Builders Online Series

기업 환경 변화에 신속하게 대응하는 안전한 솔루션 : AWS End User Computing

김종선
Solutions Architect

Agenda

data center is changing

Overview of Amazon WorkSpaces

Overview of Amazon AppStream 2.0

Overview of Amazon WorkDocs

Design considerations

More than the data center is changing

Workforce increasingly agile

1 in 5[1]
jobs
are held by contractors

79%[2]
of organizations
expect an increase in M&A

Security increasingly important

70%[3]
of workers
worked remotely

1 in 4[4]
data breaches
involve lost or stolen devices

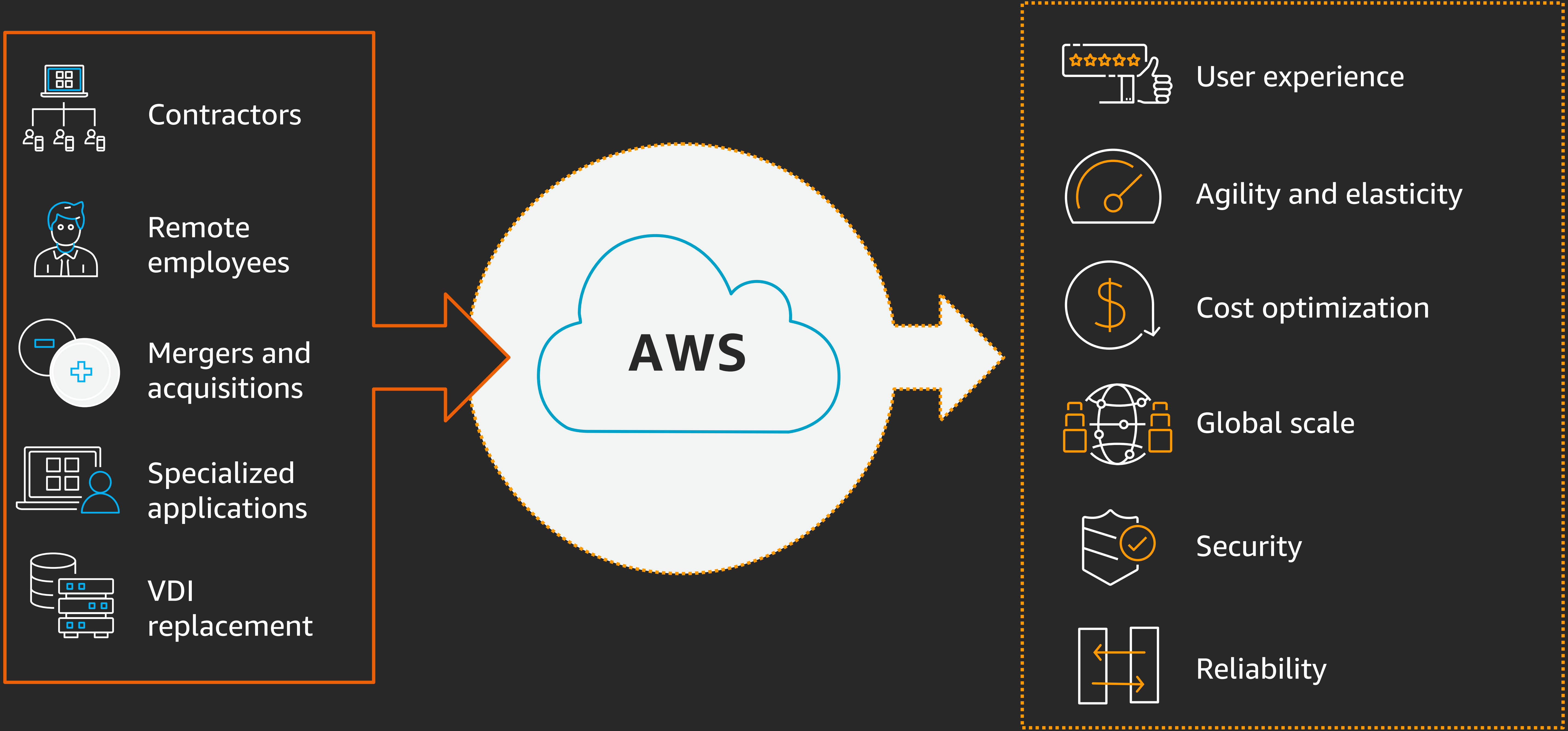
Moving to Desktop-as-a-Service (DaaS):

51%[5]

up from 43% in 2017

1. https://www.npr.org/2018/01/23/579690595/the-mystery-of-contract-work-why-so-many-guys
2. https://www2.deloitte.com/us/en/pages/mergers-and-acquisitions/articles/m-a-trends-report.html
3. https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html
4. https://www.trendmicro.com/vinfo/us/security/definition/data-breach
5. https://reprints.forrester.com/#/assets/2/374/RES135901/reports

