AWS를 활용한 개인정보 망분리 환경 구축

a.k.a AWS Workspace & Appstream

망분리...에 대해서 얼마나 알고 계신가요?

망분리… 전설의 시작

최근 대규모 개인정보 유출사고가 잇따라 발생함에 따라 유출된 개인정보로 인해 보이스피싱, 스팸메일 등 2차 피해의 발생 우려가 커지고 있다. 이에 정부는 개인정보 유출사고를 근절하기 위해 보다 높은 수준의 보안대책을 마련하였다.

그 일환으로 2012년 8월 17일에 공포된 개정 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」에 개인정보처리시스템에 접근하는 컴퓨터 등의 외부 인터넷망 차단(망분리) 조항이 신설되었다(2013년 2월 18일부터 시행). 망분리 제도가 시행됨에 따라 외부로의 정보 흐름을 차단하여 개인정보 유출사고를 효과적으로 예방할 수 있을 것으로 기대된다.

본 안내서는 망분리 제도 도입에 따른 사업자의 혼란을 해소하기 위해 외부 인터넷망과 업무망을 분리하기 위한 망분리 방식을 소개한다. 사업자는 기업의 전산 환경 및 IT 기술 발전 현황에 따라 알맞은 망분리 방식을 선택하여 구축할 수 있다.

출처: 정보통신서비스제공자등을 위한 외부 인터넷망 차단조치 안내서(2013.02)

Why?

개인정보 보호법 시행령 기준
[대통령령 제32528호, 2022. 3. 8., 타법개정]

제48조의2(개인정보의 안전성 확보 조치에 관한 특례) ① 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)와 그로부터 이용자(같은 법 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 법 제17조제1항제1호에 따라 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 이용자의 개인정보를 처리하는 경우에는 제30조에도 불구하고 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부관리계획의 수립 · 시행
가. 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성 · 운영에 관한 사항
나. 정보통신서비스 제공자등의 지휘 · 감독을 받아 이용자의 개인정보를 처리하는 자(이하 이 조에서 "개인정보취급자"라 한다)의 교육에 관한 사항
다. 제2호부터 제6호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 다음 각 목의 조치
가. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 이 조에서 "개인정보처리시스템"이라 한다)에 대한 접근 권한의 부여 · 변경 · 말소 등에 관한 기준의 수립 · 시행
나. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치 · 운영
다. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 외부 인터넷망 차단[전년도 말 기준 직전 3개월간 그 개인정보가 저장 · 관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 말한다. 이하 같다) 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다]
라. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정 및 운영
마. 그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치
3. 접속기록의 위조 · 변조 방지를 위한 다음 각 목의 조치
가. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인 · 감독
나. 개인정보처리시스템에 대한 접속기록을 별도의 저장장치에 백업 보관
4. 개인정보가 안전하게 저장 · 전송될 수 있도록 하기 위한 다음 각 목의 조치
가. 비밀번호의 일방향 암호화 저장
나. 주민등록번호, 계좌정보 및 제18조제3호에 따른 정보 등 보호위원회가 정하여 고시하는 정보의 암호화 저장
다. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신 · 수신하는 경우 보안서버 구축 등의 조치
라. 그 밖에 암호화 기술을 이용한 보안조치
5. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검 · 치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신 · 점검 조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치
② 보호위원회는 정보통신서비스 제공자등이 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.
③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.
[본조신설 2020. 8. 4.]
[종전 제48조의2는 제48조의14로 이동 <2020. 8. 4.>]

행정규칙

목 차

제 4 조 **접근통제**

제4조(접근통제) ① 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여한다.

② 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.

④ 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.

⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치 · 운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.

⑦ 정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.

출처: 개인정보의 기술적 관리적 보호조치 기준 해설서(2022. 10. 개정)

What?

⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.

출처: 개인정보의 기술적 관리적 보호조치 기준 해설서(2022. 10. 개정)

망분리 환경 구축을 추진 할 때 제일 먼저 선행되어야 하는 것은?

개인정보처리시스템이라고 전부 망분리 환경에서 접근할 필요는 없어요. (1/2)

■ 정보통신서비스 제공자등이 망분리를 할 때 인터넷망으로부터 분리되어야 하는 대상은 다음과 같다.

- 개인정보처리시스템에서 개인정보를 다운로드 할 수 있는 개인정보취급자의 컴퓨터 등

참 고

☞ 다운로드 : 개인정보처리시스템에 직접 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일형태로 저장하는 것을 말한다.

- 개인정보처리시스템에서 개인정보를 파기할 수 있는 개인정보취급자의 컴퓨터 등

참 고

☞ 파기 : 개인정보처리시스템에 저장된 개인정보 파일, 레코드, 삭제하는 것을 말한다.

