 Microsoft Managed AD의 도메인 컨트롤러에 사용됩니다.
- 동적 호스트 구성 프로토콜 (DHCP) 옵션 세트 — VPC에서 프로비저닝될 AppStream 2.0 플릿 및 이미지 빌더에 구성 정보를 전달하기 위한 표준을 제공합니다. DHCP 옵션 세트는 VPC 수준에서 정의

됩니다. 이를 통해 고객은 프로비저닝 시 AppStream 2.0 인스턴스에서 사용할 지정된 도메인 이름과 DNS 설정을 정의할 수 있습니다.

- AWS디렉터리 서비스 — Amazon Microsoft Managed AD를 AppStream 2.0 워크로드와 함께 사용할 두 개의 프라이빗 서브넷에 배포할 수 있습니다.
- AppStream 2.0 플릿 — AppStream 2.0 플릿 또는 이미지 빌더는 AWS Managed VPC에서 호스팅됩니다. 각 AppStream 2.0 인스턴스에는 두 개의 탄력적 네트워크 인터페이스(ENI) 가 있습니다. 기본 인터페이스(`eth0`)는 관리 목적과 스트리밍 게이트웨이를 통한 최종 사용자 인스턴스 연결을 중개하는 데 사용됩니다. 보조 인터페이스(`eth1`)는 고객-VPC에 삽입되며 맞춤형 VPC 또는 온프레미스의 다른 리소스에 액세스하는 데 사용할 수 있습니다.

시나리오 1: 온프레미스에 배포된 ADDS(Active Directory Domain Services)

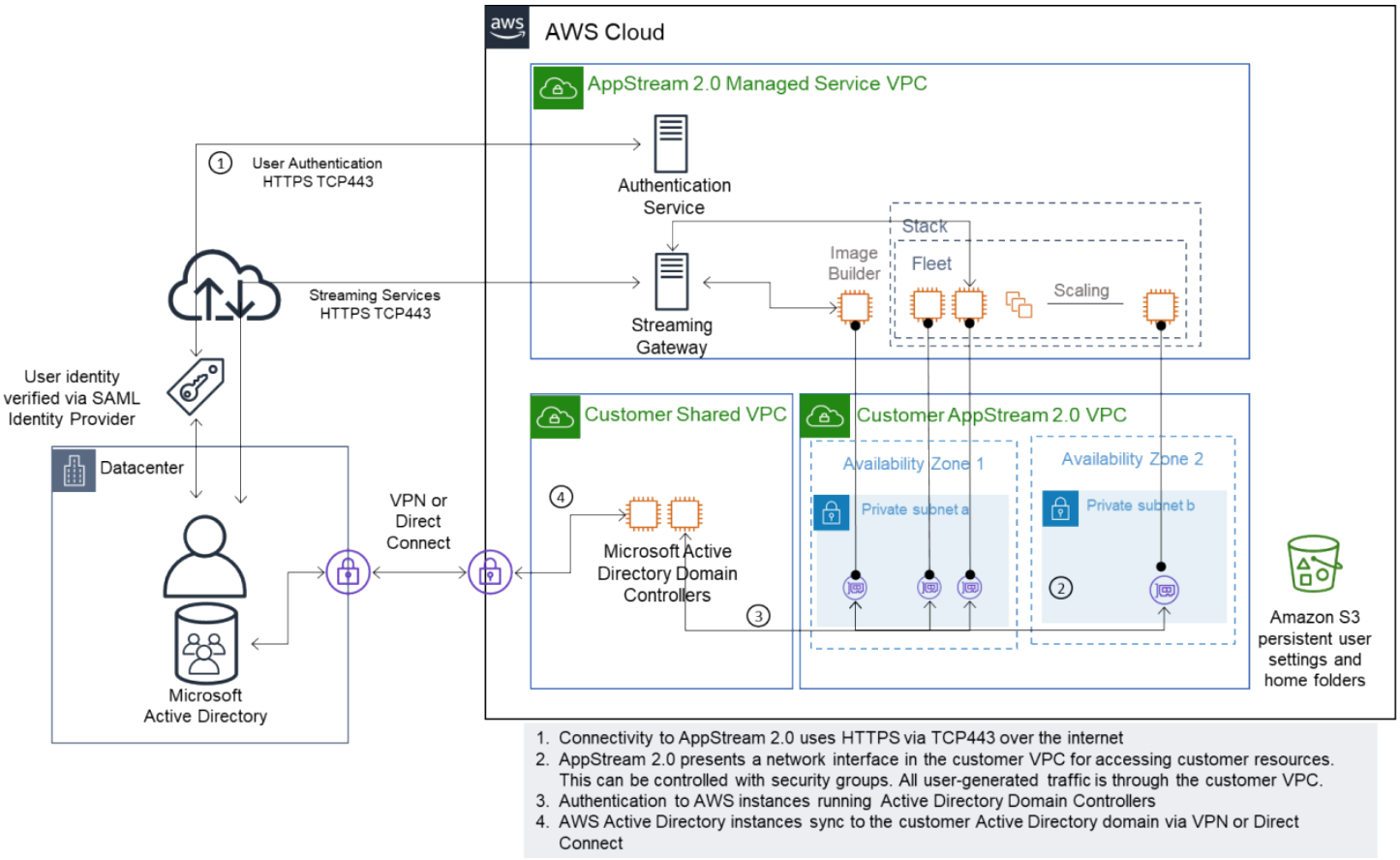
모든 인증 트래픽은 고객 VPC에서 고객 게이트웨이로 향하는 VPN 또는 Direct Connect 연결을 통과합니다. 이 시나리오의 장점은 고객 VPC에 추가 도메인 컨트롤러를 프로비저닝하지 않고도 이미 배포된 AD 환경을 사용할 수 있다는 점입니다. 단점은 AppStream 2.0 플릿에서 사용자를 인증하고 권한을 부여하는 데 VPN 또는 Direct Connect에만 의존한다는 점입니다. 네트워크 연결 문제가 있는 경우 AppStream 2.0 플릿 또는 이미지 빌더가 직접적인 영향을 받습니다. 경로가 서로 다른 이중 VPN 터널 또는 Direct Connect 연결을 제공하면 이러한 잠재적 위험을 줄일 수 있습니다.



시나리오 1: 온프레미스에 배포된 ADDS(Active Directory Domain Services)

시나리오 2: ADDS(Active Domain Services)를 AWS 고객 VPC로 확장

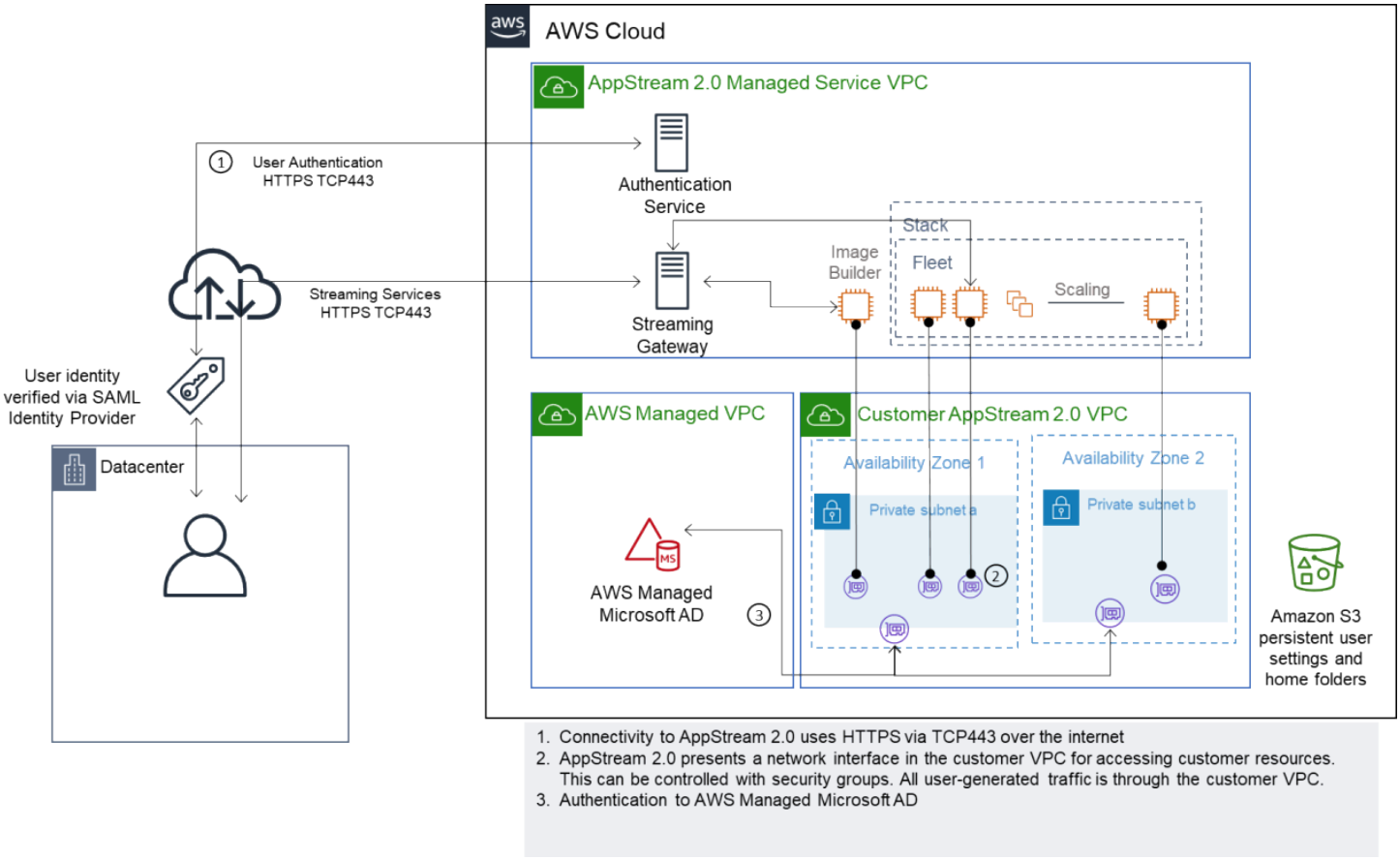
Active Directory는 고객 VPC까지 확장됩니다. 고객 VPC의 새 도메인 컨트롤러를 위한 Active Directory 사이트를 만들어야 합니다. 인증 트래픽은 VPN 또는 Direct Connect 연결을 통과하지 않고 AWS 고객 VPC의 도메인 컨트롤러로 라우팅됩니다.