Customers are choosing AWS



AWS end-user computing services

amazon AppStream 2.0

Application streaming

amazon Worklink

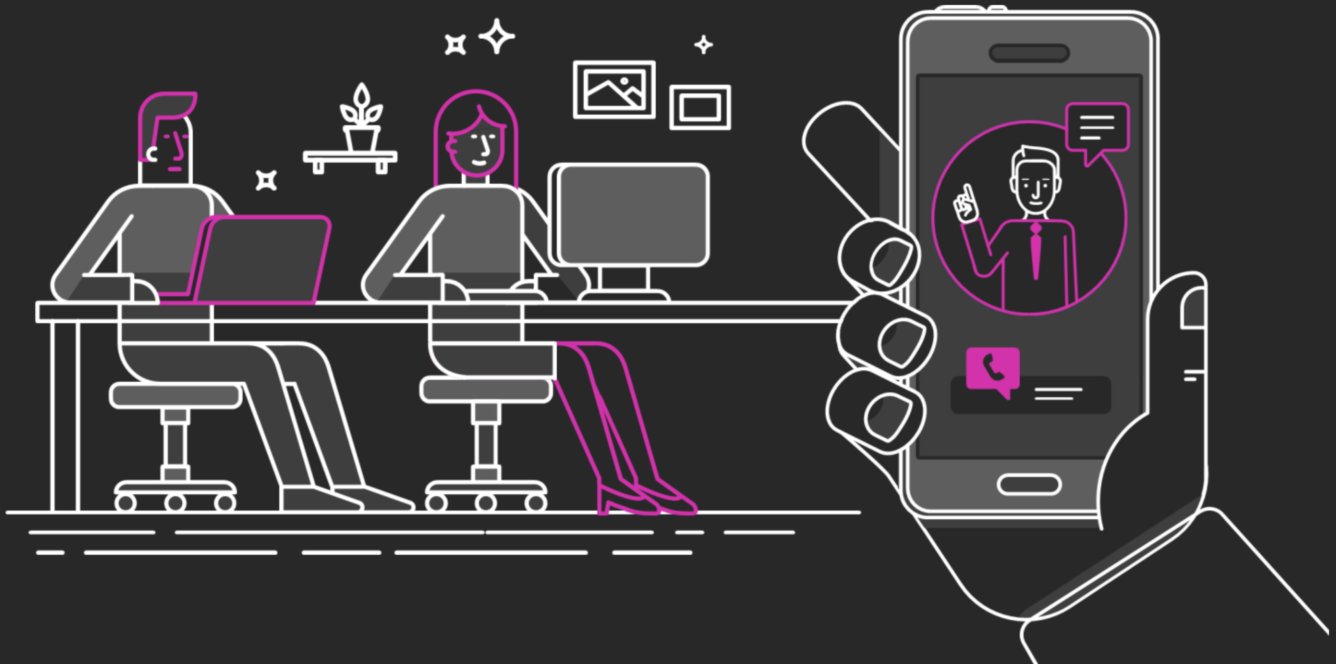
Mobile web access

amazon WorkSpaces

Desktop-as-a-Service

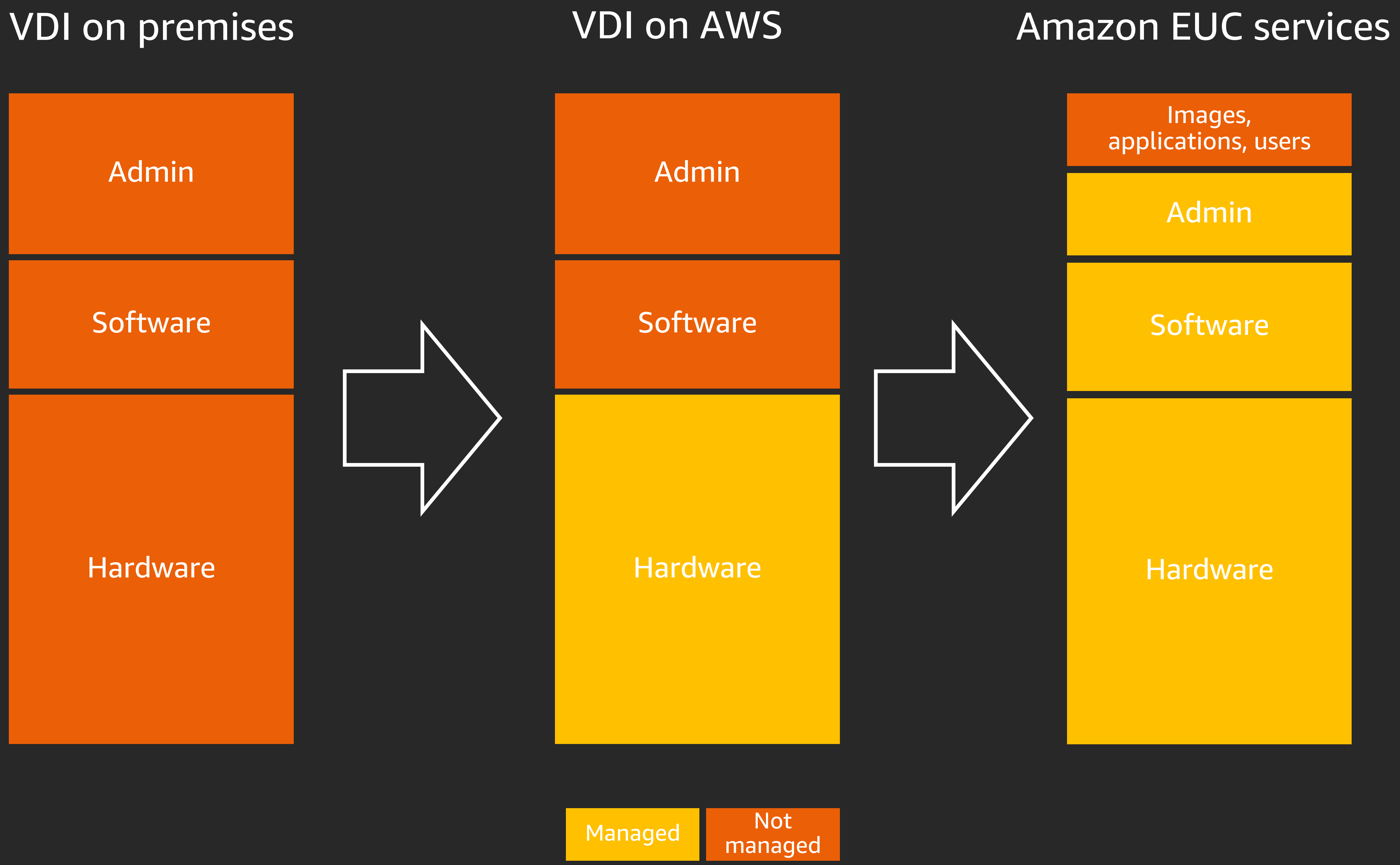
amazon WorkDocs

File storage



- Fully-managed
- Reliable & secure
- Pay-as-you-go

Fully managed



VDI on premises

Admin

Software

Hardware

VDI on AWS

Admin

Software

Hardware

Amazon EUC services

Images, applications, users

Admin

Software

Hardware

Managed

Not managed

Customers

AccelerEd Innovation Works Here.
Radboud University
MathWorks
EVARI GIS Consulting
IMDb
AMGEN
DiSTI
Case Western Reserve University EST. 1826

Serverworks
GulfMark
EndemolShine Group
SIEMENS Ingenuity for life
GERBER TECHNOLOGY
SOLIDWORKS
AUTODESK
CMC

8K Miles
AVEVA
The Whitsundays Queensland 74 Island Wonders
GE
geneia
Ayuntamiento de ALCOBENDAS
CONDÉ NAST
technologyone Transforming business, making life simple
ROK TECHNOLOGIES

eDelivery
YAMAHA
BiZZdesign
GATEWAY On Call. On Time. On Target.
corexpert by TEAMWORK
Compuware
Biogen

planalytics
OLIKKA Be Great. Be Different.
HALLIBURTON
JAMES COOK UNIVERSITY AUSTRALIA
THE UNIVERSITY OF MELBOURNE
MELBOURNE BUSINESS SCHOOL
media interactiva
Vanguard
The Software Experts Crayon

brillio
multiview FINANCIAL SOFTWARE
BLADE ENERGY PARTNERS
MACQUARIE University
GRAYHAIR
Origlio Beverage
University of Virginia
McINTIRE SCHOOL of COMMERCE

Purolator
ASU Arizona State University
SAMSUNG
SAMSUNG ENGINEERING
WORLDWIDE EXPRESS
MONROE WHEELCHAIR
CAMPUS CONSTRUCTION MANAGEMENT Building on Knowledge
Privo
VEOLIA

Overview of Amazon WorkSpaces

Amazon WorkSpaces

Access desktops from anywhere on any device

Improve security and compliance posture

Simplify desktop management

Optimize costs with flexible bundles and pricing options

Fully managed, secure Linux or Windows desktops on AWS

AWS re:Invent hands-on labs

Improves security

No sensitive data on user devices

Storage encrypted at rest

Desktop stream encrypted in transit

Amazon WorkSpaces encrypts data and streams and keeps information off devices

Plays well with existing tools

Intranet

Microsoft Active Directory

Multifactor authentication (MFA)
(RADIUS-based)

Systems/patch management
(SCCM, BigFix, WSUS)

Certificate authority

Amazon WorkSpaces integrates easily with your on-premises tools and network

Amazon WorkSpaces flexibility

Clients

Desktop
Mobile
Web

Operating system

Windows 10
Amazon Linux2 LTS

Bundles

Value
Standard
Performance
Power
PowerPro
Graphics
GraphicsPro

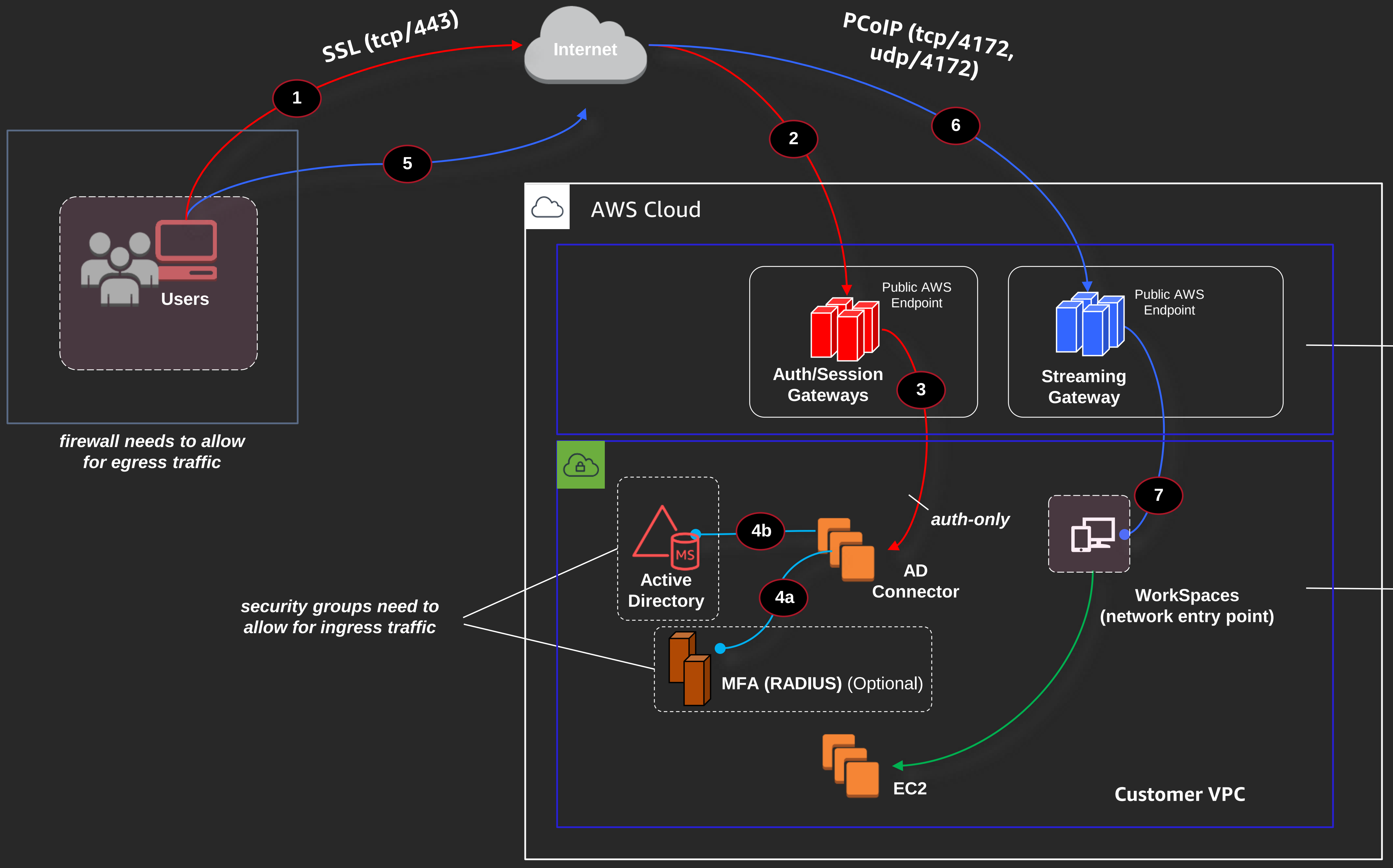
Flexible pricing

Monthly
Hourly
BYOL

Standalone Network

NETWORK TRAFFIC LEGEND

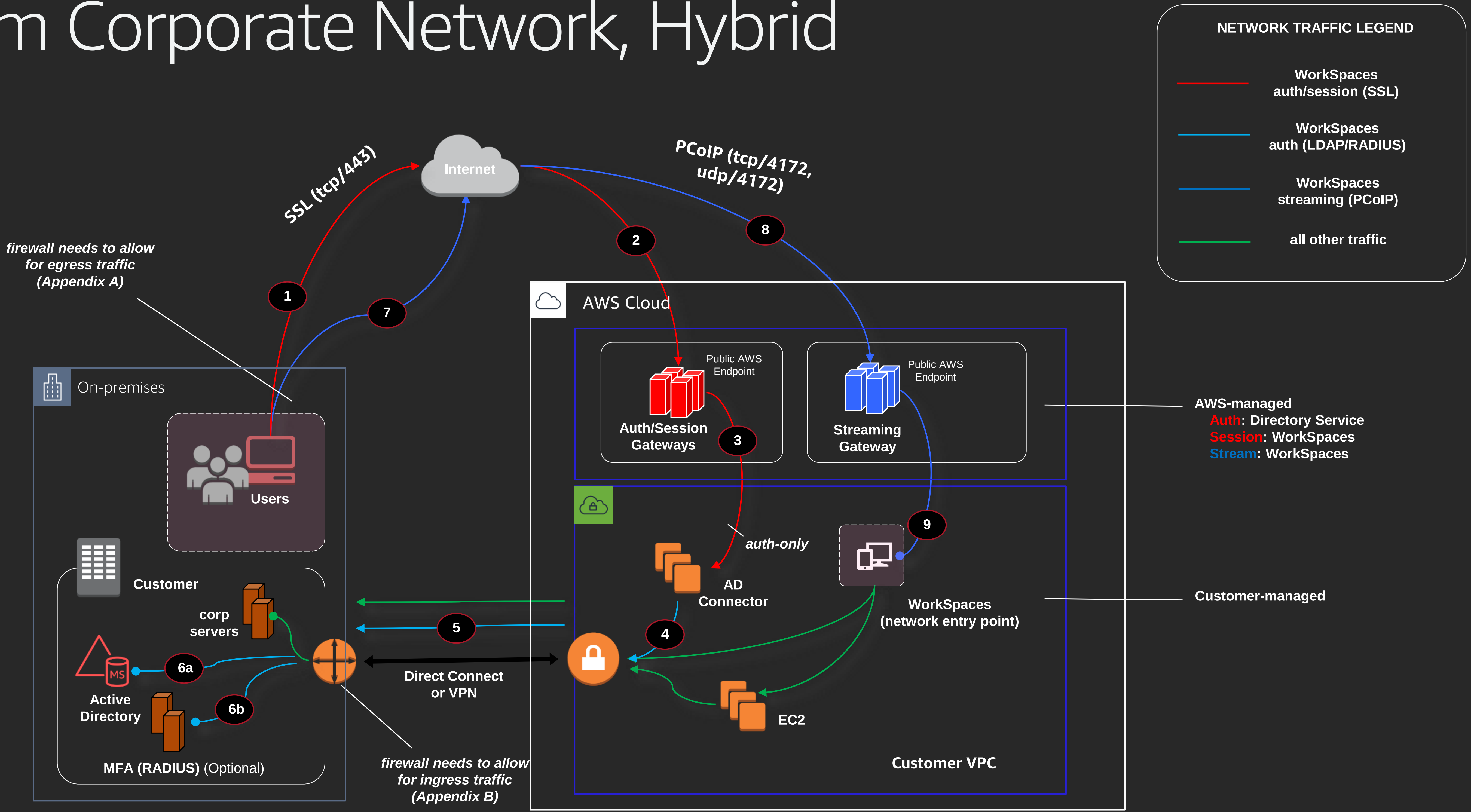
- 🟥 WorkSpaces auth/session (SSL)
- 🟦 WorkSpaces auth (LDAP/RADIUS)
- 🟦 WorkSpaces streaming (PCoIP)
- 🟩 all other traffic