- 개인정보처리시스템에 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등

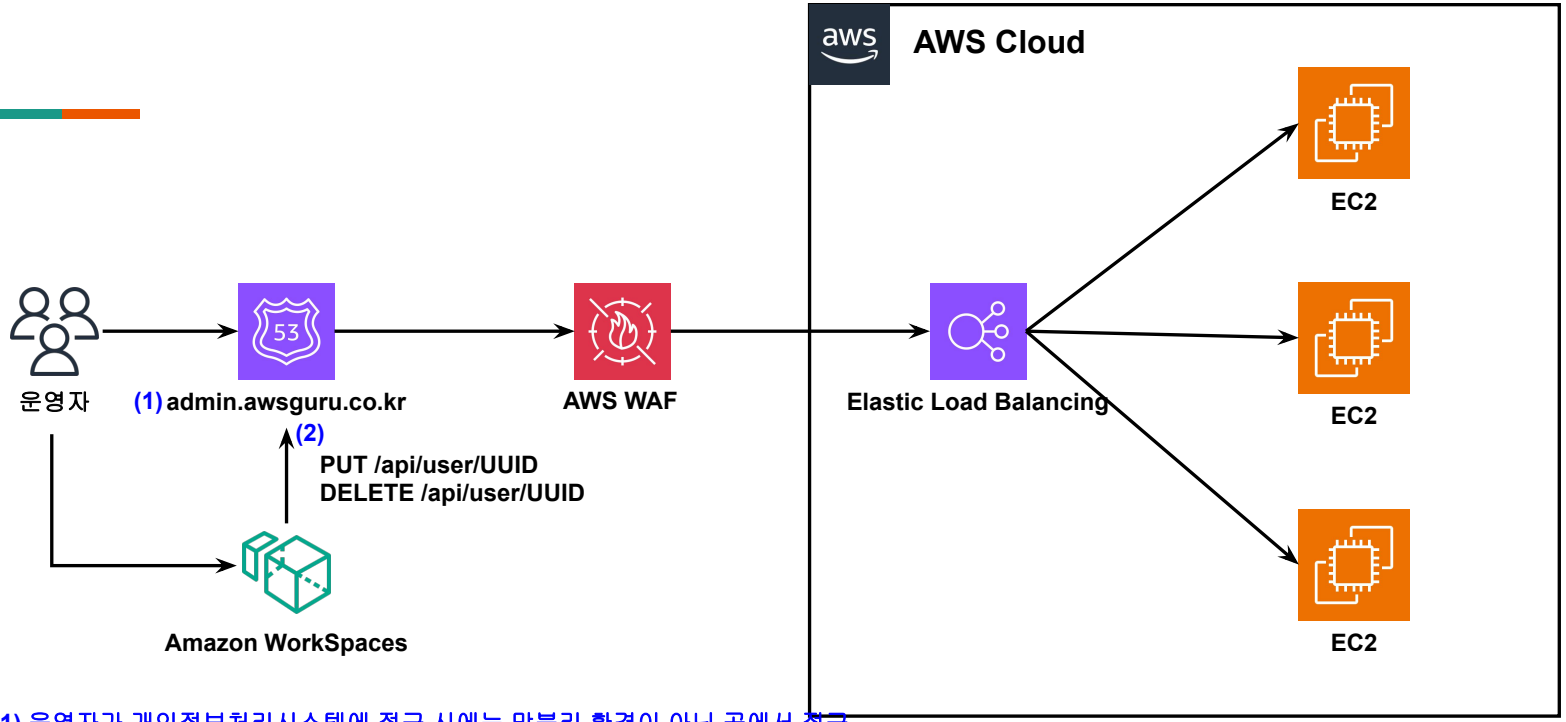
참 고

☞ 접근권한 설정 : 개인정보처리시스템에 접근하는 개인정보취급자에게 다운로드, 파기 등의 접근권한을 설정하는 것을 말한다.

- 개인정보처리시스템에서 단순히 개인정보를 열람, 조회 등만을 할 때에는 망분리를 적용하지 아니할 수 있다.

출처: 개인정보의 기술적 관리적 보호조치 기준 해설서(2022. 10. 개정)

개인정보처리시스템이라고 전부 망분리 환경에서 접근할 필요는 없어요. (2/2)

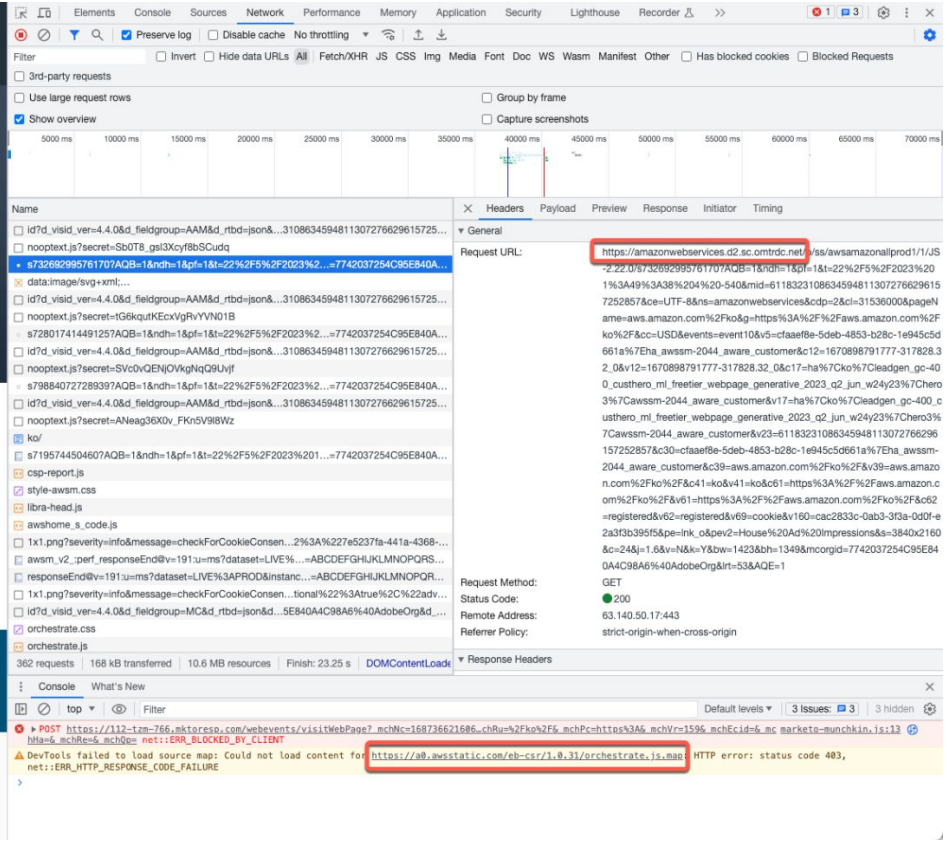


(1) 운영자가 개인정보처리시스템에 접근 시에는 망분리 환경이 아닌 곳에서 접근
> 공지사항 등록, 삭제, 상품 등록, 삭제 등 개인정보처리 업무와 무관한 업무 수행

(2) 운영자가 개인정보처리시스템에 접근 시 망분리 환경(AWS Workspaces)에서 접근
> 상품 주문내역 다운로드, 개인정보처리시스템의 계정 생성, 삭제, 권한부여 등

다음으로 선행되어야 하는 것은?