시나리오 2 — Active Domain Services를 AWS 고객 가상 프라이빗 클라우드로 확장

시나리오 3: AWS Managed Microsoft Active Directory

AWS Managed Microsoft AD는 AWS 클라우드에 배포되며 AppStream 2.0 플릿 및 이미지 빌더의 ID 및 리소스 도메인으로 사용됩니다.



시나리오 3 — AWS Managed Active Directory

Active Directory 서비스 사이트 토폴로지

Active Directory 서비스 사이트 토폴로지는 물리적 네트워크를 논리적으로 표현한 것입니다.

사이트 토폴로지는 클라이언트 쿼리와 Active Directory 복제 트래픽을 효율적으로 라우팅하는 데 도움이 됩니다. 잘 설계되고 유지 관리되는 사이트 토폴로지는 조직에서 다음과 같은 이점을 얻는 데 도움이 됩니다.

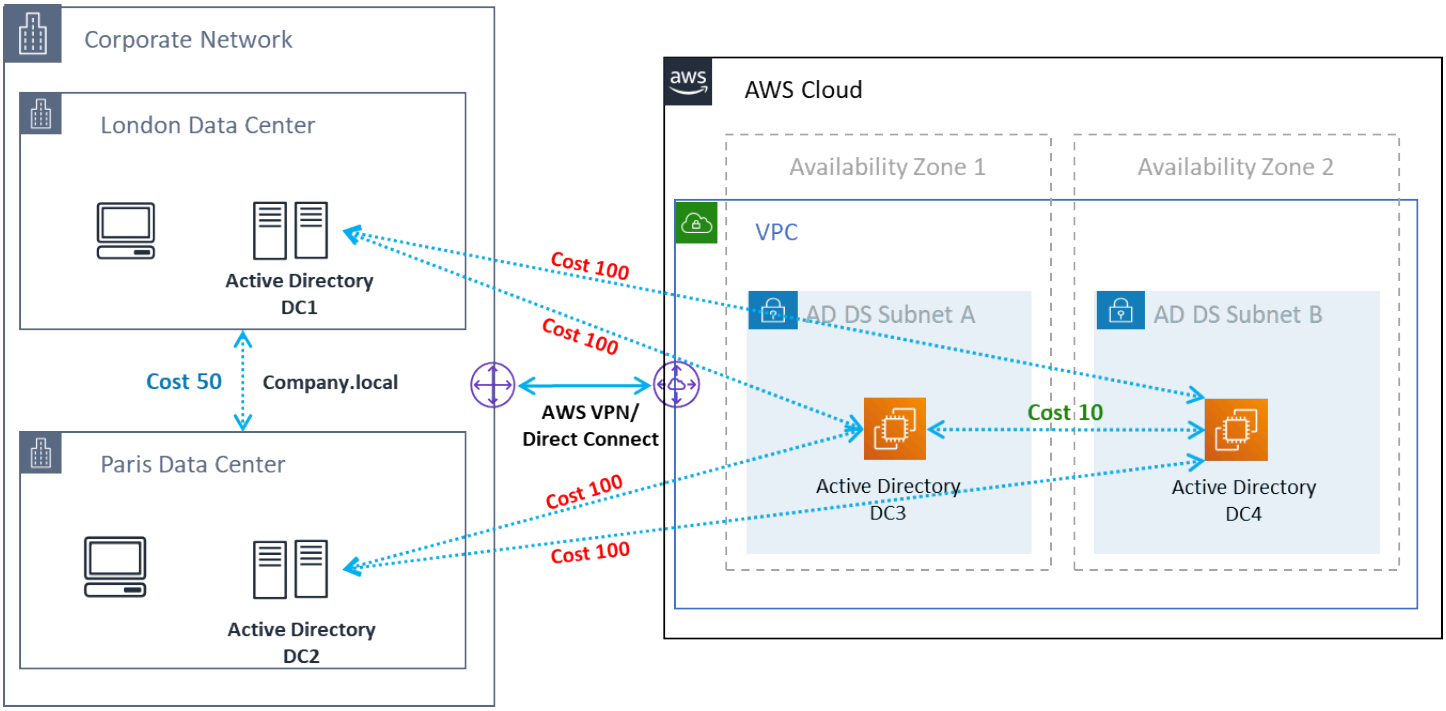
- 온프레미스와 AWS 클라우드 간에 동기화할 때 Active Directory 데이터를 복제하는 데 드는 비용을 최소화합니다.
- 도메인 컨트롤러와 같은 가장 가까운 리소스를 찾을 수 있도록 클라이언트 컴퓨터의 기능을 최적화합니다. 이를 통해 느린 WAN(Wide Area Network) 링크를 통한 네트워크 트래픽을 줄이고 로그온 및 로그오프 프로세스를 개선하며 리소스 액세스 작업의 속도를 높일 수 있습니다.

AppStream 2.0 서비스를 도입할 때는 AppStream 2.0 인스턴스의 서브넷에 사용되는 주소 범위가 사용자 환경에 맞는 올바른 사이트에 할당되었는지 확인하십시오.

시나리오 1과 시나리오 2에서 사이트와 서비스는 로그온 시간과 Active Directory 리소스 액세스 시간 측면에서 최상의 사용자 경험을 위한 중요한 구성 요소입니다.

사이트 토폴로지는 동일한 사이트 내 및 사이트 경계 전반의 도메인 컨트롤러 간 Active Directory 복제를 제어합니다.

올바른 사이트 토폴로지를 정의하면 클라이언트 유사성이 보장되므로 클라이언트(이 경우 AppStream 2.0 스트리밍 인스턴스)가 선호하는 로컬 도메인 컨트롤러를 사용합니다.



Active Directory 사이트 및 서비스의 AD 다이어그램 — 클라이언트 유사성

> **Tip**
>
> 가장 좋은 방법은 온프레미스 AD DS와 AWS 클라우드 간의 사이트 링크에 대한 높은 비용을 정의하는 것입니다. 위 그림은 사이트 독립적인 클라이언트 유사성을 보장하기 위해 사이트 링크에 할당해야 하는 비용(비용 100)의 예입니다.

사이트 토폴로지에 대한 자세한 내용은 사이트 토폴로지 설계를 참조하세요.

Active Directory 조직 단위

AWS는 구성된 OU(조직 단위)를 단일 AppStream 2.0 디렉터리 구성 객체에 저장할 것을 권장합니다. 각 AppStream 2.0 스택에는 자체 OU가 있는 것이 가장 좋습니다. 이를 통해 스택당 특정 GPO를 유연

하게 보유할 수 있습니다. AppStream 2.0 전용 정책을 온프레미스 데스크톱과 혼용하지 않도록 OU를 AppStream 2.0 컴퓨터 개체 전용으로 사용해야 합니다. AppStream 2.0을 배포하는 각 AWS 리전마다 하위 OU를 사용하는 것을 고려해 보십시오.