AWS-managed
Auth: Directory Service
Session: WorkSpaces
Stream: WorkSpaces

Customer-managed

From Corporate Network, Hybrid



NETWORK TRAFFIC LEGEND

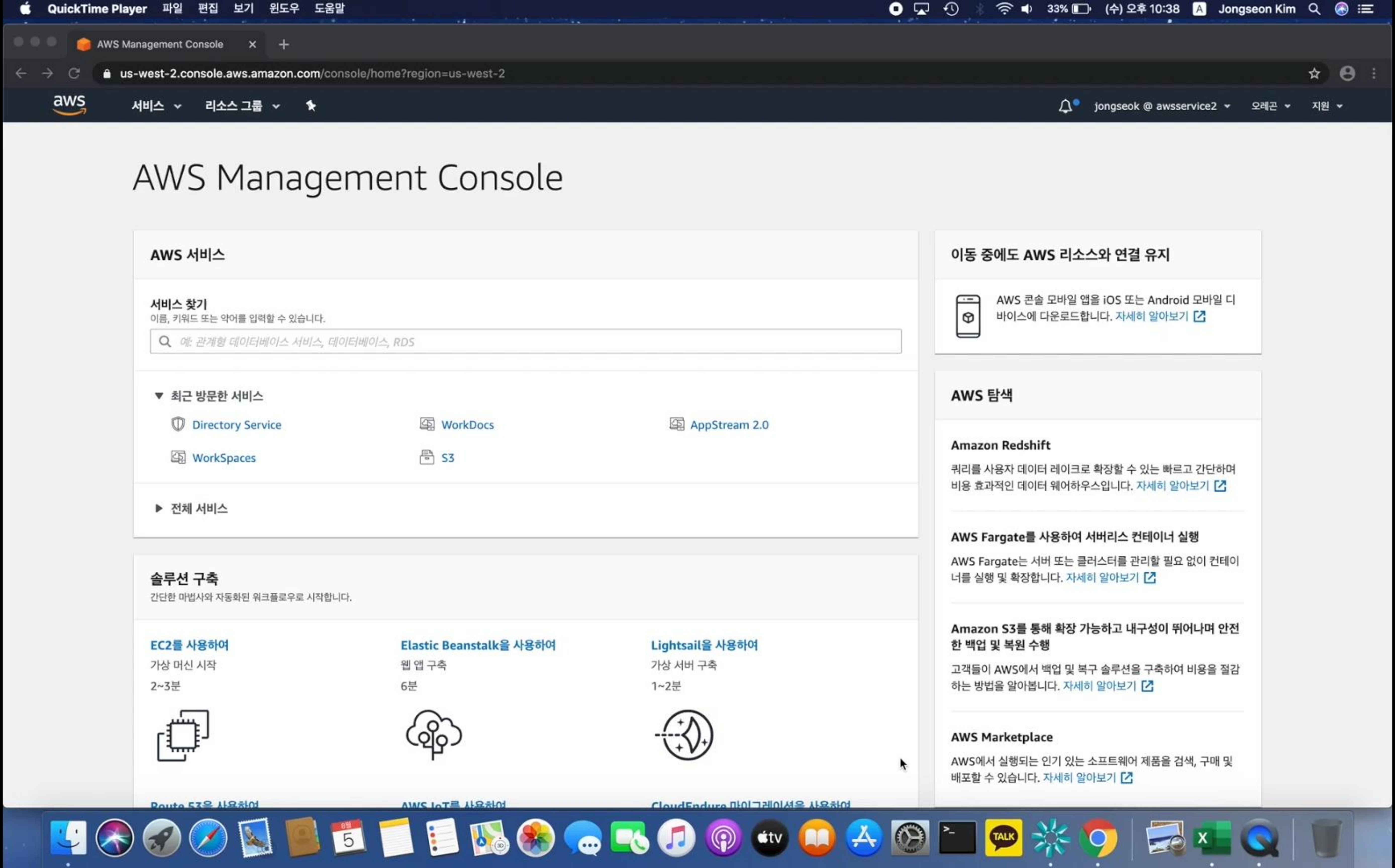
- WorkSpaces auth/session (SSL)
- WorkSpaces auth (LDAP/RADIUS)
- WorkSpaces streaming (PCoIP)
- all other traffic

firewall needs to allow for egress traffic (Appendix A)

firewall needs to allow for ingress traffic (Appendix B)

AWS-managed
Auth: Directory Service
Session: WorkSpaces
Stream: WorkSpaces

Customer-managed



AWS Management Console

AWS 서비스

서비스 찾기
이름, 키워드 또는 약어를 입력할 수 있습니다.

예: 관계형 데이터베이스 서비스, 데이터베이스, RDS

▼ 최근 방문한 서비스

- Directory Service
- WorkDocs
- AppStream 2.0
- WorkSpaces
- S3

▶ 전체 서비스

솔루션 구축

간단한 마법사와 자동화된 워크플로우로 시작합니다.