내부 서비스지만 외부의 패키지들을 호출하는 경우가 많아요.



AWS Workspace, Appstream에 대해 아시나요?

Desktop VS Application

End User Computing

AppStream 2.0

Stream desktop applications securely to any web browser

WorkSpaces

Desktops in the Cloud

WorkSpaces Web

Cloud-native secure web access

Workspace는 Desktop이다.

Appstream 2.0은 Browser 기반이다.

SAML 2.0과 같이 SSO 인증을 적용합시다. - MFA는 필수!

Setting up SAML 2.0

PDF | RSS

Enable WorkSpaces client application registration and signing in to WorkSpaces for your users by using their SAML 2.0 identity provider (IdP) credentials and authentication methods by setting up identity federation using SAML 2.0. To set up identity federation using SAML 2.0, use an IAM role and a relay state URL to configure your IdP and enable AWS. This grants your federated users access to a WorkSpaces directory. The relay state is the WorkSpaces directory endpoint to which users are forwarded after successfully signing in to AWS.

Contents

Setting Up SAML

PDF | RSS

To enable users to sign in to AppStream 2.0 by using their existing credentials, and start streaming applications, you can set up identity federation using SAML 2.0. To do this, use an IAM role and a relay state URL to configure your SAML 2.0-compliant identity provider (IdP) and enable AWS to permit your federated users to access an AppStream 2.0 stack. The IAM role grants users the permissions to access the stack. The relay state is the stack portal to which users are forwarded after successful authentication by AWS.

Contents

출처: https://d1.awsstatic.com/whitepapers/workspaces/workspaces-saml-implementation-guide_2022.pdf
https://docs.aws.amazon.com/workspaces/latest/adminguide/setting-up-saml.html
https://docs.aws.amazon.com/ko_kr/appstream2/latest/developerguide/external-identity-providers-setting-up-saml.html

비용은...?

시간당 요금? 월간 요금?


월드 오브 워크래프트®:
판다리아의 안개™
월드 오브 워크래프트® 정액제 & 정량제
일자에 관계 없이 구매한 게임 시간만큼 이용 가능
5시간 - 3,900 KRW
30시간 - 14,900 KRW
정해진 기간 동안 무제한 게임 이용 가능
7일 - 7,040 KRW
30일 - 19,800 KRW
90일 - 47,520 KRW

Workspace에도 백신은 필요해요.

Ubuntu Linux 번들 옵션 | Linux 번들 옵션 | Windows 번들 옵션 | Windows 번들 옵션 - 기존 보유 라이선스 사용(BYOL) *

각 Windows 번들 옵션에는 WorkSpace당 Microsoft 원격 데스크톱 서비스(RDS) 구독자 액세스 라이선스(SAL)가 포함됨

리전: 아시아 태평양(서울)

Value	루트 볼륨	사용자 볼륨	월별 요금	시간별 요금
1 vCPU, 2 GB 메모리	80 GB	10 GB	30.00 USD	10.00 USD/월 + 0.23 USD/시간
1 vCPU, 2 GB 메모리	80 GB	50 GB	34.00 USD	14.00 USD/월 + 0.23 USD/시간
1 vCPU, 2 GB 메모리	80 GB	100 GB	39.00 USD	19.00 USD/월 + 0.23 USD/시간
1 vCPU, 2 GB 메모리	175 GB	100 GB	45.00 USD	26.00 USD/월 + 0.23 USD/시간

Standard	루트 볼륨	사용자 볼륨	월별 요금	시간별 요금
2 vCPU, 4 GB 메모리	80 GB	10 GB	40.00 USD	10.00 USD/월 + 0.36 USD/시간
2 vCPU, 4 GB 메모리	80 GB	50 GB	43.00 USD	14.00 USD/월 + 0.36 USD/시간
2 vCPU, 4 GB 메모리	80 GB	100 GB	48.00 USD	19.00 USD/월 + 0.36 USD/시간
2 vCPU, 4 GB 메모리	175 GB	100 GB	56.00 USD	26.00 USD/월 + 0.36 USD/시간

Performance	루트 볼륨	사용자 볼륨	월별 요금	시간별 요금
2 vCPU, 8 GB 메모리	80 GB	10 GB	55.00 USD	10.00 USD/월 + 0.59 USD/시간
2 vCPU, 8 GB 메모리	80 GB	50 GB	60.00 USD	14.00 USD/월 + 0.59 USD/시간
2 vCPU, 8 GB 메모리	80 GB	100 GB	65.00 USD	19.00 USD/월 + 0.59 USD/시간
2 vCPU, 8 GB 메모리	175 GB	100 GB	72.00 USD	26.00 USD/월 + 0.59 USD/시간

Power	루트 볼륨	사용자 볼륨	월별 요금	시간별 요금
4 vCPU, 16 GB 메모리	80 GB	10 GB	86.00 USD	10.00 USD/월 + 0.86 USD/시간
4 vCPU, 16 GB 메모리	80 GB	50 GB	90.00 USD	14.00 USD/월 + 0.86 USD/시간
4 vCPU, 16 GB 메모리	80 GB	100 GB	93.00 USD	19.00 USD/월 + 0.86 USD/시간
4 vCPU, 16 GB 메모리	175 GB	100 GB	98.00 USD	26.00 USD/월 + 0.86 USD/시간