Active Directory 컴퓨터 객체 정리

AppStream 2.0 인스턴스는 휘발성입니다. 플릿이 스케일 아웃 및 스케일 인할 때 플릿은 Active Directory 컴퓨터 객체를 만들고 재사용합니다.

AWS는 AppStream 플릿이 제거된 후에도 존재할 수 있는 오래된 Active Directory 컴퓨터 객체를 삭제하기 위한 AD 정리 프로세스를 만들 것을 권장합니다.

보안

Amazon Web Services(AWS)에서 가장 우선순위가 높은 것이 클라우드 보안입니다. 보안 및 규정 준수는 AWS 와 고객 간의 공동 책임입니다. 자세한 내용은 공동 책임 모델을 참조하세요. AWS 및 AppStream 2.0 고객은 스택, 플릿, 이미지 및 네트워킹과 같은 다양한 계층에 보안 조치를 구현하는 것이 중요합니다.

일시적인 특성으로 인해 애플리케이션 및 데스크톱 전송을 위한 안전한 솔루션으로 AppStream 2.0이 선호되는 경우가 많습니다. Windows 배포에서 흔히 볼 수 있는 바이러스 백신 솔루션이 미리 정의되고 사용자 세션이 끝나면 제거되는 환경의 사용 사례에 적합한지 생각해 보십시오. 바이러스 백신은 가상화된 인스턴스에 오버헤드를 추가하므로 불필요한 활동을 줄이는 것이 가장 좋습니다. 예를 들어 부팅 시 시스템 볼륨(간헐적)을 스캔해도 전체 보안인 AppStream 2.0에 추가되지 않습니다.

보안 AppStream 2.0의 두 가지 주요 질문은 다음과 같습니다.

- 세션 이후에도 사용자 상태를 유지하는 것이 필수인가요?
- 세션 내에서 사용자는 어느 정도의 액세스 권한을 가져야 하나요?

영구 데이터 보호

AppStream 2.0을 배포하려면 사용자 상태가 일부 형태로 지속되어야 할 수 있습니다. 개별 사용자에 대한 데이터를 유지하거나 공유 폴더를 사용하여 공동 작업을 위해 데이터를 유지하는 것일 수 있습니다. AppStream 2.0 인스턴스 스토리지는 임시적이며 암호화 옵션이 없습니다.

AppStream 2.0은 Amazon S3의 홈 폴더 및 애플리케이션 설정을 통해 사용자 상태 지속성을 제공합니다. 일부 사용 사례에서는 사용자 상태 지속성을 더 잘 제어해야 합니다. 이러한 사용 사례의 경우 에서는 서버 메시지 블록(SMB) 파일 공유를 사용할 것을 AWS 권장합니다.

사용자 상태 및 데이터

대부분의 Windows 애플리케이션은 사용자가 생성한 애플리케이션 데이터와 함께 배치할 때 가장 안전하고 최상의 성능을 발휘하기 때문에 이 데이터를 AppStream 2.0 플릿 AWS 리전 과 동일하게 유지하는 것이 가장 좋습니다. 이 데이터를 암호화하는 것이 가장 좋습니다. 사용자 홈 폴더의 기본 동작은 AWS 키 관리 서비스()의 Amazon S3-managed형 암호화 키를 사용하여 저장 중인 파일 및 폴더를 암호화하는 것입니다AWS KMS. AWS 콘솔 또는 Amazon S3 버킷에 액세스할 수 있는 AWS 관리 사용자는 이러한 파일에 직접 액세스할 수 있습니다.

사용자 파일 및 폴더를 저장하기 위해 Windows 파일 공유의 서버 메시지 블록(SMB) 대상이 필요한 설계에서는 프로세스가 자동으로 진행되거나 구성이 필요합니다.

표 5 — 사용자 데이터 보안 옵션

SMB 대상	Encryption-at-rest	Encryption-in-transit	바이러스 백신(AV)
FSx Windows File Server용	자동 통과 AWS KMS	SMB 암호화를 통한 자동	원격 인스턴스에 설치된 AV는 매핑된 드라이브에서 스캔을 수행합니다.
파일 게이트웨이, AWS Storage Gateway	기본적으로 S3 AWS Storage Gateway 에에 저장된 모든 데이터는 Amazon S3-Managed 암호화 키(-SSE-S3)를 사용하여 서버 측에서 암호화됩니다. (AWS Key Management Service KMS)를 사용하여 저장된 데이터를 암호화하도록 다양한 게이트웨이 유형을 선택적으로 구성할 수 있습니다.	모든 유형의 게이트웨이 어플라이언스와 AWS 스토리지 간에 전송되는 모든 데이터는 를 사용하여 암호화됩니다SSL.	원격 인스턴스에 설치된 AV는 매핑된 드라이브에서 스캔을 수행합니다.
EC2기반 Windows 파일 서버	EBS 암호화 활성화	PowerShell; `Set-SmbServer Configuration - EncryptData $True`	서버에 설치된 AV는 로컬 드라이브에서 스캔을 수행합니다.

엔드포인트 보안 및 바이러스 백신

Amazon AppStream 2.0 인스턴스의 짧은 임시 특성과 데이터의 지속성 부족은 영구 데스크톱에서 필요한 활동으로 인해 사용자 경험과 성능이 손상되지 않도록 다른 접근 방식이 필요함을 의미합니다. Endpoint Security 에이전트는 조직 정책이 있거나 이메일, 파일 수신, 외부 웹 브라우징과 같은 외부 데이터 수신과 함께 사용되는 경우 AppStream 2.0 이미지에 설치됩니다.

고유 식별자 제거

엔드포인트 보안 에이전트에는 플릿 인스턴스 생성 프로세스 중에 재설정해야 하는 전역 고유 식별자(GUID)가 있을 수 있습니다. 공급업체에는 이미지에서 생성된 각 인스턴스에 대해 새 GUID가 생성되도록 이미지에 제품을 설치하는 방법에 대한 지침이 있습니다.

GUID 이 생성되지 않도록 하려면 AppStream 2.0 Assistant를 실행하여 이미지를 생성하기 전에 엔드포인트 보안 에이전트를 마지막 작업으로 설치합니다.

성능 최적화

엔드포인트 보안 공급업체는 AppStream 2.0의 성능을 최적화하는 스위치와 설정을 제공합니다. 설정은 공급업체마다 다르며 일반적으로 의 섹션에서 해당 설명서에서 찾을 수 있습니다VDI. 일부 일반 설정에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 부팅 검사를 끄면 인스턴스 생성, 시작 및 로그인 시간이 최소화됩니다.
- 불필요한 검사를 방지하려면 예약 검사를 끄십시오.
- 서명 캐시를 해제하여 파일 열거를 방지합니다.
- VDI 최적화된 IO 설정 활성화
- 성능 보장을 위해 애플리케이션에 필요한 제외 사항

엔드포인트 보안 공급업체는 성능을 최적화하는 가상 데스크톱 환경에서 사용하기 위한 지침을 제공합니다.

- 가상 데스크톱 인프라에 대한 Trend Micro Office 스캔 지원 - Apex One/OfficeScan(trendmicro.com)
- CrowdStrike 및 데이터 센터에 CrowdStrike Falcon을 설치하는 방법
- Sophos 및 Sophos Central Endpoint: 골드 이미지에 설치하여 ID 중복을 방지하는 방법 및 Sophos Central: 가상 데스크톱 환경에 Windows 엔드포인트를 설치할 때의 모범 사례
- McAfee 가상 McAfee 데스크톱 인프라 시스템에서 및 에이전트 프로비저닝 및 배포

- Microsoft Endpoint Security 및 비영구 VDI 머신용 Microsoft Defender Antivirus 구성 - Microsoft Tech Community

스캔 제외

보안 소프트웨어가 AppStream 2.0 인스턴스에 설치된 경우 보안 소프트웨어가 다음 프로세스를 방해해서는 안 됩니다.

표 6 — AppStream 2.0은 보안 소프트웨어가 다음 프로세스를 방해해서는 안 되는 프로세스를 처리합니다.

서비스	프로세스
AmazonCloudWatchAgent	“C:\Program Files\AmazonAmazonCloudWatchAgent\start-amazon- cloudwatch-agent.exe”
AmazonSSMAgent	“C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe”
NICE DCV	“C:\Program Files\NICE\DCV\Server\bin\dcvserver.exe” “C:\Program Files\NICEDCV\Server\bin\dcvagent.exe”
AppStream 2.0	“C:\ProgramFiles\Amazon\AppStream2\StorageConnector\StorageConnector.exe” "C:\Program Files\Amazon\Photon\" 폴더에서 “.\에이전트\PhotonAgent.exe' “.\에이전트\s5cmd.exe' “.\WebServer\PhotonAgentWebServer.exe” “.\CustomShell\PhotonWindowsAppSwitcher.exe” “.\CustomShell\PhotonWindowsCustomShell.exe”

서비스	프로세스
	“.\CustomShell\PhotonWindowsCustomShellBackground.exe”

폴더

보안 소프트웨어가 AppStream 2.0 인스턴스에 설치된 경우 소프트웨어가 다음 폴더를 방해해서는 안 됩니다.