EC2를 사용하여
가상 머신 시작
2~3분

Elastic Beanstalk을 사용하여
웹 앱 구축
6분

Lightsail을 사용하여
가상 서버 구축
1~2분

Route 53을 사용하여

AWS IoT를 사용하여

CloudEndure 마이그레이션을 사용하여

이동 중에도 AWS 리소스와 연결 유지

AWS 콘솔 모바일 앱을 iOS 또는 Android 모바일 디바이스에 다운로드합니다. 자세히 알아보기

AWS 탐색

Amazon Redshift

쿼리를 사용자 데이터 레이크로 확장할 수 있는 빠르고 간단하며 비용 효과적인 데이터 웨어하우스입니다. 자세히 알아보기

AWS Fargate를 사용하여 서버리스 컨테이너 실행

AWS Fargate는 서버 또는 클러스터를 관리할 필요 없이 컨테이너를 실행 및 확장합니다. 자세히 알아보기

Amazon S3를 통해 확장 가능하고 내구성이 뛰어나며 안전한 백업 및 복원 수행

고객들이 AWS에서 백업 및 복구 솔루션을 구축하여 비용을 절감하는 방법을 알아봅니다. 자세히 알아보기

AWS Marketplace

AWS에서 실행되는 인기 있는 소프트웨어 제품을 검색, 구매 및 배포할 수 있습니다. 자세히 알아보기

Overview of Amazon AppStream 2.0

Amazon AppStream 2.0

Secure application streaming

Centrally manage applications

It integrates with existing IT

Scale without infrastructure

amazon AppStream 2.0

Deliver desktop applications to any computer

A Managed Service: Breaking down the stack

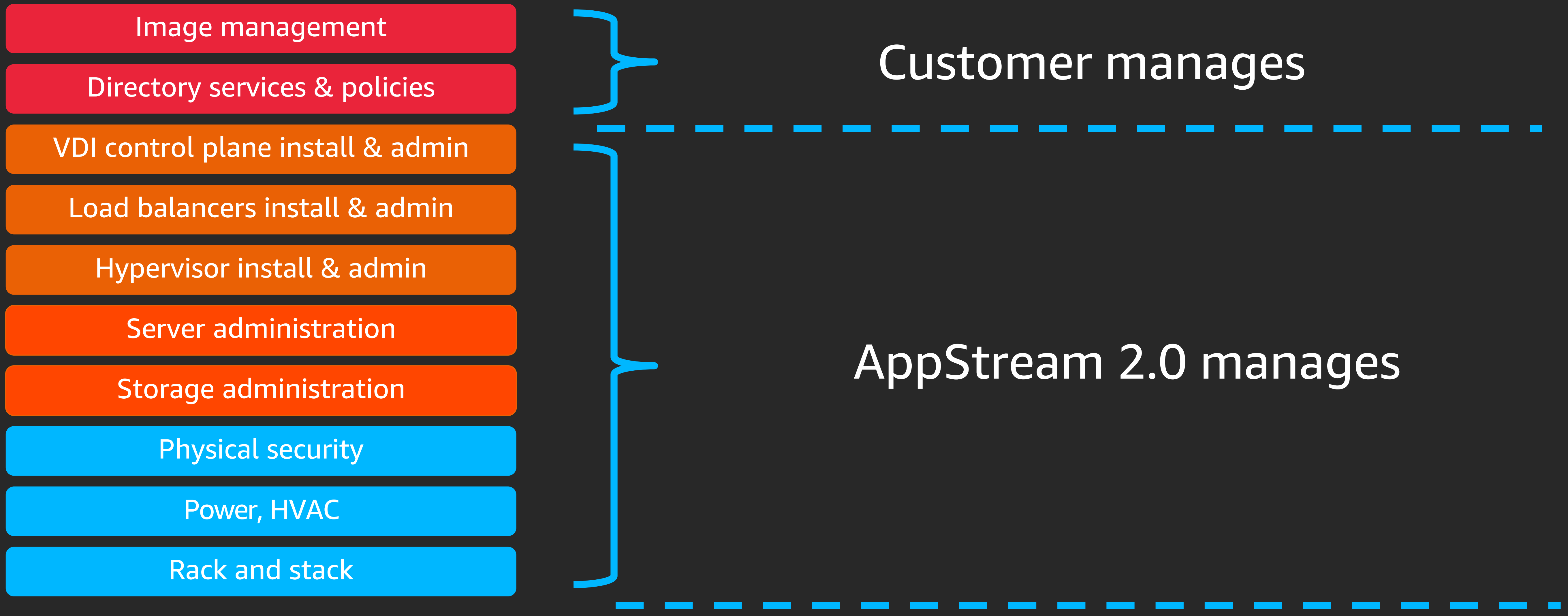


Image management

Directory services & policies

VDI control plane install & admin

Load balancers install & admin

Hypervisor install & admin

Server administration

Storage administration

Physical security

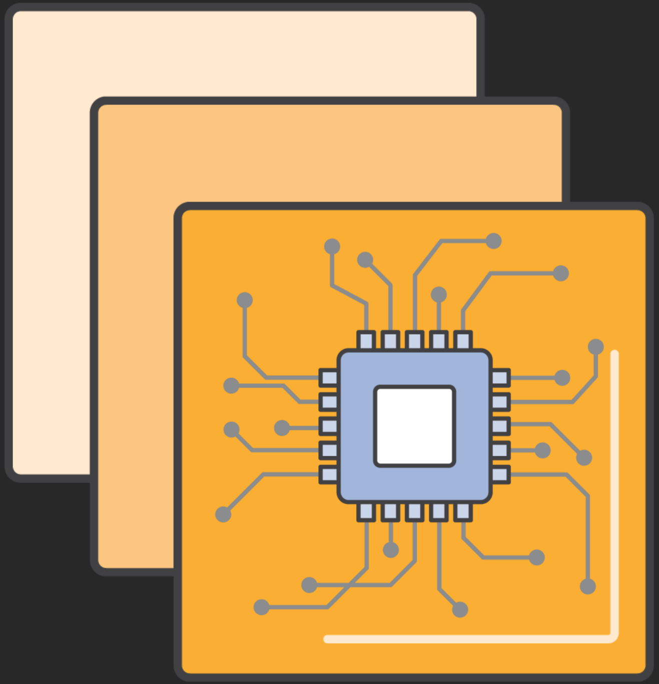
Power, HVAC

Rack and stack

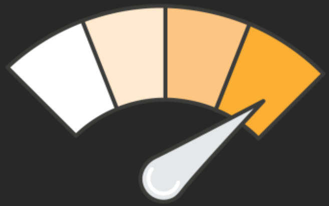
Customer manages

AppStream 2.0 manages

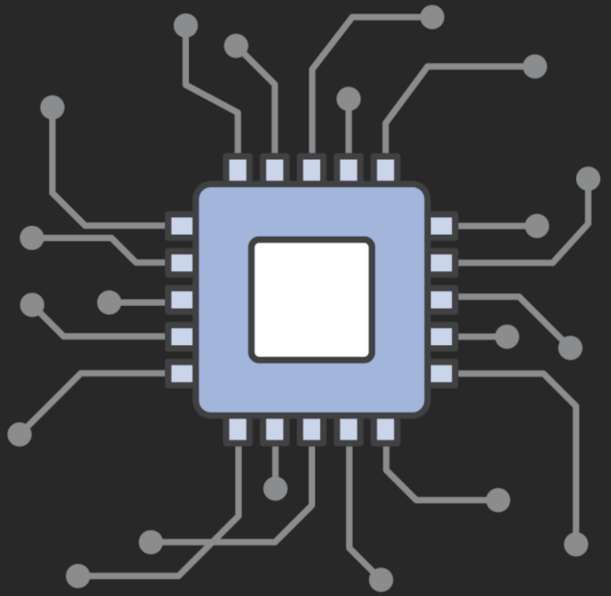
Multiple instance families



- One session – one VM = consistent performance
- Match application workload to instance characteristics
  - General purpose: Knowledge-worker applications
  - Compute optimized: Compute-bound applications that benefit from high-performance processors
  - Memory optimized: Applications that process large datasets in memory
  - Graphics optimized: High graphics requirements



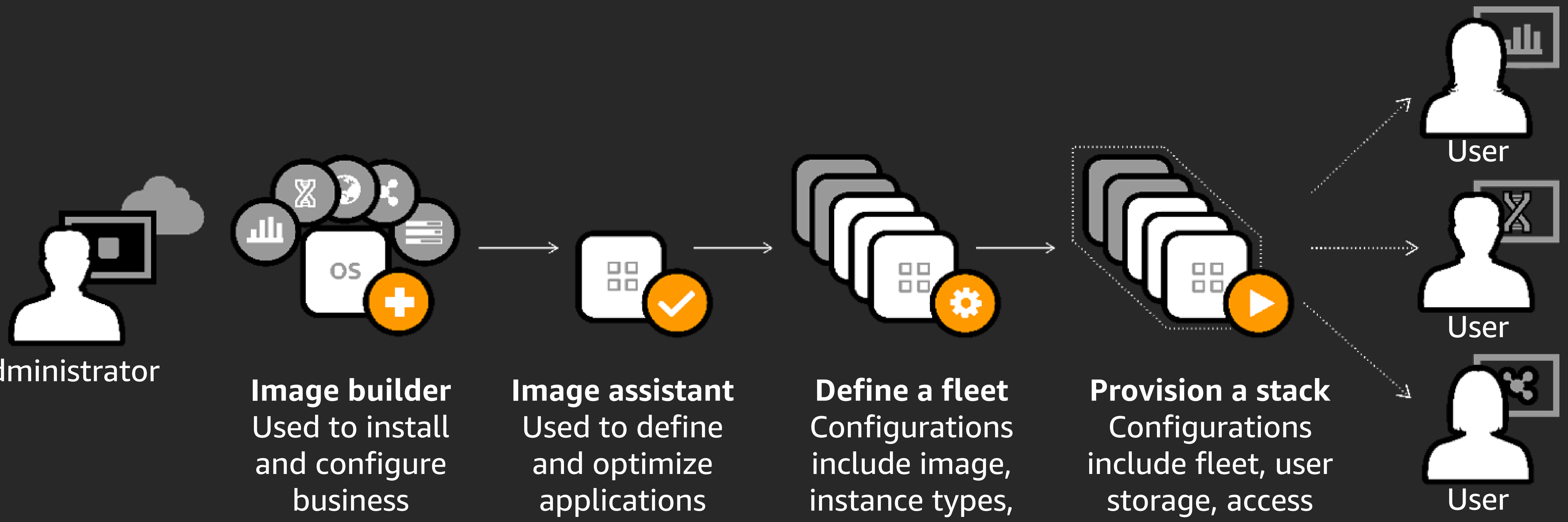
Graphics instance families



Instance family	Graphics G4	Graphics design	Graphics pro
Number of instance sizes	6	4	3
Price	$1.00 ~ $10.28	$0.25 ~ $2.00	$2.05 ~ $8.20
GPU memory	16 GiB	1–8 GiB	8–32 GiB
vCPUs	4 ~ 64	2 ~16	16 ~ 64
Instance memory	16 ~ 256 GiB	7.5 ~ 61 GiB	122 ~ 488 GiB
GPU vendor	NVIDIA T4	AMD FirePro S7150x2	NVIDIA Tesla M60
Libraries supported	CUDA, DirectX, OpenGL, OpenCL	DirectX, OpenGL, OpenCL	CUDA, DirectX, OpenGL, OpenCL

https://aws.amazon.com/appstream2/pricing/?nc=sn&loc=4

AppStream 2.0 administrator workflow



Administrator

Image builder
Used to install and configure business applications

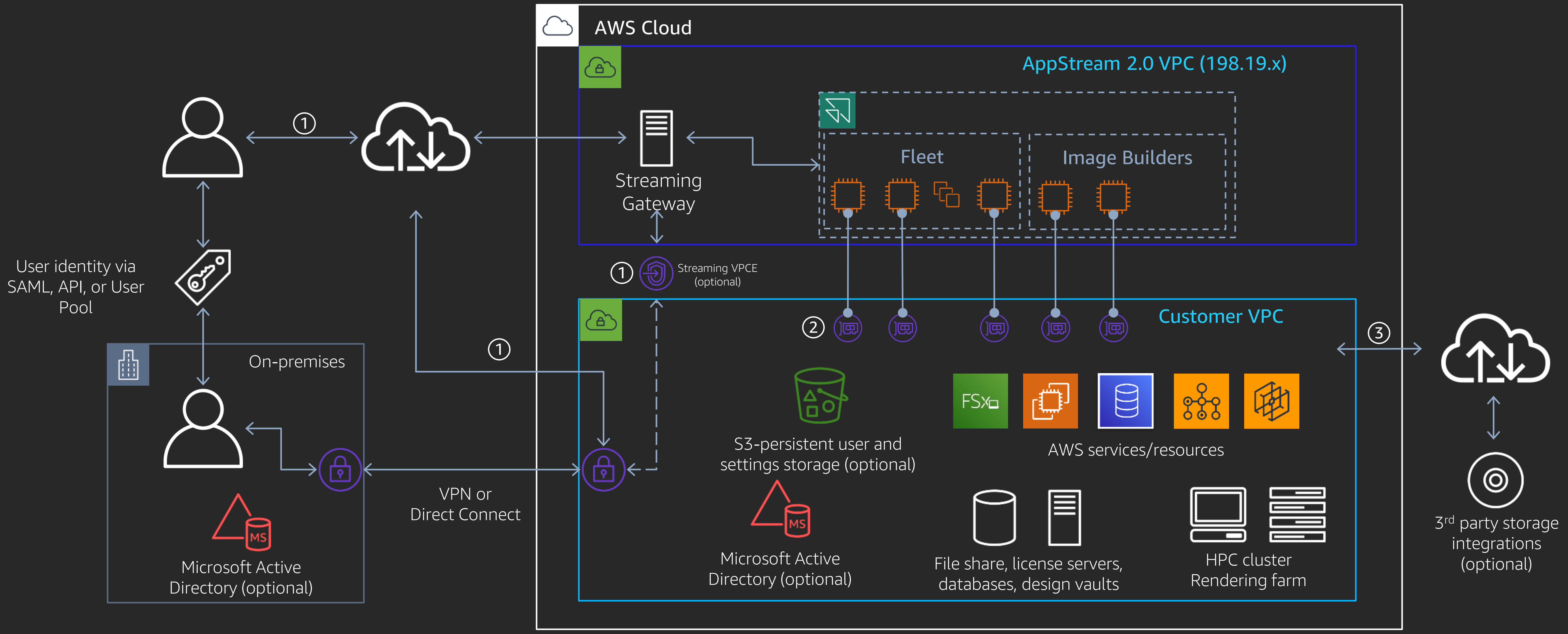
Image assistant
Used to define and optimize applications presented, configure default user settings, and create an image