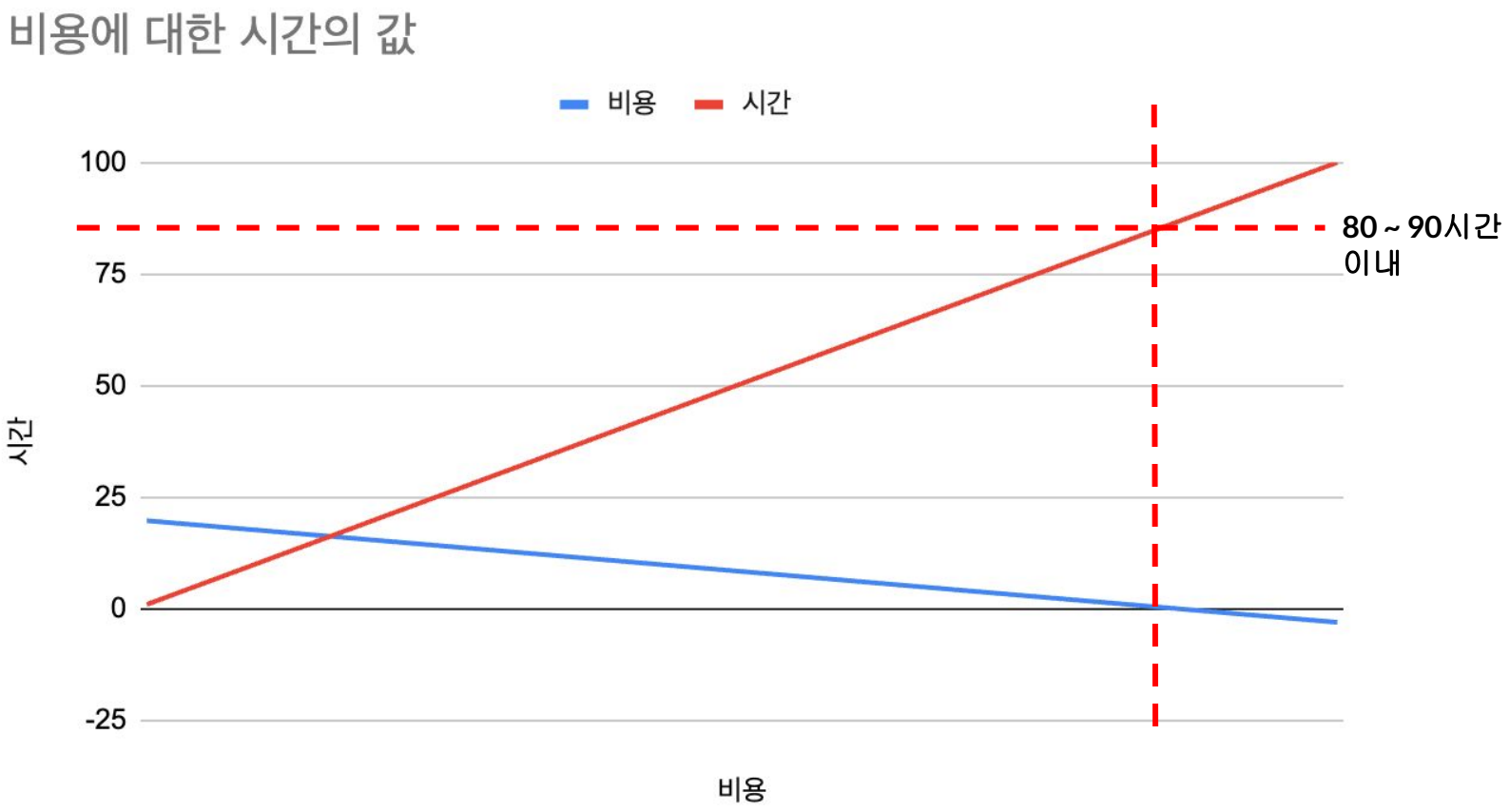
PowerPro	루트 볼륨	사용자 볼륨	월별 요금	시간별 요금
8 vCPU, 32 GB 메모리	80 GB	10 GB	147.00 USD	10.00 USD/월 + 1.67 USD/시간
8 vCPU, 32 GB 메모리	80 GB	50 GB	152.00 USD	14.00 USD/월 + 1.67 USD/시간
8 vCPU, 32 GB 메모리	80 GB	100 GB	157.00 USD	19.00 USD/월 + 1.67 USD/시간
8 vCPU, 32 GB 메모리	175 GB	100 GB	165.00 USD	26.00 USD/월 + 1.67 USD/시간

	Graphics G4dn	루트 볼륨	사용자 볼륨	월별 요금	시간별 요금
Graphics.g4dn	vCPU 4개, 16GiB 메모리, 1GPU, 16GiB 비디오 메모리, 125GB 로컬 인스턴스 스토어	100GB	100GB	586.00 USD	30.00 USD/월 + 1.74 USD/시간
GraphicsPro.g4dn	vCPU 16개, 64GiB 메모리, 1GPU, 16GiB 비디오 메모리, 225GB 로컬 인스턴스 스토어	100GB	100GB	1,048.00 USD	90.00 USD/월 + 12.57 USD/시간

애플리케이션 번들	애플리케이션	추가 월별 요금
Default 애플리케이션 번들	유틸리티(Internet Explorer 11, Firefox)	추가 요금 없음
Windows Server 2016 지원 WorkSpaces 용 추가 애플리케이션 번들	32비트 Microsoft Office 2016 Professional Plus, Trend Micro Worry-Free Business Security Services 및 유틸리티(Internet Explorer 11, Firefox)	추가 15.00 USD/월
Windows Server 2019 지원 WorkSpaces 용 추가 애플리케이션 번들	64비트 Microsoft Office 2019 Professional Plus 및 유틸리티(Internet Explorer 11, Firefox)	월별 추가 14.75 USD

출처: https://aws.amazon.com/ko/workspaces/pricing

Workspace는 Autostop보다 Always가 비용 저렴하다.