Example

```
C:\Program Files\Amazon\*
C:\ProgramData\Amazon\*
C:\Program Files (x86)\AWS Tools\*
C:\Program Files (x86)\AWS SDK for .NET\*
C:\Program Files\NICE\*
C:\ProgramData\NICE\*
C:\AppStream\*
C:\Program Files\Internet Explorer\*
C:\Program Files\nodejs\
```

엔드포인트 보안 콘솔 위생

Amazon AppStream 2.0은 사용자가 유휴 및 연결 해제 제한 시간 이후에 연결할 때마다 새 고유 인스턴스를 생성합니다. 인스턴스는 고유한 이름을 갖게 되며 엔드포인트 보안 관리 콘솔에 구축됩니다. 4일 이상 오래된(또는 AppStream 2.0 세션 제한 시간에 따라 더 낮은) 미사용 노후화된 시스템을 삭제하도록 설정하면 콘솔에서 만료된 인스턴스 수가 최소화됩니다.

네트워크 제외

AppStream 2.0 관리 네트워크 범위(198.19.0.0/16) 및 다음 포트와 주소는 AppStream 2.0 인스턴스 내의 보안/방화벽 또는 바이러스 백신 솔루션에 의해 차단되어서는 안 됩니다.

표 7 - AppStream 2.0 스트리밍 인스턴스의 포트 보안 소프트웨어가

포트	사용량
8300, 3128	스트리밍 연결을 설정하는 데 사용됩니다.
8000	AppStream 2.0에서 스트리밍 인스턴스를 관리하는 데 사용됩니다.
8443	AppStream 2.0에서 스트리밍 인스턴스를 관리하는 데 사용됩니다.
53	DNS

표 8 — AppStream 2.0 관리형 서비스는 보안 소프트웨어가

포트	사용량
169.254.169.123	NTP
169.254.169.249	NVIDIA GRID 라이선스 서비스
169.254.169.250	KMS
169.254.169.251	KMS
169.254.169.253	DNS
169.254.169.254	메타데이터

AppStream 세션 보안

애플리케이션 및 운영 체제 제어 제한

AppStream 2.0을 사용하면 관리자는 애플리케이션 스트리밍 모드에서 웹 페이지에서 시작할 수 있는 애플리케이션을 정확히 지정할 수 있습니다. 하지만 이렇게 해도 지정된 애플리케이션만 실행할 수 있다는 보장은 없습니다.

Windows 유틸리티 및 애플리케이션은 조직이 필요로 하는 애플리케이션만 실행할 수 있도록 Microsoft AppLocker를 사용하여 운영 체제를 통해 추가 means. AWS recommends를 통해 시작할 수

있습니다. 기본 규칙은 모든 사람에게 중요한 시스템 디렉터리에 대한 경로 액세스 권한을 부여하므로 수정해야 합니다.

> **Note**
>
> Windows Server 2016 및 2019에서는 AppLocker 규칙을 적용하기 위해 Windows Application Identity 서비스를 실행해야 합니다. Microsoft를 사용한 AppStream 2.0의 애플리케이션 액세스 AppLocker 는 AppStream 관리자 안내서에 자세히 설명되어 있습니다.

Active Directory 도메인에 조인된 플릿 인스턴스의 경우 그룹 정책 객체(GPOs)를 사용하여 사용자 및 시스템 설정을 전달하여 사용자 애플리케이션 및 리소스 액세스를 보호합니다.

방화벽 및 라우팅

AppStream 2.0 플릿을 생성할 때는 서브넷과 보안 그룹을 할당해야 합니다. 서브넷에는 네트워크 액세스 제어 목록(NACLs) 및 라우팅 테이블(들)에 대한 기존 할당이 있습니다. 새 이미지 빌더를 시작하거나 새 플릿을 생성할 때 최대 5개의 보안 그룹을 연결할 수 있습니다. 보안 그룹은 기존 보안 그룹에서 최대 5개까지 할당할 수 있습니다. 각 보안 그룹에 대해 인스턴스에 대한 아웃바운드 및 인바운드 네트워크 트래픽을 제어하는 규칙을 추가합니다.

NACL 는 하나 이상의 서브넷으로 들어오고 나가는 트래픽을 제어하기 위한 상태 비저장 방화벽 역할을 VPC 하는 에 대한 선택적 보안 계층입니다. 에 보안 계층을 추가하기 위해 보안 그룹ACLs과 유사한 규칙으로 네트워크를 설정할 수 있습니다VPC. 보안 그룹과 네트워크 간의 차이점에 대한 자세한 내용은 보안 그룹 비교 및 페이지를 ACLs참조하세요. NACLs

Security Group 및 NACL 규칙을 설계하고 적용할 때는 최소 권한에 대한 AWS Well-Architected 모범 사례를 고려하세요. 최소 권한은 작업을 완료하는 데 필요한 권한만 부여하는 원칙입니다.

(AWSDirect Connect를 AWS 통해) 온프레미스 환경을 에 연결하는 고속 프라이빗 네트워크가 있는 고객의 경우 용 VPC 엔드포인트 사용을 고려할 수 있습니다. 즉 AppStream, 스트리밍 트래픽은 퍼블릭 인터넷을 통과하는 대신 프라이빗 네트워크 연결을 통해 라우팅됩니다. 이 주제에 대한 자세한 내용은 이 문서의 AppStream 2.0 스트리밍 인터페이스 VPC 엔드포인트 섹션을 참조하세요.

데이터 손실 방지

두 가지 유형의 데이터 손실 방지에 대해 살펴보겠습니다.

클라이언트에서 AppStream 2.0 인스턴스로의 데이터 전송 제어

표 9 — 데이터 수신 및 송신 제어 지침

설정	옵션	지침
클립보드	• 원격 세션에만 복사 및 붙여넣기 • 로컬 디바이스로만 복사 • Disabled(비활성)	이 설정을 비활성화해도 세션 내에서 복사 및 붙여넣기가 비활성화되지 않습니다. 세션에 데이터를 복사해야 하는 경우 데이터 유출 가능성을 최소화하려면 원격 세션에만 붙여넣기를 선택하십시오.
파일 전송	• 업로드 및 다운로드 • 업로드만 • 다운로드만 • Disabled(비활성)	데이터 유출을 방지하려면 이 설정을 활성화하지 마십시오.
로컬 디바이스로 인쇄	• 활성화됨 • Disabled(비활성)	인쇄가 필요한 경우 조직에서 제어하고 모니터링하는 네트워크 매핑 프린터를 사용하십시오.

스택 설정에 비해 기존 조직 데이터 전송 솔루션의 이점을 고려해 보십시오. 이러한 구성은 포괄적인 보안 데이터 전송 솔루션을 대체하도록 설계되지 않았습니다.

AppStream 2.0 인스턴스에서 송신 트래픽 제어

데이터 손실이 우려되는 경우 사용자가 AppStream 2.0 인스턴스 내에 있으면 액세스할 수 있는 내용을 은폐하는 것이 중요합니다. 네트워크 출구(또는 송신) 경로는 어떤 모습입니까? AppStream 2.0 인스턴스 내에서 최종 사용자가 퍼블릭 인터넷에 액세스할 수 있도록 하는 것이 일반적인 요구 사항이므로 WebProxy 또는 콘텐츠 필터링 솔루션을 네트워크 경로에 배치하는 것을 고려해야 합니다. 다른 고려 사항에는 로컬 안티바이러스 애플리케이션 및 AppStream 인스턴스 내의 기타 엔드포인트 보안 조치가 포함됩니다(자세한 내용은 “엔드포인트 보안 및 안티바이러스” 단원 참조).