Define a fleet
Configurations include image, instance types, networking, and scaling configurations

Provision a stack
Configurations include fleet, user storage, access permission options, and customer branding

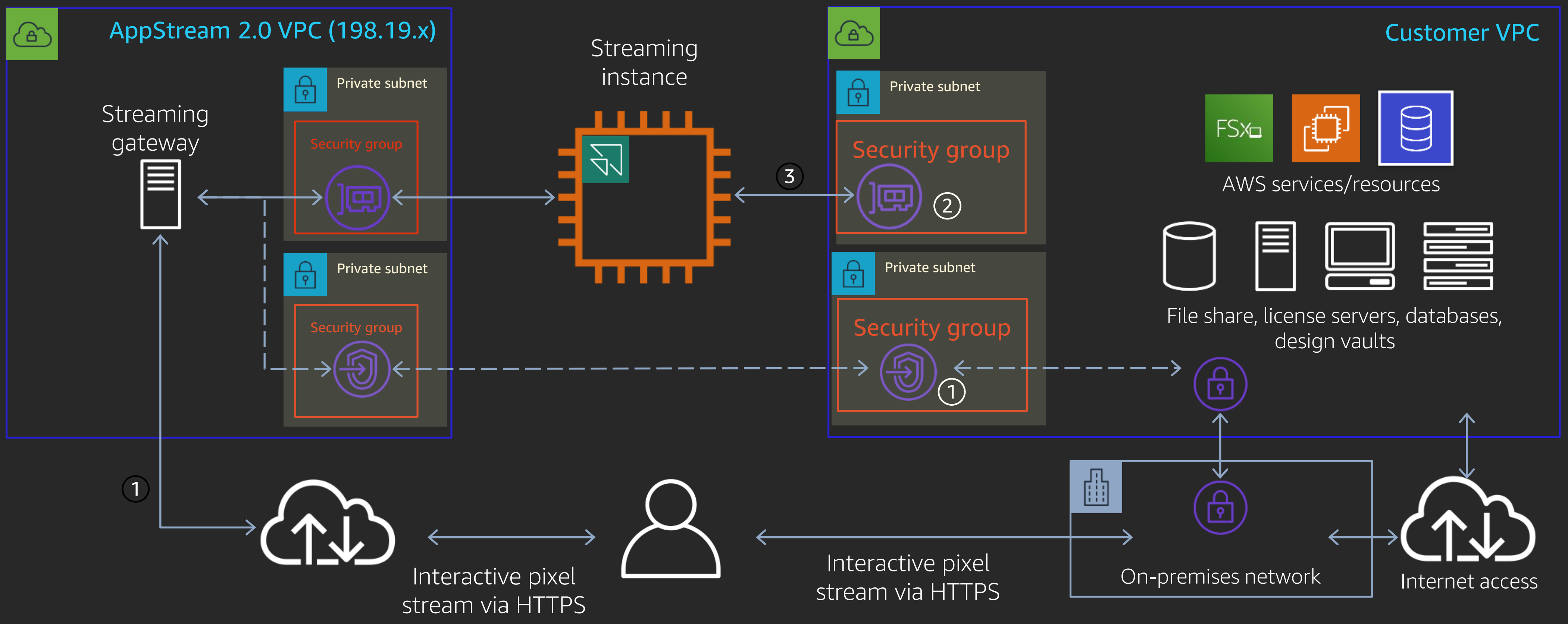
AD + SAML or user pools
Used to define users and grant stack access

AppStream 2.0 - Network Flow


AWS Cloud
AppStream 2.0 VPC (198.19.x)
①
Streaming Gateway
Fleet
Image Builders
User identity via SAML, API, or User Pool
On-premises
Microsoft Active Directory (optional)
①
VPN or Direct Connect
①
Streaming VPCE (optional)
②
Customer VPC
③
S3-persistent user and settings storage (optional)
FSx
AWS services/resources
Microsoft Active Directory (optional)
MS
File share, license servers, databases, design vaults
HPC cluster Rendering farm
3rd party storage integrations (optional)

1. Connectivity to AppStream 2.0 uses HTTPS via TCP443 over the internet
   a) Using the optional streaming VPCE maintains the pixel, USB, user input, audio, clipboard, file upload/download, and printer traffic within the customer VPC
   b) The user needs internet access for the AppStream 2.0 web assets and authentication
2. Security groups are used to control network access to the customer VPC
3. AppStream 2.0 streaming instance access to the internet is through the customer VPC

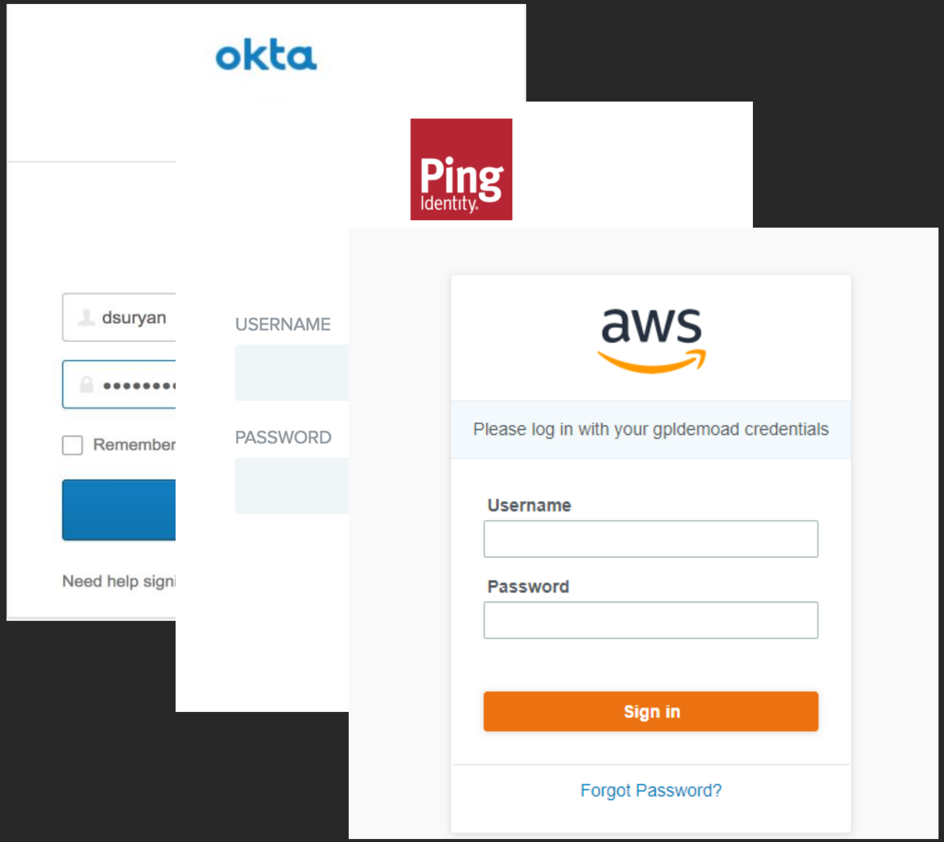
AppStream 2.0 - Instance network details



- The AppStream 2.0 streaming instance is in the AWS-managed VPC with an Elastic Network Interface (ENI) in the customer-selected VPC/subnet
- Fleet streaming instances are ephemeral; they are terminated after the user session completes
- Streaming instances are launched from the customer-created image with the instance type and size chosen

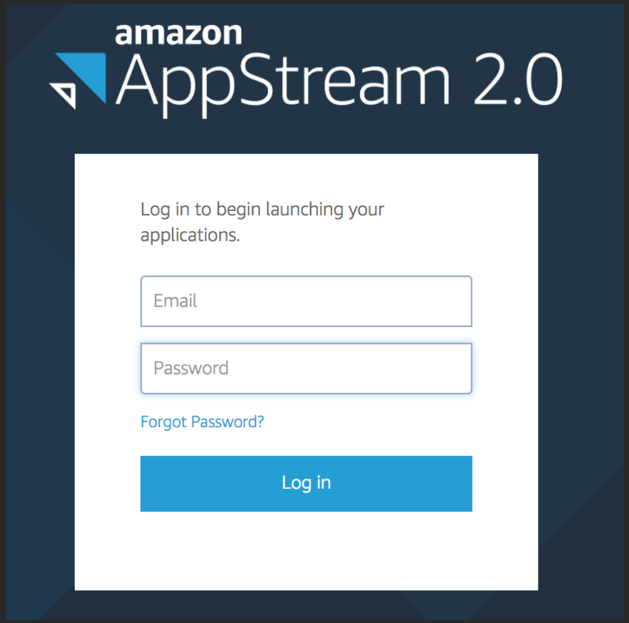
1. Connectivity to AppStream 2.0 uses HTTPS via TCP443 over the Internet
   a) Using the optional streaming VPCE maintains the pixel, USB, user input, audio, clipboard, file upload/download, and printer traffic within the customer VPC
   b) The user needs Internet access for the AppStream 2.0 web assets and authentication
2. Security groups are used to control network access to the customer VPC
3. All user-generated traffic is through the customer network interface/VPC

Identity: Bring your own or built-in



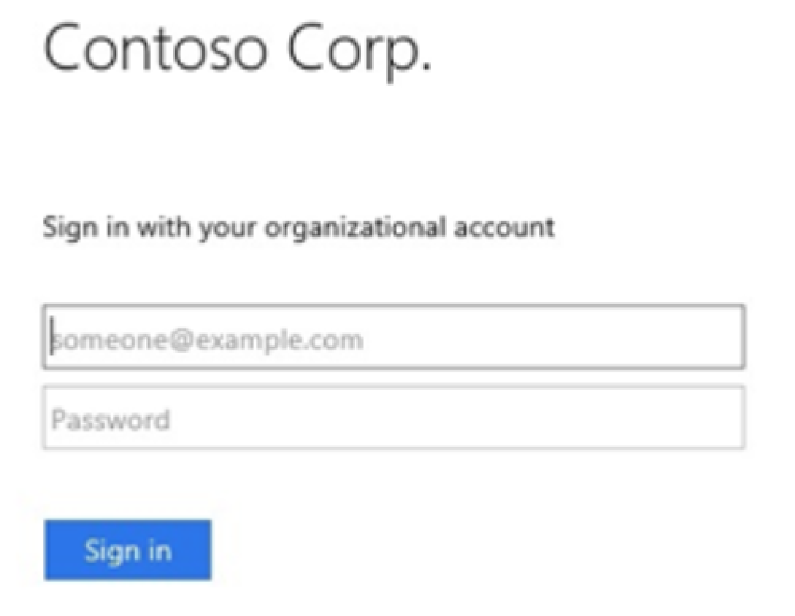
Please log in with your gpldemoad credentials

SAML 2.0



Log in to begin launching your applications.