Appstream은 월간 플랜이 없어요.

Amazon AppStream 2.0 Pricing – Always-On, On-Demand, and image builder instances

Windows Instances | Linux Instances

Region: Asia Pacific (Seoul)

General purpose instances

	vCPU	Memory (GiB)	Hourly pricing*
stream.standard.small	1	2	$0.09
stream.standard.medium	2	4	$0.12
stream.standard.large	2	8	$0.24
stream.standard.xlarge	4	16	$0.48
stream.standard.2xlarge	8	32	$0.96

Elastic fleets streaming session pricing

Windows Instances | Linux Instances

Region: Asia Pacific (Seoul)

General purpose instances

	vCPU	Memory (GiB)	Hourly pricing*
stream.standard.small	2	2	$0.14
stream.standard.medium	2	4	$0.18
stream.standard.large	2	8	$0.35
stream.standard.xlarge	4	16	$0.696
stream.standard.2xlarge	8	32	$1.392

* Elastic fleets are billed for duration of the streaming session, in seconds, with a minimum of 15 minutes. Pricing is per instance-hour. An additional user fee may be assessed when users stream applications from streaming instances using the Microsoft Windows Server operating system.

On-Demand stopped instance fee

	Hourly pricing*
All instance types	$0.029

* Hourly pricing fee charged for running instances only. For Image Builder and Always-On fleets, instances may be considered running if they are available for use, even if no user is connected. For On-Demand fleets, instances are considered running only if users are connected with an active streaming session.

Workspace, Appstream 운영이 쉽지 않아요...

숨이 턱턱 막히는 트러블슈팅

Troubleshoot specific issues

The following information can help you troubleshoot specific issues with your WorkSpaces.

Issues

- I can't create an Amazon Linux WorkSpace because there are non-valid characters in the user name
- I changed the shell for my Amazon Linux WorkSpa
- My Amazon Linux WorkSpaces won't start
- Launching WorkSpaces in my connected directory
- Launching WorkSpaces fails with an internal error
- When I try to register a directory, the registration
- My users can't connect to a Windows WorkSpace w
- My users can't connect to a Windows WorkSpace
- My users are having issues when they try to log on
- The Amazon WorkSpaces client displays a gray "Lo message appears.
- My users receive the message "WorkSpace Status: few minutes."
- My users receive the message "This device is not a
- My users receive the message "No network. Netwo help." when trying to connect to a WSP WorkSpac
- The WorkSpaces client gives my users a network e
- My WorkSpace users see the following error messa
- My PCoIP zero client users are receiving the error "
- USB printers and other USB peripherals aren't wor
- My users skipped updating their Windows or macO
- My users are unable to install the Android client a
- My users aren't receiving invitation emails or passw
- My users don't see the Forgot password? option on the client login screen
- I receive the message "The system administrator has set policies to prevent this installation" when I try to install applications on a Windows WorkSpace
- No WorkSpaces in my directory can connect to the internet
- My WorkSpace has lost its internet access
- I receive a "DNS unavailable" error when I try to connect to my on-premises directory
- I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory
- I receive an "SRV record" error when I try to connect to my on-premises directory
- My Windows WorkSpace goes to sleep when it's
- One of my WorkSpaces has a state of UNHEALT
- My WorkSpace is unexpectedly crashing or rebo
- The same username has more than one WorkSp
- I'm having trouble using Docker with Amazon W
- I receive ThrottlingException errors to some of
- My WorkSpace keeps disconnecting when I let i
- SAML 2.0 federation isn't working. My users are
- My users are getting disconnected from their W
- My users get a redirect URI error when they fed of the WorkSpaces client application starts ever
- My users receive the message, "Something wen in to the WorkSpaces client application after fe
- My users receive the message, "Unable to valida federating to the IdP.
- My users receive the message, "The client and t
- My microphone or webcam is not working on W
- My users cannot login using certificate-based a Windows logon screen when they connect to th
- I am trying to do somthing that requires Windo
- I want to launch WorkSpaces with an existing A