AWS 서비스 사용

AWS Identity and Access Management

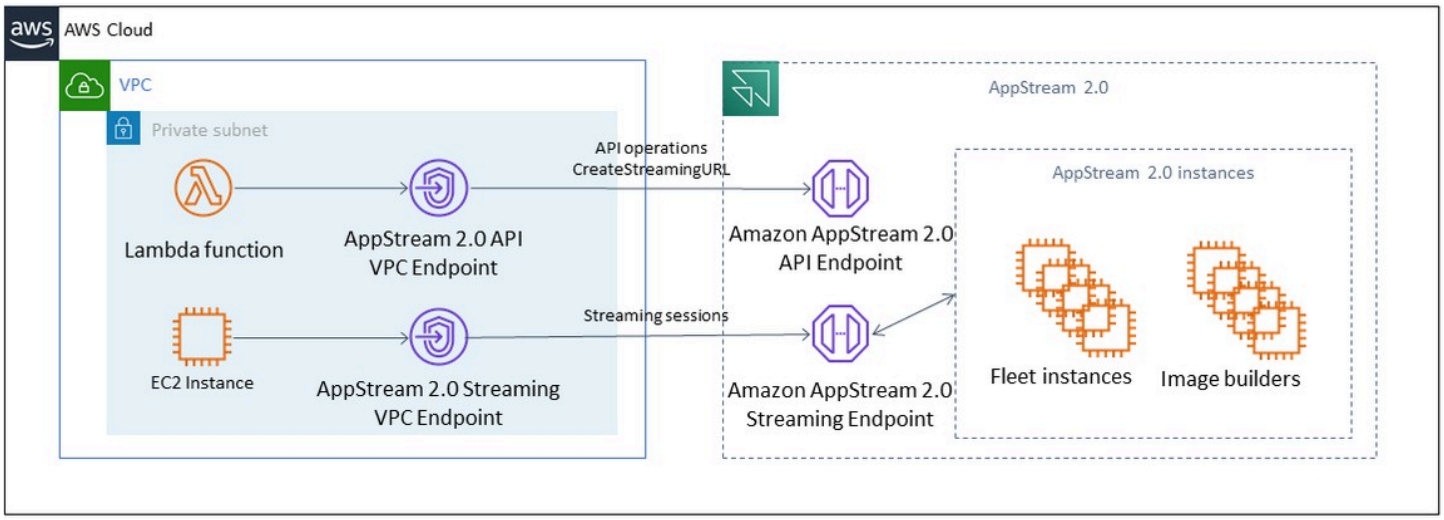
IAM 역할에 따라 AWS 서비스에 액세스하고 연결된 IAM 정책에 특정하는 것이 AppStream 2.0 세션의 사용자만 추가 보안 인증 정보를 관리하지 않고도 액세스할 수 있도록 하는 모범 사례입니다. AppStream 2.0에서 IAM 역할을 사용하는 모범 사례를 따릅니다.

홈 폴더와 애플리케이션 설정 지속성 모두에서 사용자 데이터를 유지하도록 생성된 IAM Amazon S3 버킷을 보호하는 정책을 생성합니다. 이렇게 하면 AppStream 2.0이 아닌 관리자가 액세스할 수 없습니다.

VPC 엔드포인트

VPC 엔드포인트는 VPC 와 지원되는 AWS 서비스 간의 프라이빗 연결을 가능하게 하고 로 구동되는 VPC 엔드포인트 서비스는 프라이빗 IP 주소를 사용하여 프라이빗하게 서비스에 액세스할 수 있는 기술 AWS PrivateLink AWS PrivateLink 입니다. VPC 와 다른 서비스 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다. AWS 서비스에 대해서만 퍼블릭 인터넷 액세스가 필요한 경우 VPC 엔드포인트는 NAT 게이트웨이 및 인터넷 게이트웨이에 대한 요구 사항을 모두 제거합니다.

자동화 루틴 또는 개발자가 AppStream 2.0을 API 호출해야 하는 환경에서는 AppStream 2.0 API 작업을 위한 인터페이스 VPC 엔드포인트를 생성합니다. 예를 들어 퍼블릭 인터넷 액세스가 없는 프라이빗 서브넷에 EC2 인스턴스가 있는 경우 AppStream 2.0용 VPC 엔드포인트를 사용하여 와 같은 2.0 API 작업을 호출API AppStream할 수 있습니다CreateStreamingURL. 다음 다이어그램은 Lambda 함수 API 및 EC2 인스턴스에서 AppStream 2.0 및 스트리밍 VPC 엔드포인트를 사용하는 예제 설정을 보여줍니다.



VPC 엔드포인트

스트리밍 VPC 엔드포인트를 사용하면 VPC 엔드포인트를 통해 세션을 스트리밍할 수 있습니다. 스트리밍 인터페이스 엔드포인트는 내에서 스트리밍 트래픽을 유지합니다VPC. 스트리밍 트래픽에는 픽셀, USB, 사용자 입력, 오디오, 클립보드, 파일 업로드 및 다운로드, 프린터 트래픽이 포함됩니다. VPC 엔드포인트를 사용하려면 AppStream 2.0 스택에서 VPC 엔드포인트 설정을 활성화해야 합니다. 이는 인터넷 액세스가 제한되어 있고 Direct Connect 인스턴스를 통해 액세스하는 것이 유리한 위치에서 퍼블릭 인터넷을 통해 사용자 세션을 스트리밍하는 대신 사용할 수 있습니다. VPC 엔드포인트를 통해 사용자 세션을 스트리밍하려면 다음이 필요합니다.

- 인터페이스 엔드포인트와 연결된 보안 그룹은 사용자가 연결하는 IP 주소 범위에서 포트443(TCP) 및 포트1400-1499(TCP)에 대한 인바운드 액세스를 허용해야 합니다.
- 서브넷의 네트워크 액세스 제어 목록은 임시 네트워크 포트1024-65535(TCP)에서 사용자가 연결하는 IP 주소 범위로의 아웃바운드 트래픽을 허용해야 합니다.
- 사용자를 인증하고 AppStream 2.0이 작동하는 데 필요한 웹 자산을 제공하려면 인터넷 연결이 필요합니다.

AppStream 2.0을 사용하는 AWS 서비스로 트래픽을 제한하는 방법에 대한 자세한 내용은 VPC 엔드포인트 에서 생성 및 스트리밍하기 위한 관리 안내서를 참조하세요.

전체 퍼블릭 인터넷 액세스가 필요한 경우 Image Builder에서 Internet Explorer 향상된 보안 구성(ESC)을 비활성화하는 것이 좋습니다. 자세한 내용은 AppStream 2.0 관리 가이드를 참조하여 Internet Explorer 고급 보안 구성을 비활성화합니다.

재해 복구

Amazon AppStream 2.0에는 최대 3개의 가용 영역에 걸쳐 이중화가 내장되어 있습니다. 즉, 사용자가 가용 영역에서 활성 세션을 진행하다가 성능이 저하된 경우 간단히 연결을 끊었다가 다시 연결하면 용량이 있다고 가정할 때 정상적인 가용 영역에 세션을 예약할 수 있습니다. 이렇게 하면 리전 내에서 고가용성이 제공되지만 리전 수준에서 서비스에 문제가 발생하는 경우 재해 복구 솔루션이 제공되지 않습니다.

AppStream 2.0 사용자를 위한 재해 복구 계획을 제공하려면 먼저 보조 리전에 AppStream 2.0 환경을 구축해야 합니다. 설계 관점에서 볼 때 이 환경은 온프레미스 환경에 대한 중복 연결이 있어야 하며(해당하는 경우) 기본 리전에 대한 종속성이 없어야 합니다. 예를 들어 AppStream 2.0 플릿이 도메인에 가입되어 있는 경우 사이트 및 서비스가 구성된 보조 리전에 추가 도메인 컨트롤러가 있어야 합니다. AppStream 2.0 관점에서 볼 때 이 환경은 기본 리전에 있는 것과 동일한 플릿 및 스택 설정으로 구성되어야 합니다. 플릿 자체는 동일한 기본 이미지를 실행해야 하며, 콘솔을 통해 또는 프로그래밍 방식으로 이 기본 이미지를 보조 리전으로 복사할 수 있습니다. AppStream 2.0 세션 내에서 실행되는 애플리케이션이 기본 리전에 연결된 백엔드 종속성을 가지고 있는 경우 기본 리전이 다운되더라도 사용자가 애플리케이션의 백엔드에 계속 액세스할 수 있도록 해당 리전에도 리전 중복성이 있어야 합니다. 대상 리전의 서비스 수준 한도는 기본 리전과 일치해야 합니다.

ID 라우팅

DR 시나리오에서 애플리케이션에 대한 액세스를 제공하는 두 가지 방법이 있습니다. 개괄적으로 보면 두 가지 방법은 사용자가 장애 조치 리전으로 이동하는 방식에 따라 다릅니다. 첫 번째 방법은 IdP의 단일 AppStream 2.0 애플리케이션 구성을 사용하여 수행되고 두 번째 방법은 두 개의 개별 애플리케이션 구성을 사용하는 것입니다.