Built-in user pool

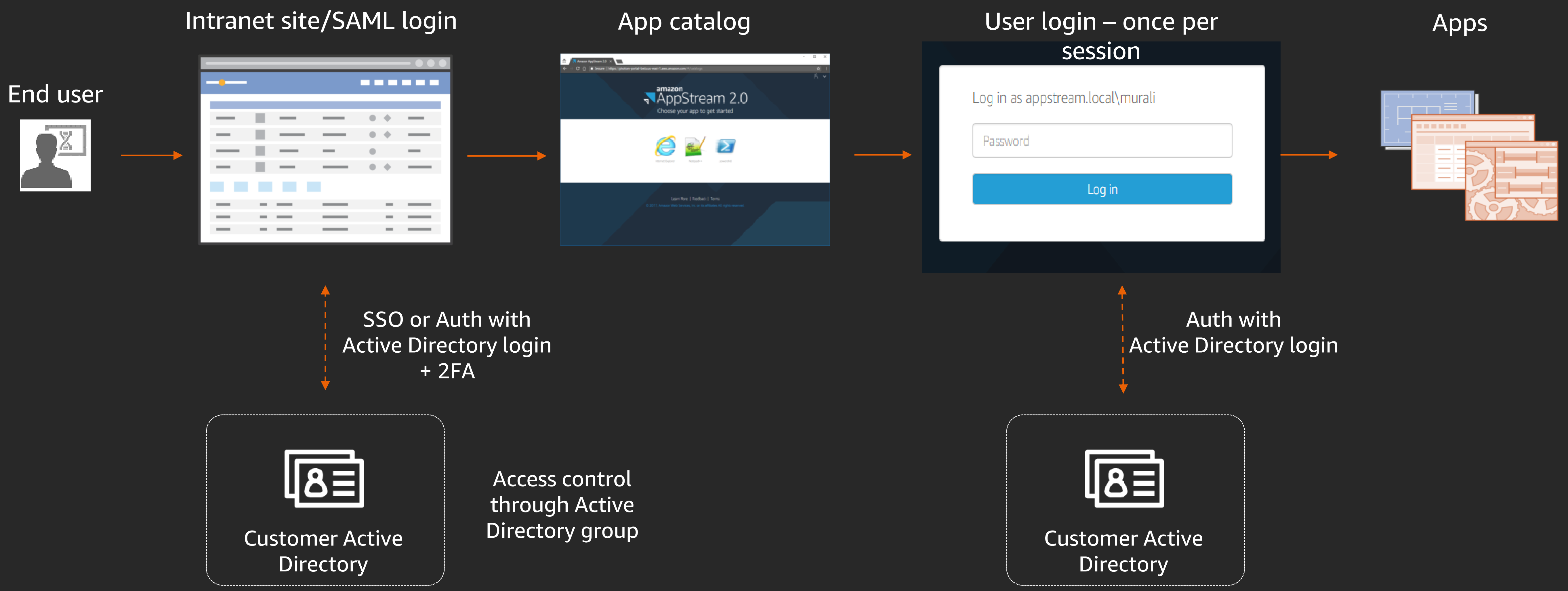


Contoso Corp.

Sign in with your organizational account

Custom identity

Domain join: User experience



End user

Intranet site/SAML login

App catalog

amazon AppStream 2.0

Choose your app to get started

User login – once per session

Log in as appstream.local\murali

Password

Log in

Apps

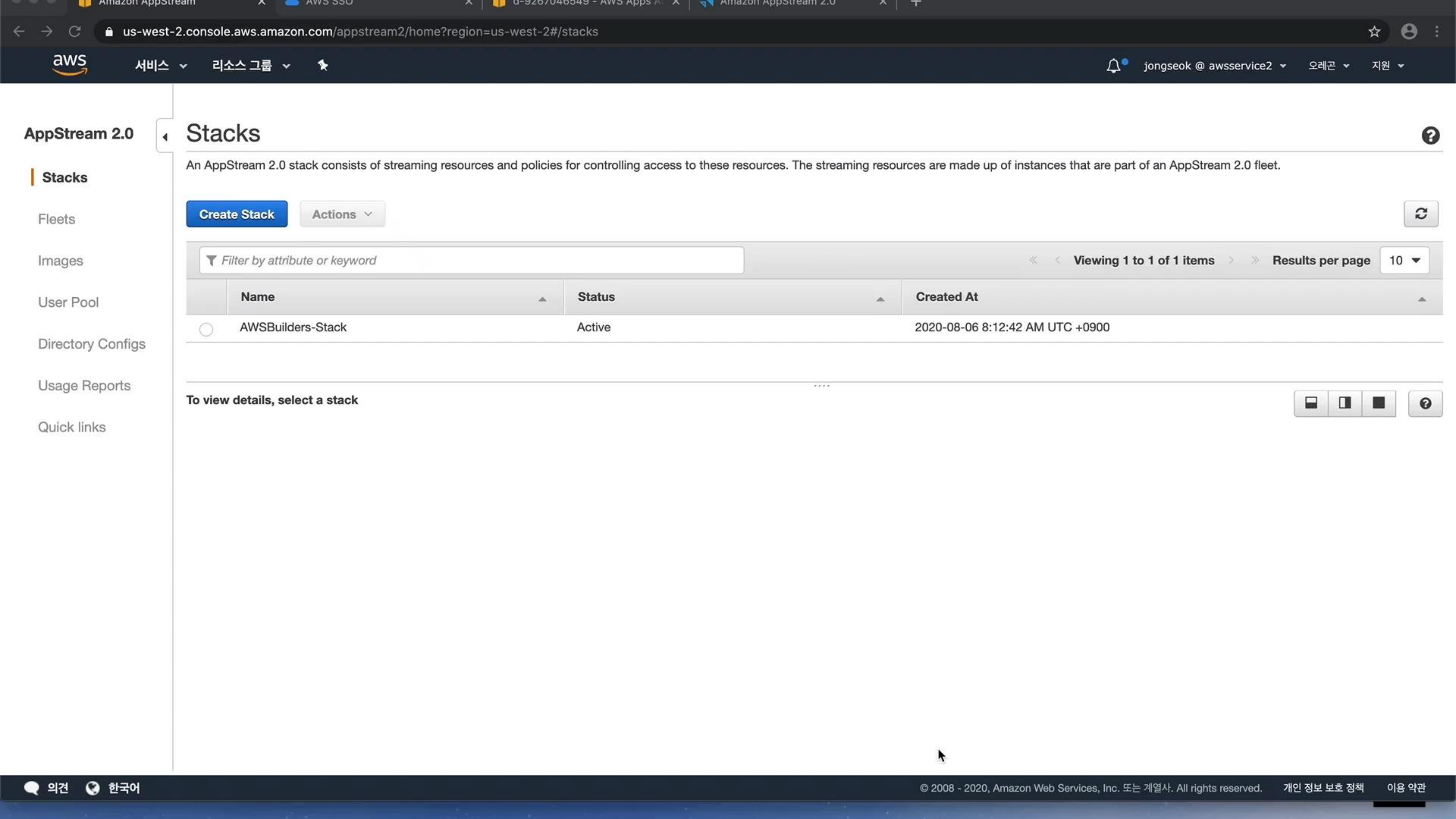
SSO or Auth with Active Directory login + 2FA

Customer Active Directory

Access control through Active Directory group

Auth with Active Directory login

Customer Active Directory



Stacks

An AppStream 2.0 stack consists of streaming resources and policies for controlling access to these resources. The streaming resources are made up of instances that are part of an AppStream 2.0 fleet.

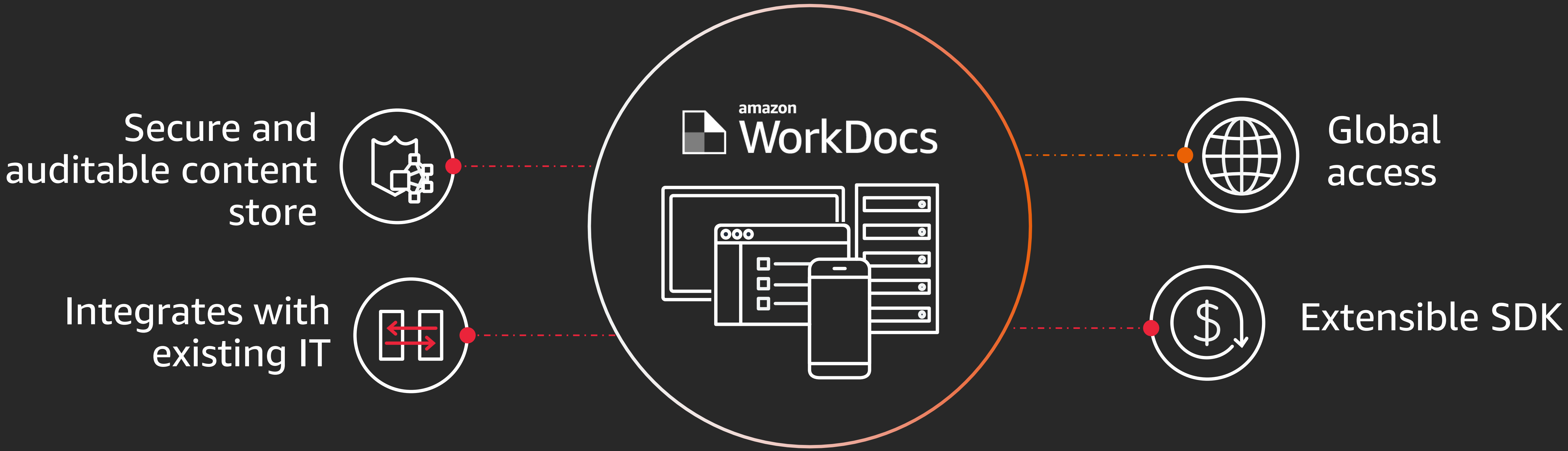
	Name	Status	Created At
○	AWSBuilders-Stack	Active	2020-08-06 8:12:42 AM UTC +0900