Troubleshooting

PDF | RSS

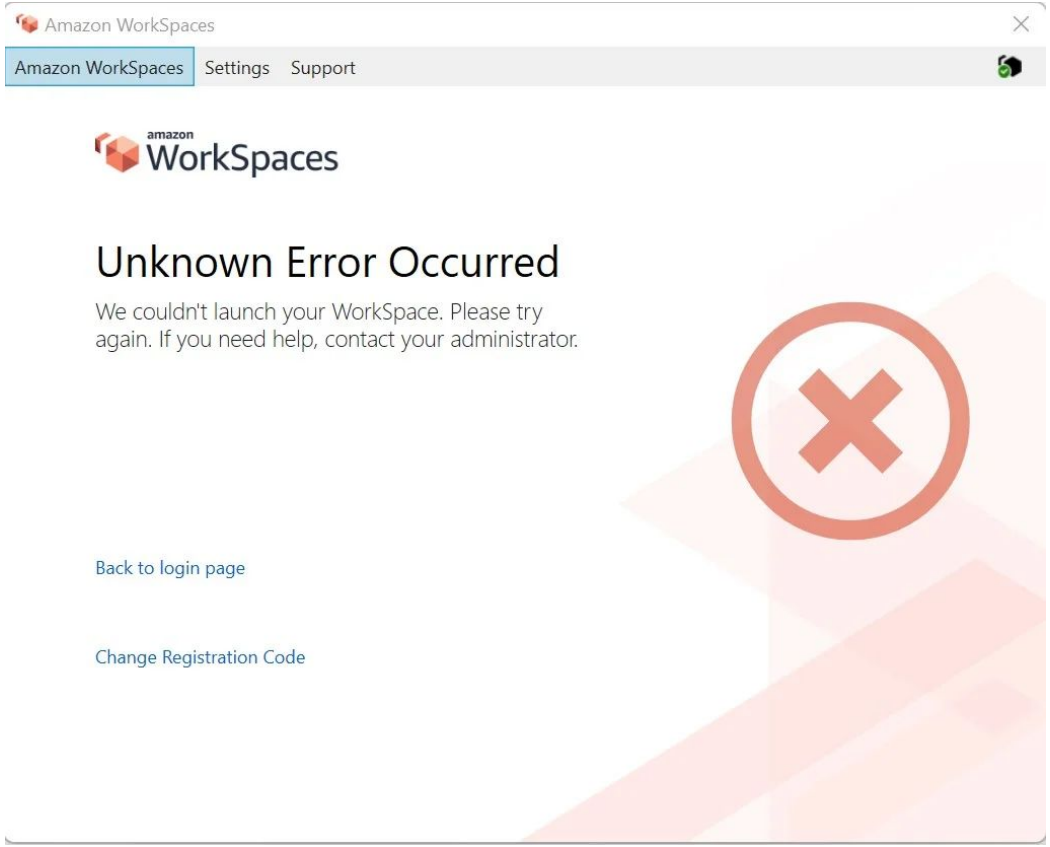
If you encounter difficulties when working with Amazon AppStream 2.0, consult the following troubleshooting resources.

Contents

- General Troubleshooting
- Troubleshooting Image Builders
- Troubleshooting Fleets
- Troubleshooting Active Directory
- Troubleshooting AppStream 2.0 User Issues
- Troubleshooting Persistent Storage Issues
- Troubleshooting Notification Codes

출처:
https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-troubleshooting.html
https://docs.aws.amazon.com/appstream2/latest/developerguide/troubleshooting.html

Workspace는.. 정말 알 수가 없어요



알 수 없는 에러...

안 되면 재부팅이 답입니다.

Clipboard는 제한해야 하지 않을까요?

Enable or disable clipboard redirection for PCoIP

By default, WorkSpaces supports clipboard redirection. If needed for Windows WorkSpaces, you can use Group Policy settings to disable this feature.

To enable or disable clipboard redirection

1. Make sure that you've installed the most recent WorkSpaces Group Policy administrative template for PCoIP (32-Bit) or WorkSpaces Group Policy administrative template for PCoIP (64-Bit).
2. On a directory administration WorkSpace or an Amazon EC2 instance that is joined to your WorkSpaces directory, open the Group Policy Management tool (**gpmc.msc**) and navigate to **PCoIP Session Variables**.
3. Open the **Configure clipboard redirection** setting.
4. In the **Configure clipboard redirection** dialog box, choose **Enabled** and then choose one of the following settings to determine the
   - Disabled in both directions
   - Enabled agent to client only (WorkSpace to local computer)
   - Enabled client to agent only (local computer to WorkSpace)
   - Enabled in both directions
5. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace sessior
   - Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions**, **Reboot WorkSpaces**).
   - In an administrative command prompt, enter `gpupdate /force`.

Known limitation

With clipboard redirection enabled on the WorkSpace, if you copy content that is larger than 890 KB from a Microsoft Office application,

6. For **Step 3: User Settings**, configure the following settings. When you're done, choose **Review**.

Clipboard, file transfer, print to local device, and authentication permissions options:

- **Clipboard** — By default, users can copy and paste data between their local device and streaming applications. You can limit Clipboard options so that users can paste data to their remote streaming session only or copy data to their local device only. You can also disable Clipboard options entirely. Users can still copy and paste between applications in their streaming session.
- **File transfer** — By default, users can upload and download files between their local device and streaming session. You can limit file transfer options so that users can upload files to their streaming session only or download files to their local device only. You can also disable file transfer entirely.

> **Important**
> If your users require AppStream 2.0 file system redirection to access local drives and folders during their streaming sessions, you must enable both file upload and download. To use file system redirection, your users must have AppStream 2.0 client version 1.0.480 or later installed. For more information, see Enable File System Redirection for Your AppStream 2.0 Users.

- **Print to local device** — By default, users can print to their local device from within a streaming application. When they choose **Print** in the application, they can download a .pdf file that they can print to a local printer. You can disable this option to prevent users from printing to a local device.
- **Password sign in for Active Directory** — Users can enter their Active Directory domain password to sign in to an AppStream 2.0 streaming instance that is joined to an Active Directory domain.

  You can also enable **Smart card sign in for Active Directory**. At least one authentication must be enabled.
- **Smart card sign in for Active Directory** — Users can use a smart card reader and smart card connected to their local computer to sign in to an AppStream 2.0 streaming instance that is joined to an Active Directory domain.