방법 1: 애플리케이션의 릴레이 상태 변경

사용자가 ID 공급자(IdP)에서 AppStream 2.0에 로그인하면 인증 후 액세스하려는 리전 및 스택에 맞는 특정 URL로 릴레이됩니다. 릴레이 상태 URL에 대한 자세한 내용은 Amazon AppStream 2.0 관리 안내서를 참조하세요. 관리자는 동일한 AppStream 2.0 이미지에 구축된 교차 리전 스택을 사용자가 장애 조치할 기본 리전으로 구성할 수 있습니다. 관리자는 장애 조치 스택을 가리키도록 릴레이 상태 URL을 업데이트하기만 하면 이 장애 조치를 제어할 수 있습니다. 이 방법이 제대로 작동하려면 연결된 IAM 정책에 기본 스택과 장애 조치 스택 모두에 대한 액세스가 반영되어야 합니다. 이러한 IAM 정책을 구성하는 방법에 대한 자세한 내용은 다음 예제 정책을 참조하세요.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "appstream:Stream",
            "Resource": [
            "arn:aws:appstream:PrimaryRegion:190836837966:stack/StackName",
            "arn:aws:appstream:FailoverRegion:190836837966:stack/StackName"
            ],
            "Condition": {
                "StringEquals": {
                    "appstream:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

방법 2: IdP 내에서 두 개의 AppStream 2.0 애플리케이션 구성

이 방법을 사용하려면 관리자가 IdP 내에 AppStream 2.0용 애플리케이션 두 개를 별도로 구축해야 합니다. 그런 다음 두 애플리케이션을 모두 제시하여 사용자가 이동할 위치를 선택하도록 하거나 장애 조치가 완료될 때까지 애플리케이션을 잠그거나 숨길 수 있습니다. 이 방법은 전 세계 사용자가 자주 이동하는 사용 사례에 더 적합합니다. 이러한 사용자는 가장 가까운 엔드포인트에서 스트리밍해야 합니다. 따라서 두 애플리케이션을 모두 할당하면 가장 가까운 리전에 맞게 구성된 애플리케이션을 선택할 수 있습니다. 이를 자동화할 수도 있습니다. 자세한 내용은 이 블로그 게시물을 참조하세요.

스토리지 지속성

애플리케이션 지속성 및 홈 폴더 동기화와 같은 AppStream 2.0에 포함된 데이터 지속성 기능을 활용할 때는 해당 데이터를 장애 조치 리전에 복제해야 합니다. 이러한 기능은 지정된 AppStream 2.0 리전의 Amazon S3 버킷에 영구 데이터를 저장합니다. 데이터가 리전 간에 유지되도록 하려면 원본 버킷의 모든 변경 사항을 장애 조치 리전의 AppStream 2.0 버킷에 복제해야 합니다. 이는 Amazon S3 리전 간 복제와 같은 기본 Amazon S3 기능을 사용하여 수행할 수 있습니다. 각 사용자의 영구 데이터는 해시된 사용자 이름의 폴더 아래에 위치합니다. 사용자 이름은 동일한 리전 간에 해시되므로 데이터를 복제하기만 하면 보조 리전에서도 데이터 지속성을 유지할 수 있습니다. AppStream 2.0에서 사용하는 Amazon S3 버킷에 대한 자세한 내용은 이 안내서를 참조하세요.

모니터링

대시보드 사용

플릿 사용률 모니터링은 CloudWatch 지표와 대시보드 생성을 통해 수행할 수 있는 정기적인 활동입니다. 또는 AppStream 2.0 콘솔에서 플릿 사용량 탭을 사용할 수도 있습니다. 사용자 행동을 항상 예측할 수 있는 것은 아니며 수요가 일급 선결제 계획조차 초과할 수 있으므로 플릿 사용량을 정기적으로 모니터링하십시오. AppStream 2.0 지표 및 차원의 전체 목록은 모니터링 리소스의 AppStream 2.0 관리 가이드에서 확인할 CloudWatch 수 있습니다.

성장 예측

`PendingCapacity`에서 대규모 점프가 발생할 때마다 Auto Scaling 이벤트가 발생했습니다. 새 AppStream 2.0 플릿 인스턴스를 사용자 세션을 호스팅할 수 있게 될 때까지 이를 확인하고 반비례 관계를 유지하는 것이 중요합니다. `AvailableCapacity` `PendingCapacity` 각 AppStream 2.0 플릿에 `InsufficientCapacityError` 대해 CloudWatch 경보를 생성하여 자동 확장이 수요에 뒤처지지 않도록 관리자에게 알리십시오.

수요가 용량을 초과하고 `InsufficientCapacityError` 지표 값이 일반적인 경우, 근무일 시작 시 예약된 규모 조정 정책을 통해 최소 용량을 늘리는 것을 고려해 보십시오. 또한 수요가 충족된 후 최소 용량을 낮추는 두 번째 예약된 규모 조정 정책을 마련하십시오. 최소 용량 값을 낮추더라도 기존 세션에는 영향을 미치지 않는다는 점에 유의하세요. 업무가 끝나기 전에 최소 용량을 낮추면 `ActualCapacity`의 값을 낮춰 규모 조정이 의도한 대로 작동할 수 있습니다. 이를 통해 비용이 최적화됩니다.

수요를 지속적으로 예측할 수 없는 경우 Target Tracking 조정 정책을 사용하여 AppStream 2.0 플릿이 사용 패턴을 결정하는 동시에 수요를 충족하기에 `AvailableCapacity` 충분한지 확인하십시오. 목표 추적에서 플릿 사용량의 일정 비율을 사용하므로 계속 모니터링하십시오. 총 플릿 인스턴스 수가 증가하면 미사용 플릿 인스턴스 수가 크게 증가합니다. 최대 용량을 보수적인 값으로 설정하지 않으면 낭비가 될 수 있습니다. 여러 유형의 조정 정책(예: 예약 및 목표 추적)을 사용하여 안정성과 비용 최적화의 균형을 유지하십시오.

사용자 사용량 모니터링

순 사용자 모니터링(사용자 요금 형태로 비용이 발생) 이 사용자 요금은 Image Assistant(RDS) 구독자 액세스 라이선스(SAL)로 인한 것입니다. 순 사용자 평가는 인증이 수행되는 IdP의 보고 또는 사용량 보고서를 통해 수행할 수 있습니다.

사용량 보고서는 S3 버킷에 별도의 .csv 파일로 저장되며, 타사 BI(비즈니스 인텔리전스) 도구를 사용하여 다운로드하고 분석할 수 있습니다. 보고서를 다운로드하지 않고도 사용량 데이터를 분석하거나 여러 파일을 AWS 연결하지 않고도 사용자 지정 날짜 범위에 대한 보고서를 만들 수 있습니다. .csv 예를 들어 Amazon Athena와 Amazon을 QuickSight 사용하여 2.0 사용 데이터에 대한 사용자 지정 보고서 및 시각화를 생성할 수 있습니다 AppStream .

애플리케이션 및 Windows 이벤트 로그 유지

AppStream 2.0 인스턴스 세션이 완료되면 인스턴스가 종료됩니다. 즉, 세션에서 사용된 모든 애플리케이션 및 Windows 이벤트 로그가 손실됩니다. 이러한 애플리케이션 및 Windows 이벤트 로그를 유지해야 하는 경우 한 가지 방법은 Amazon Data Firehose를 사용하여 실시간으로 S3에 전송하고 OpenSearch Amazon 서비스 OpenSearch (서비스) 로 검색하는 것입니다. 쿼리가 빈번하지 않을 것으로 예상되는 경우 비용을 최적화하려면 Amazon Service를 실행하는 대신 Amazon Athena를 사용하여 검색하십시오. OpenSearch

감사 네트워크 및 관리 활동

아직 설정하지 않았다면 Amazon AppStream 2.0을 AWS CloudTrail사용하도록 구성하는 것이 가장 좋습니다. AWS 계정 AppStream 2.0 API 호출을 구체적으로 감사하려면 값이 인 필터 이벤트 소스를 사용하십시오appstream.amazonaws.com.

VPC 흐름 로그를 활성화하여 고객 관리 리소스에 대한 액세스를 감사할 수 있습니다. 감사가 필요한 경우 VPC 흐름 로그를 CloudWatch Logs에 게시하여 쿼리를 수행할 수 있습니다.

2.0 플릿이 성장함에 따라 서브넷 IP 할당을 모니터링하는 것이 중요합니다. AppStream describe-subnets CLI를 실행하여 플릿에 할당된 각 서브넷에서사용 가능한 IP 주소를 보고하여 IP 할당을 보고합니다. 조직에 최대 용량으로 실행되는 모든 플릿의 수요를 충족할 수 있는 충분한 IP 주소 용량이 있는지 확인하십시오.