To view details, select a stack

© 2008 - 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

Overview of Amazon WorkDocs

Amazon WorkDocs



amazon WorkDocs
Secure and auditable content store
Integrates with existing IT
Global access
Extensible SDK

Secure, fully managed file storage with an extensible SDK

Amazon WorkDocs Features

Secure File Sharing

Enterprise security

Replace network file shares

Real time auditing and compliance

Smart search

Tasks and simple workflows

Mobile and field productivity

Developer SDK for integration

Security

User security

Strong Authentication, authorization, and access controls
Enterprise AD integration
OAuth 2.0 Authentication
Multi-factor Authentication

Site security controls

Sharing controls
Storage limits
Real time site wide activity auditing
User management

File security controls

Auditing and reporting
Unlimited versions
Recycle restores within 180 days
Disable file downloads & print
Links with expiration and access code

Governance and compliance

HIPAA compliant
PCI/DSS compliant
ISO 9001, 27001, 27017, 27018

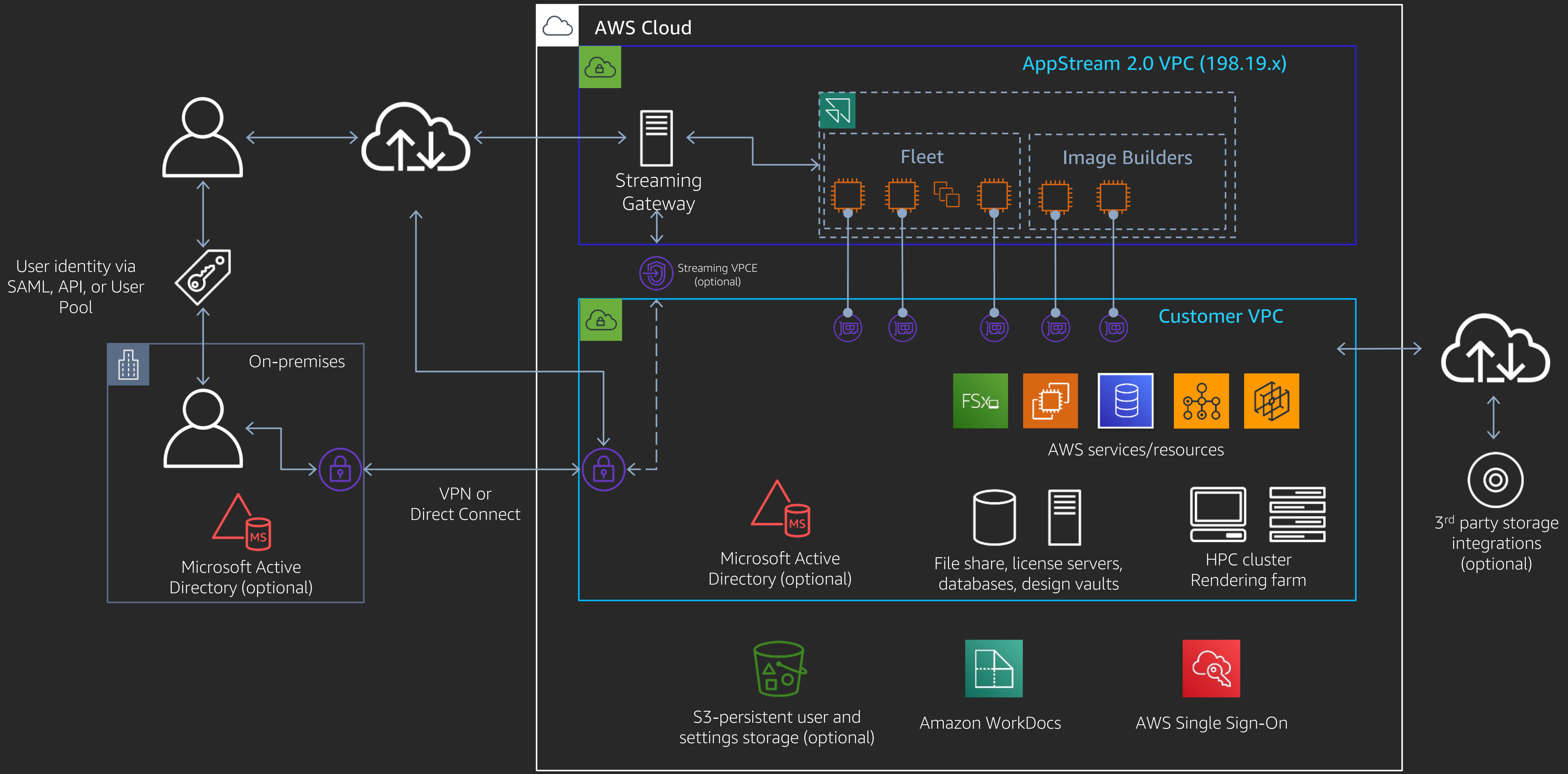
Network security

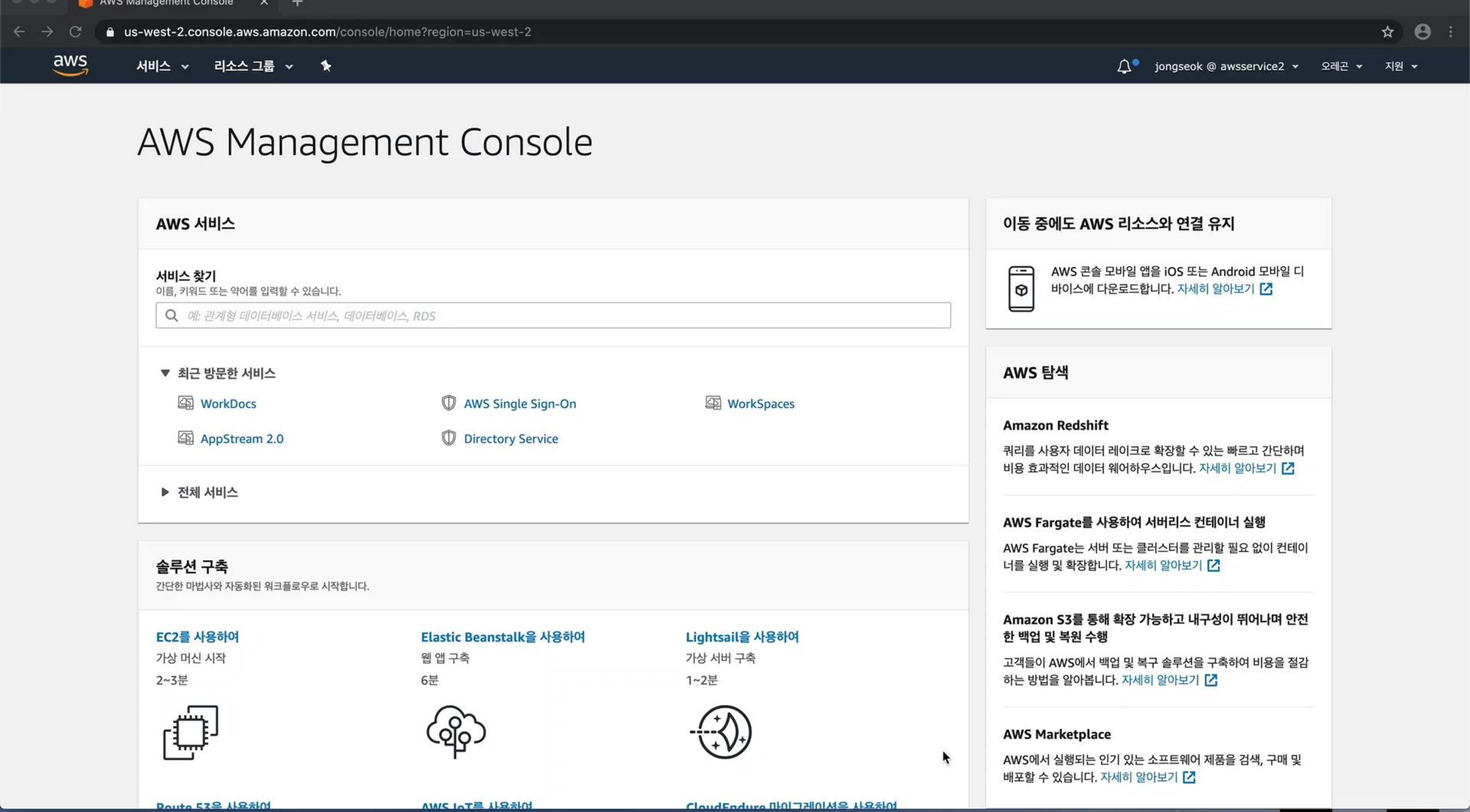
SSL/TLS secure tunnel for files transmission
256-bit encryption applied to all data in rest and transit

Datacenter security

SSAE 16 and SAS 70 compliant
Disaster recovery policies
Continuous threat assessment
Physical security, 24-hour surveillance
Biometric access controls

AppStream 2.0 & WorkDocs - Network Flow


AWS Cloud
AppStream 2.0 VPC (198.19.x)
Streaming Gateway
Fleet
Image Builders
Streaming VPCE (optional)
Customer VPC
User identity via SAML, API, or User Pool
On-premises
Microsoft Active Directory (optional)
VPN or Direct Connect
FSx
AWS services/resources
Microsoft Active Directory (optional)
File share, license servers, databases, design vaults
HPC cluster Rendering farm
3rd party storage integrations (optional)
S3-persistent user and settings storage (optional)
Amazon WorkDocs
AWS Single Sign-On



AWS Management Console

AWS 서비스

서비스 찾기
이름, 키워드 또는 약어를 입력할 수 있습니다.

예: 관계형 데이터베이스 서비스, 데이터베이스, RDS

▼ 최근 방문한 서비스

- WorkDocs
- AppStream 2.0
- AWS Single Sign-On
- Directory Service
- WorkSpaces

▶ 전체 서비스

솔루션 구축

간단한 마법사와 자동화된 워크플로우로 시작합니다.