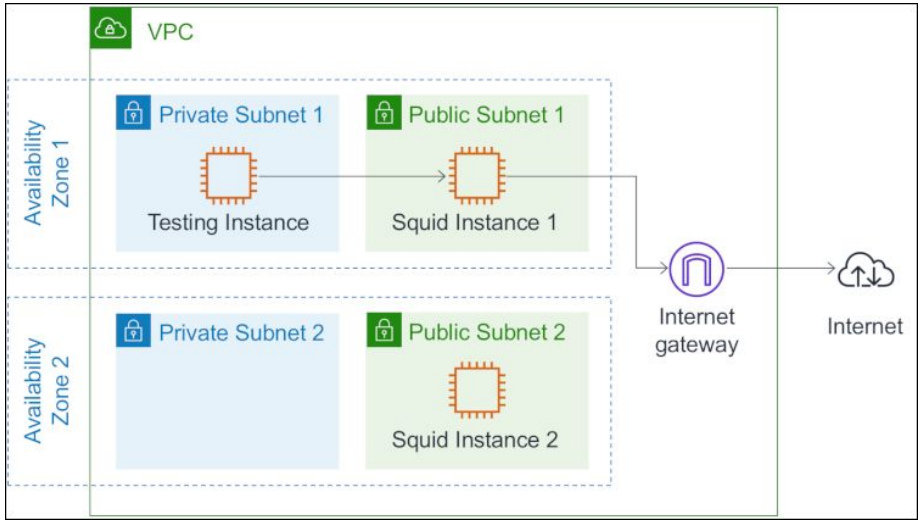
  You can also enable **Password sign in for Active Directory**. At least one authentication method must be enabled.

> **Note**
> **Clipboard, file transfer, and print to local device settings** — These settings control only whether users can use AppStream 2.0 data transfer features. If your image provides access to a browser, network printer, or other remote resource, your users might be able to transfer data to or from their streaming session in other ways.
>
> **Authentication settings** — These settings control only the authentication method that can be used for Windows sign in to an AppStream 2.0 streaming instance (fleet or image builder). They do not control the authentication method that can be used for in-session authentication, after a user signs in to a streaming instance. For information about configuration requirements for using smart cards for Windows sign in and in-session authentication, see Smart Cards. These settings are not supported for Linux-based stacks.

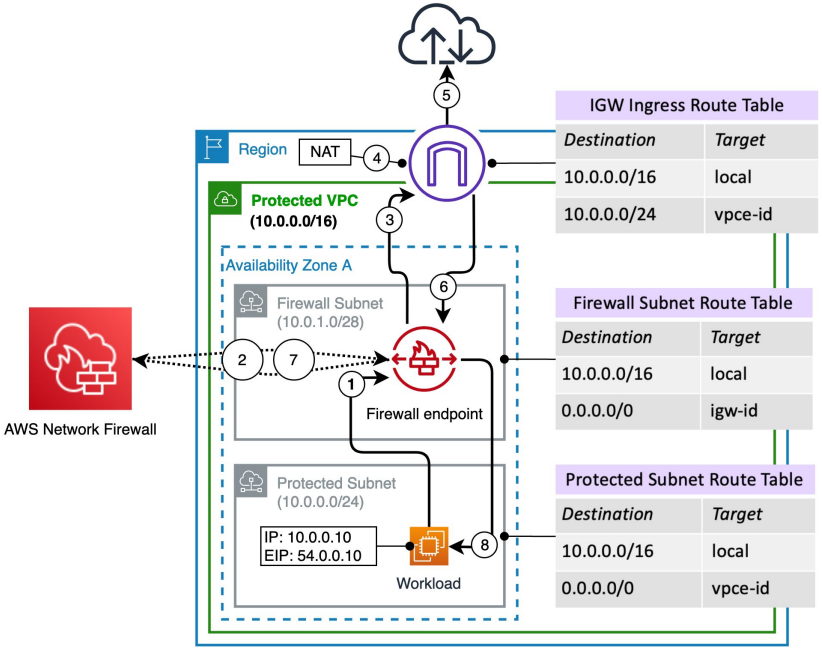
but... 화면캡처방지는 지원하지 않아요...

출처: https://docs.aws.amazon.com/appstream2/latest/developerguide/set-up-stacks-fleets.html
https://docs.aws.amazon.com/workspaces/latest/adminguide/group_policy.html

망분리 환경에서 인터넷 환경에 접근이 필요하다면…? (Windows & 백신 Update)



squid proxy



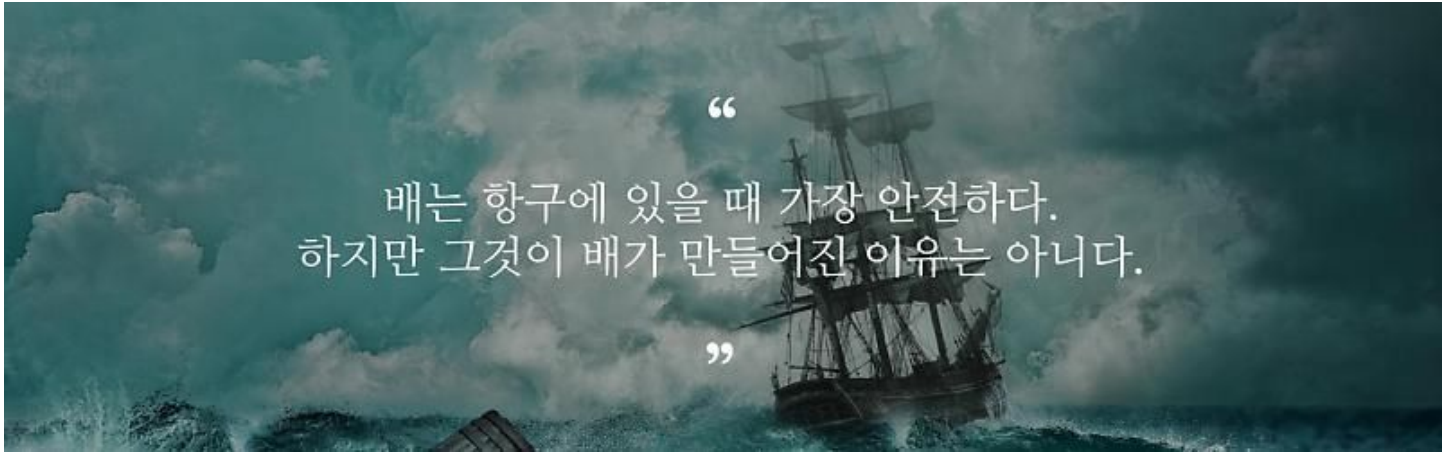
Network Firewall

Github와 같은 SaaS 서비스는 데이터 유출 경로로 이용될 수 있으니 주의가 필요합니다.