비용 최적화

비용 최적화 요소는 불필요한 비용을 피하는 데 중점을 둡니다. 주요 주제에는 자금이 어디에 쓰이는지 이해하고 통제하는 것, 가장 적절하고 정확한 리소스 유형 수 선택 등이 포함됩니다. 시간 경과에 따른 지출을 분석하고 비즈니스 요구 사항에 맞게 규모를 조정하세요. 다음과 같은 AppStream 2.0 리소스에는 “사용한 만큼 지불”하는 요금이 발생합니다.

- 상시 작동 플릿 인스턴스
- 온디맨드 플릿 인스턴스
- 온디맨드 중지 인스턴스 요금
- 이미지 빌더 인스턴스
- 사용자 요금

현재 요금 정보는 Amazon AppStream 2.0 요금에 대한 AWS 웹 사이트를 참조하세요.

비용 효율적인 AppStream 2.0 배포 설계

AppStream 2.0 배포를 계획하고 설계하는 첫 번째 단계는 간단한 가격 책정 도구를 사용하여 사용량과 관련된 AWS 요금의 기준을 추정하는 것입니다. 총 사용자 수, 시간당 실제 동시 사용량, 인스턴스 유형 및 플릿 사용률을 제공하면 요금 도구가 사용자당 가격을 추정합니다. 또한 상시 작동 플릿 대신 온디맨드 플릿을 사용할 때의 예상 가격 절감액도 보여줍니다.

고객은 사용자의 스트리밍 요구 사항을 충족하기 위해 프로비저닝한 인스턴스에 대해서만 비용을 지불하는 AppStream 2.0 요금 모델을 선호합니다. 이 모델은 기존 애플리케이션 스트리밍 환경과는 다릅니다. 이는 일반적으로 부하가 적은 야간, 주말 및 공휴일에도 최대 용량에 대한 프로비저닝을 기반으로 합니다. Amazon AppStream 2.0 요금 도구는 AppStream 2.0 사용과 관련된 예상 AWS 요금만 제공하며 적용될 수 있는 세금은 포함하지 않습니다. 실제 요금은 AWS 서비스의 실제 사용량을 포함한 다양한 요인에 따라 달라집니다.

AppStream 2.0 가격 도구는 Microsoft Excel 또는 OpenOffice Calc 스프레드시트로 제공됩니다. 이 스프레드시트를 사용하면 플릿에 대한 기본 정보를 입력한 다음 사용 패턴을 기반으로 온디맨드 및 상시 작동 플릿에 대한 AppStream 2.0 환경의 예상 비용을 제공할 수 있습니다. 과거 또는 예상 사용 추세를 기반으로 비용을 시뮬레이션할 수 있습니다. 탄력적 플릿을 사용하면 관리자가 이러한 기능을 내장하여 사용량을 예측하고, 확장 정책 및 이미지를 생성, 유지 관리할 필요가 없습니다. Amazon Linux 2를 실행하는 탄력적 플릿과 인스턴스(모든 플릿 유형)에는 스트리밍 세션 기간(초), 최소 15분의 요금이 청구됩니다.

인스턴스 유형 선택을 통한 비용 최적화

플릿 및 이미지 빌더 인스턴스의 경우 애플리케이션에 맞게 다양한 인스턴스 패밀리와 유형을 선택할 수 있습니다.

최종 사용자 테스트 — 다음 단계는 AppStream 2.0 플릿을 파일럿 사용자 그룹에 배포하여 테스트하고 선택한 인스턴스 유형을 검증하는 것입니다. 파일럿 사용자에게 메모리, CPU 및 그래픽과 관련된 지표를 캡처하기 위해 정기적이고 사용량이 많은 워크플로를 모두 테스트하도록 요청하여 기본 성능 지표를 캡처할 수 있도록 하는 것이 중요합니다. 파일럿 그룹에는 애플리케이션을 사용하는 다양한 사용자 역할이 포함되어야 여러 사용자 경험을 통해 애플리케이션을 테스트할 수 있습니다. 사용자 수용 테스트를 통해 스트리밍 세션 환경에 대한 피드백을 수집할 수 있습니다. 스택을 만들거나 업데이트할 때 사용자 지정 피드백 URL을 사용할 수 있는 옵션이 있습니다. 사용자가 피드백 보내기 링크를 선택하여 애플리케이션 스트리밍 환경에 대한 피드백을 제출한 후 사용자는 이 URL로 리디렉션됩니다. 성능 병목 현상이 있는 경우 Windows 성능 메트릭을 사용하여 리소스 제약을 분석하십시오. 예를 들어 현재 플릿 인스턴스 유형인 stream.standard.medium에 리소스 제약이 있는 경우 인스턴스 유형을 stream.standard.large로 업그레이드하십시오. 반대로, 성능 지표에서 리소스 사용률이 낮은 것으로 나타나는 경우 인스턴스 유형을 다운그레이드해 보십시오.

플릿 유형 선택을 통한 비용 최적화

새 AppStream 2.0 플릿을 생성할 때 개발자는 상시 작동 플릿 또는 온디맨드 플릿 유형을 선택해야 합니다. 요금 관점에서 인스턴스 유형을 선택할 때는 AppStream 2.0이 플릿 인스턴스를 관리하는 방법을 이해하는 것이 중요합니다. 상시 작동 플릿의 경우 플릿 인스턴스는 실행 상태를 유지합니다. 따라서 사용자가 세션을 스트리밍하려고 하면 플릿 인스턴스가 항상 스트리밍 세션을 시작할 준비가 된 것입니다.

온디맨드 플릿의 경우 플릿 인스턴스가 시작된 후 중지된 상태로 유지됩니다. 중지된 인스턴스 요금은 실행 인스턴스 요금보다 저렴하므로 비용 절감에 도움이 될 수 있습니다. 온디맨드 플릿 인스턴스는 중지된 상태에서 시작해야 합니다. 사용자는 스트리밍 세션을 사용할 수 있을 때까지 약 2분 정도 기다려야 합니다.

탄력적 플릿은 Amazon Simple Storage Service(Amazon S3) 버킷에 저장된 가상 하드 드라이브에 설치할 수 있는 애플리케이션에 적합합니다. 탄력적 플릿은 스트리밍 기간 동안만 초당 요금이 청구되기 때문에 일부 사용 사례의 경우 비용을 추가로 절감할 수 있습니다. 요금은 플릿을 생성할 때 선택한 인스턴스 유형, 크기 및 운영 체제에 따라 달라집니다.

최종 사용자가 업무 시간 중에 플릿 인스턴스를 필요로 하는 경우 동일한 스트리밍 세션을 유지하는 것이 좋습니다. 플릿 인스턴스는 시간당 요금이 부과되고 새 스트리밍 세션이 시작될 때마다 플릿 인스턴스 요금이 추가로 발생하기 때문입니다.

표 10 — AppStream 2.0 플릿 유형 비교

플릿 유형	장점	고려 사항
상시 작동	스트리밍 세션의 대기 시간 감소	인스턴스를 중지된 상태로 유지할 수 있는 옵션이 없으므로 사용자는 시간당 인스턴스 요금을 지불합니다.
온디맨드	인스턴스가 중지된 상태로 유지되므로 비용이 절감	스트리밍 세션의 대기 시간 증가
탄력적	초당 청구는 가상 하드 디스크에 설치할 수 있는 애플리케이션의 사용 패턴이 산발적으로 나타나는 사용 사례에 유용할 수 있습니다.	애플리케이션 가상 하드 디스크의 크기가 커지면 스트리밍 인스턴스에 마운트하는 데 걸리는 시간이 길어질 수 있습니다.

AppStream 2.0은 플릿 사용률을 모니터링하고 가장 낮은 비용으로 사용자 요구를 충족할 수 있도록 플릿 용량을 자동으로 조정합니다. 용량 조정은 현재 사용률 또는 일정에 따라 사용자가 정의한 조정 정책을 기반으로 이루어집니다. 플릿 사용량 지표를 정기적으로 검토하여 플릿 조정 정책에 높은 수준의 예비 용량이 없는지 확인하십시오.

조정 정책

플릿 Auto Scaling을 사용하면 사용자가 로그인하기를 기다리는 동안 리소스를 과도하게 커밋하지 않아도 되므로 플릿 리소스를 최적화할 수 있습니다. 관리자는 사용자 요구에 맞게 다양한 사용률을 기반으로 플릿 크기를 조정할 수 있습니다. CloudWatch AppStream 2.0 플릿 지표 또는 타사 모니터링 도구를 사용하여 사용자 활동에 대해 알아보고 예상 사용량에 따라 AppStream 2.0 플릿을 확장 또는 축소하는 조정 정책을 구성할 수 있습니다. 사용자 로그는 실제 사용량을 파악하기 위한 필수 메커니즘입니다. 이 인사이트는 Auto Scaling을 기반으로 플릿 크기를 동적으로 변경하는 데 사용할 수 있습니다.