EC2를 사용하여
가상 머신 시작
2~3분

Elastic Beanstalk을 사용하여
웹 앱 구축
6분

Lightsail을 사용하여
가상 서버 구축
1~2분

Route 53을 사용하여

AWS IoT를 사용하여

CloudEndure 마이그레이션을 사용하여

이동 중에도 AWS 리소스와 연결 유지

AWS 콘솔 모바일 앱을 iOS 또는 Android 모바일 디바이스에 다운로드합니다. 자세히 알아보기

AWS 탐색

Amazon Redshift

쿼리를 사용자 데이터 레이크로 확장할 수 있는 빠르고 간단하며 비용 효과적인 데이터 웨어하우스입니다. 자세히 알아보기

AWS Fargate를 사용하여 서버리스 컨테이너 실행

AWS Fargate는 서버 또는 클러스터를 관리할 필요 없이 컨테이너를 실행 및 확장합니다. 자세히 알아보기

Amazon S3를 통해 확장 가능하고 내구성이 뛰어나며 안전한 백업 및 복원 수행

고객들이 AWS에서 백업 및 복구 솔루션을 구축하여 비용을 절감하는 방법을 알아봅니다. 자세히 알아보기

AWS Marketplace

AWS에서 실행되는 인기 있는 소프트웨어 제품을 검색, 구매 및 배포할 수 있습니다. 자세히 알아보기

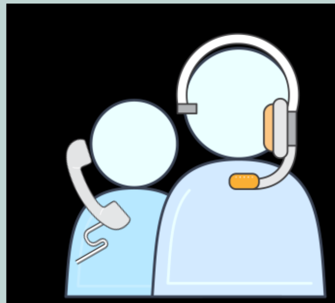
Design considerations

The approach

- Decide on user segmentation
- Select the initial use cases
- Evaluate performance characteristics
- Build the pilot solution
- Run user acceptance testing
- Deploy
- Iterate

Corporate personas and use cases

Typical business drivers: End user experience | TCO | Security



Task workers

Call center

WorkSpaces

Standard bundle

AppStream 2.0

General-purpose instances

Devices
Thin client,* zero client,* or lower-end laptop

User experience
Willing to work as directed

Applications
Web and a few low-compute-intensity apps

Specialists

Designer, developer, analyst, finance

WorkSpaces

PowerPro, Graphics, or GraphicsPro;

WorkSpaces for Linux for developers;

AppStream if only 1–2 apps

Devices
BYOD or corporate device

User experience
Near-native responsiveness and experience; full desktop

Applications
A few high-intensity apps

Knowledge workers

Sales, marketing, finance, operations, manufacturers

WorkSpaces

Standard, performance or Power bundles

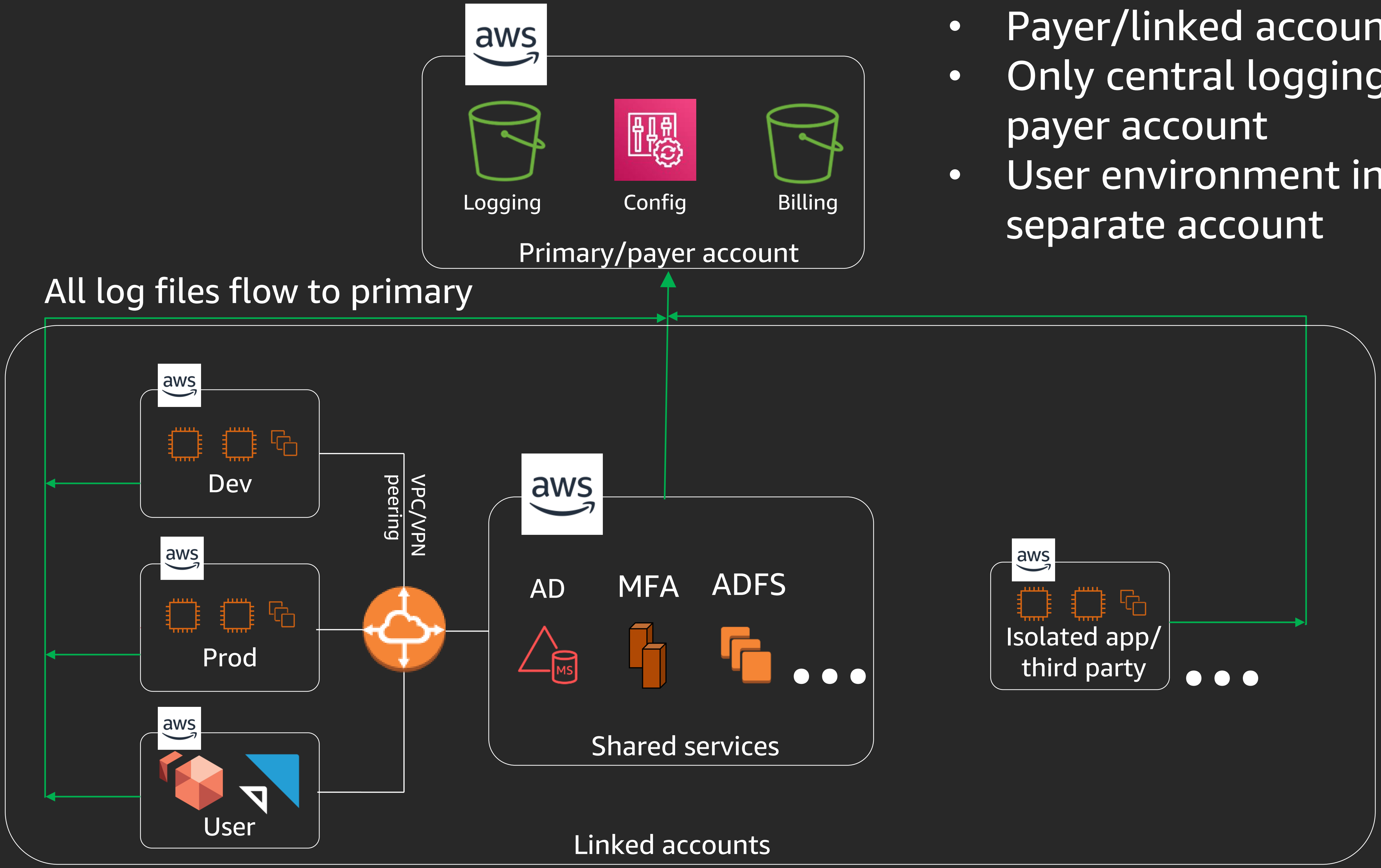
Devices
BYOD or agency device

User Experience
Near-native responsiveness and experience; full desktop

Applications
Variety of applications over time

*Thin and zero clients for WorkSpaces require working directly with Teradici

AWS account structure



Key recommendations

- Payer/linked account structure
- Only central logging in payer account
- User environment in separate account

Network design: Subnets

- ✓ Amazon WorkSpaces requires two subnets in different Availability Zones
- ✓ AppStream 2.0 **should** be deployed across two subnets in different Availability Zones
- ✓ Subnets should be sized to accommodate the target end-state capacity

Elastic network interfaces

- ✓ An instance in either service has two network interfaces
    - ➢ ETH0 is the service interface
    - ➢ ETH1 is the interface in your VPC
- ✓ Routing rules and security groups affect ETH1; you have full control of this interface
- ✓ User traffic can route to file servers, backend databases, licensing servers, and so on, either in your VPC, in a peered VPC, or on premises

Directory integration

amazon WorkSpaces

- All WorkSpaces will be joined to an Active Directory domain
- AWS Directory Service is required to connect users to their WorkSpace

amazon AppStream 2.0

- Fleets can be domain-joined or stand-alone
- AD-joined fleets integrate via SAML2.0 with your identity provider

Active Directory recommendations

- Extend your Active Directory into AWS on Amazon Elastic Compute Cloud (Amazon EC2) instances
- AWS Transit Gateway/VPC Peering:
  enable connectivity between Workspaces VPC and the Shared Services VPC

- Define your VPCs in Active Directory sites and services
- Separate Active Directory OUs by service and Region

Try it now

amazon WorkSpaces

Try Amazon WorkSpaces;
free tier available!

Run two standard bundle WorkSpaces for 40 hours a month

Amazon Linux 2 or Windows 10 experience, including WorkDocs with 50 GB user storage

amazon AppStream 2.0

40 hours per month for use of the stream.standard.large instance type when using Image Builder

Try sample applications—business, design, engineering, and developer

Upload your own files, test a workflow, save your work, and print

amazon WorkDocs

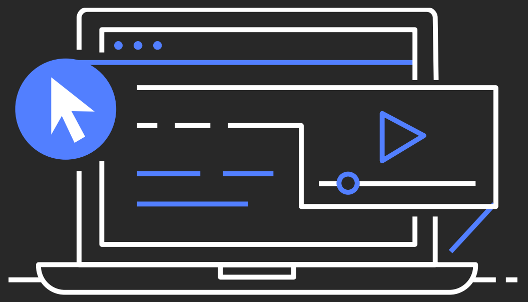
Try WorkDocs;
free tier available!

30-day free trial with 1 TB of storage per user for up to 50 users

Amazon WorkSpaces users get WorkDocs with 50 GB of storage for no additional charge

https://aws.amazon.com/free/

AWS 온라인 교육 과정



자신의 속도에 맞춰 학습하세요.

무료 AWS 디지털 교육을 통해
편한 시간에 원하는 장소에서
최신 클라우드 기술을
학습할 수 있습니다.

- AWS Cloud Practitioner Essentials
  AWS 클라우드의 기초를 배우고, AWS Certified Cloud Practitioner 공인 자격 시험을 준비할 수 있는 과정입니다.
  https://www.aws.training/Details/Curriculum?id=32442

- AWS 클라우드 보안 기초
  AWS 액세스 제어 및 관리, 거버넌스, 로깅 및 암호화 방법 등 AWS의 보안 개념을 소개합니다.
  https://www.aws.training/Details/Curriculum?id=11048

- Amazon Elastic Block Storage (EBS) 소개
  AWS 클라우드의 Amazon EC2 인스턴스에 사용할 블록 스토리지 볼륨을 제공하는 Amazon Elastic Block Store(EBS)를 소개합니다.
  https://www.aws.training/Details/Video?id=37393

aws.training

AWS Builders Online Series에 참석해주셔서 대단히 감사합니다.

저희가 준비한 내용, 어떻게 보셨나요?
더 나은 세미나를 위하여 **설문을 꼭 작성해 주시기 바랍니다.**

- aws-korea-marketing@amazon.com
- twitter.com/AWSKorea
- facebook.com/amazonwebservices.ko
- youtube.com/user/AWSKorea
- slideshare.net/awskorea
- twitch.tv/aws

Builders Online Series

Thank you