대부분의 경우 AppStream 2.0 플릿은 최대 사용자 수를 기준으로 생성되며 야간 및 주말과 같이 일일 및 주의 다른 시간대에 맞게 조정되지 않습니다. 스트리밍 애플리케이션의 동시 사용자 수가 총 사용자 수보다 적은 경우가 종종 있습니다. 특히 사용자가 유연하게 원격으로 작업할 수 있는 경우에는 더욱 그렇습니다. 사용 패턴을 예측할 때는 이러한 요소를 고려하는 것이 중요합니다. 과대평가하면 AppStream 2.0 인스턴스가 과도하게 프로비저닝되어 추가 비용이 발생합니다. 최적의 구성에 도달하려면 하나 이상의 예약된 규모 조정 정책을 스케일 아웃 정책과 결합해야 할 수 있습니다.

조정 정책을 구현하는 방법에 대해 자세히 알아보려면 Amazon AppStream 2.0 플릿 조정을 검토하십시오.

사용자 요금

사용자 요금은 사용자가 AppStream 2.0 플릿 인스턴스에서 애플리케이션을 스트리밍할 AWS 리전마다 사용자당, 월별로 부과됩니다. 다른 사용자 ID를 생성하는 대신 AppStream 2.0 사용자에 대해 일관된 사용자 ID를 사용하십시오. 이미지 빌더에 연결할 때는 사용자 요금이 부과되지 않습니다.

학교, 대학교 및 특정 공공 기관은 사용자당 월 0.44 달러의 Microsoft RDS SAL 사용자 요금 감면 혜택을 받을 수 있습니다. 자격 요구 사항은 Microsoft 라이선스 약관 및 문서를 참조하세요.

Microsoft 라이선스 모빌리티를 보유하고 있는 경우 자체 Microsoft RDS CAL(클라이언트 액세스 라이선스)을 가져와 Amazon AppStream 2.0과 함께 사용할 수 있습니다. 자체 라이선스가 적용되는 경우 월별 사용자 요금이 발생하지 않습니다. 기존 Microsoft RDS CAL 라이선스를 Amazon AppStream 2.0 2.0과 함께 사용할 수 있는지 여부에 대한 자세한 내용은 AWS라이선스 모빌리티 지침을 참조하거나 Microsoft 라이선스 담당자에게 문의하십시오.

Image Builder 사용

AppStream 2.0 Image Builder 인스턴스는 시간당 요금이 부과됩니다. Image Builder 인스턴스 요금에는 스트리밍 프로토콜에서 사용하는 컴퓨팅, 스토리지 및 모든 네트워크 트래픽이 포함됩니다. 실행 중인 모든 Image Builder 인스턴스에는 해당하는 인스턴스 실행 요금이 부과됩니다. 이 요금은 연결된 관리자가 없는 경우에도 인스턴스 유형과 크기를 기준으로 부과됩니다.

비용을 최적화하는 가장 좋은 방법은 사용하지 않는 Image Builder 인스턴스를 종료하는 것입니다. CloudWatch Events 규칙을 사용하여 Lambda 함수를 호출하여 이미지 빌더 인스턴스를 중지하는 등의 일일 작업을 예약할 수 있습니다.

관리형 AppStream 2.0 이미지 업데이트를 사용하여 AppStream 2.0 이미지를 최신 상태로 유지할 수 있습니다. 이 업데이트 방법은 최신 Windows 운영 체제 업데이트 및 드라이버 업데이트와 최신 AppStream 2.0 에이전트 소프트웨어를 제공합니다. 이 방법을 사용하여 이미지를 업데이트하면 관리형 서비스 프로세스의 일부로 Image Builder가 자동으로 시작되고 중지됩니다.

결론

AppStream 2.0을 통해 AWS에 기존 데스크톱 애플리케이션을 손쉽게 추가하고 사용자가 애플리케이션을 즉시 스트리밍하도록 할 수 있습니다. Windows 사용자는 AppStream 2.0 클라이언트 또는 HTML5 호환 웹 브라우저를 애플리케이션 스트리밍에 사용할 수 있습니다. 각 애플리케이션의 단일 버전을 유지할 수 있으므로 애플리케이션을 더 쉽게 관리할 수 있습니다. 사용자는 항상 최신 버전의 애플리케이션에 액세스할 수 있습니다. 애플리케이션은 AWS 컴퓨팅 리소스에서 실행되고 데이터는 사용자의 디바이스에 저장되지 않으므로 애플리케이션은 항상 높은 성능과 안전한 환경을 얻을 수 있습니다.

데스크톱 애플리케이션 스트리밍을 위한 기존 온프레미스 솔루션과는 달리, AppStream은 선행 투자가 필요 없고 유지 관리할 인프라도 없는 선불형 종량 요금제를 제공합니다. 언제 어디에서든지 규모 조정이 가능하기 때문에 사용자에게는 항상 최상의 경험이 보장됩니다.

Amazon AppStream 2.0은 기존 IT 시스템 및 프로세스에 통합되도록 설계되었으며, 이 백서에서는 이를 위한 모범 사례를 설명했습니다. 이 백서의 지침을 따른 결과 AWS 글로벌 인프라에서 비즈니스와 함께 안전하게 규모 조정할 수 있는 비용 효율적인 클라우드 데스크톱 배포가 가능해졌습니다.

기여자

다음은 이 문서의 기여자입니다.

- 앤드루 우드, 선임 솔루션 아키텍트, Amazon Web Services
- 앤드류 모건, EUC 스페셜리스트 SA, 아마존 웹 서비스
- 아룬 PC, 수석 EUC 스페셜리스트 SA, Amazon Web Services
- 애스리엘 아그로닌, 선임 솔루션 아키텍트, Amazon Web Services
- 더스틴 쉘턴 PC, 수석 EUC 스페셜리스트 SA, Amazon Web Services
- 제레미 쉬퍼, 선임 솔루션 아키텍트, Amazon Web Services
- 내비 매기, 수석 솔루션 아키텍트, Amazon Web Services
- 피트 퍼거스, 선임 클라우드 지원 엔지니어, Amazon Web Services
- 필 퍼슨, 수석 EUC 스페셜리스트 SA, Amazon Web Services
- 리처드 스페이븐, 수석 EUC 스페셜리스트 SA, Amazon Web Services
- 스펜서 디브로스, 선임 솔루션스 아키텍트, Amazon Web Services
- 스티븐 스테틀러, 선임 솔루션 아키텍트, Amazon Web Services
- 타카 마츠모토, 선임 클라우드 지원 엔지니어, Amazon Web Services
- 바산트 시르샛, 수석 EUC 스페셜리스트 SA, Amazon Web Services

참조 자료

자세한 내용은 다음을 참조하세요.

- 아마존 AppStream 2.0 관리 가이드
- 아마존 AppStream API 레퍼런스
- Windows File Server용 Amazon FSx 및 FSLogix를 사용하여 Amazon 2.0에서의 애플리케이션 설정 지속성을 최적화할 수 있습니다. AppStream
- 아마존 ElasticSearch 및 아마존 파이어호스로 아마존 AppStream 2.0 모니터링
- 아마존 아테나와 아마존을 사용하여 아마존 AppStream 2.0 사용 보고서를 분석하세요 QuickSight
- Amazon AppStream 2.0 플릿을 확장하세요
- AppLocker Microsoft를 사용하여 Amazon AppStream 2.0에서의 애플리케이션 경험을 관리합니다
- Amazon AppStream 2.0에서 사용자 지정 도메인 사용
- 2.0에서 자체 Microsoft RDS CAL을 AppStream 사용하려면 어떻게 해야 하나요?
- 아마존 AppStream 2.0 가격 책정 도구
- AppStream 2.0으로 온라인 소프트웨어 평가판 생성
- 아마존 2.0으로 SaaS 포털 만들기 AppStream

문서 수정

이 백서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
업데이트된 문서	탄력적 플릿, 속성 기반 애플리케이션 권한, 멀티스택 애플리케이션 카탈로그, Linux 기반 플릿, 데이터 수신 및 송신, 재해 복구 및 기타 업데이트를 포함하도록 업데이트되었습니다.	2022년 6월 14일
업데이트된 문서	HTML 버전이 게시되었습니다.	2023년 1월 19일
최초 게시	백서가 게시되었습니다.	2021년 6월 8일

고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공의 목적으로만 제공되고, (b) 사전 통지 없이 변경될 수 있는 현재 AWS 제품 및 관행을 나타내고, (c) AWS 및 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약속이나 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

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