출처: https://aws.amazon.com/blogs/security/how-to-add-dns-filtering-to-your-nat-instance-with-squid/

마지막으로...

보안은 서비스를 안전하게 하는 것이 목적이다.



Question

AWS Console 콘솔도 망분리 대상인가요?

Answer

AWS Console도 개인정보처리시스템이다. 대부분의 기업들이 **AWS**를 개인정보처리방침에 기재하고 있으므로 **AWS Console**도 망분리를 해야한다고 생각합니다.

다만, 앞서 말씀 드렸다시피 개인정보보호법상 망분리의 요건은 "개인정보를 다운로드, 파기 또는 개인정보처리시스템에 접근권한을 설정할 수 있는 개인정보취급자의 단말기를 인터넷이 차단된 환경에서 접근하도록 한다"이며, **AWS Console 전체가 아닌 망분리 요건에 해당되는 권한을 소유한 사용자의 권한을 최소화 하는 방법을 고민**해야 한다. 사용자에게는 해당 권한을 제공하지 않고 **IaC와 같이 시스템적으로 해결하는 방법**을 찾아야 합니다.

AWS Console과 같은 **SaaS** 형태의 서비스가 **로컬PC, 망분리 환경 양쪽에서 모두 접근이 가능**하다면 망연계 시스템과 같이 데이터 유출의 포인트 **(Lateral Movement)**가 될 수 있기 때문에 주의가 필요합니다.

특히, 프록시 서버와 같이 **도메인을 통제하는 방식으로 인터넷을 통제**하는 경우 **망분리 환경 내에서 취득한 데이터를 회사의 AWS Console이 아닌 개인의 AWS Console로 업로드**한다면 로깅 등이 남지 않는 위험이 존재하므로 이런 부분들이 모두 해소되지 않는 상태에서 적용하는 것은 더 큰 위험을 야기할 수 있다고 생각합니다.

Question

오랫 동안 AWS Workspace 운영/관리하셨는데 자동화 등 관리는 어떻게 하셨는지?

Answer

수동으로 관리했습니다... AWS Workspace 생성 오류도 자주 발생하고, 한 번에 생성되는 개수도 제한되어 있어서 생성을 자동화 하는 데에 한계가 있습니다.
제가 생각하기에 AWS Workspace, Appstream과 같은 서비스의 본질은 "업무를 효율적으로" 하기 위한 목적인데 조금 다른 방식으로 서비스를 이용하고 있어 알 수 없는 문제들이 발생한다고 생각합니다.

23페이지의 알 수 없는 에러와 동시에 Workspace 생성이 안되는 이슈로 AWS Support의 도움을 받았지만 결국 해결하지는 못했습니다... 이용자가 Self-Control을 할 수 있는 영역(Workspace 시작/중지/재부팅 등)을 Slack Bot 등으로 제공하고 이용 가이드를 자세하게 작성해서 질문을 최소화 하는 정도 외에는 관리를 효율적으로 하기는 어려운 부분이 있습니다. (가끔... 나는 보안 담당자인가 PC HelpDesk인가 고민 하기도...)

Workspace 생성을 Jira Workflow에 따라서 자동화 해볼까도 생각했었지만 생성 중 실패되는 경우가 너무나 자주 발생하여 그 부분도 결국은 해결하지 못하였는데, 제가 시도해 보지 못한 Best Practices for Deploying WorkSpaces 부분을 참고해서 그 문제를 해결해 볼 수 있지 않을까 생각됩니다.

Question

로컬PC와 AWS Workspace간 데이터를 이동해야 하는 경우가 필요한데, 이 부분은 어떻게 해결하였는지?

Answer

망연계 솔루션은 업무상 반드시 필요합니다. 시장에 나와 있는 망연계 솔루션들을 검토해봤지만 대부분이 클라우드를 지원하지 않거나 구축 경험이 없는 경우가 많았습니다. 또한 Agent 방식이 MacOS를 호환하지 않는다는 단점들도 존재하였습니다.

결국은 자체 개발조직을 통해서 시스템이 개발하여서 해결했습니다.

만약 망연계 솔루션을 자체 개발하고자 한다면 파일 암호화, 악성코드 검출 이 2가지에 대한 기능은 적용되어야 합니다.
처음 시작부터 해당 기능들을 넣기 부담스럽다면 파일 암호화에 대한 기능은 필수로 적용을 해주세요.

여기에서 말씀 파일 암호화는 엑셀, 워드 등 파일 자체에 대한 암호화를 권고 드리며, 기술적으로 적용이 어렵다면 압축파일 암호화를 차선이라도 고민해 보시기 바랍니다.

그 외에는 망분리 환경에서 로컬PC로 데이터를 반출할 때에는 문서 암호화를 하도록 개발자 교육 등을 통해서 관리적으로 해결해야 겠습니다.

Question

Workspace 동작모드(Autostop, AlwaysOn)별 관리는 어떻게?

Answer

1개월 이내 단기 계약직이 아니라면 AutoStop보다 AlwaysOn 방식이 무조건 비용 저렴합니다. 말씀 드린거처럼 AutoStop 방식은 켜두는 시간에 따라서 Limit 없이 비용이 계속 늘어나는 구조입니다. 즉, 관리를 잘못하면 AlwaysOn 방식보다 비용이 더 비싸게 나올 수 있는 구조이고... 저렴하다고 하더라도 AlwaysOn 대비 30% 이상 비용 효율적으로 운영할 수는 없습니다. 오히려 30% 이상 비용 효율적으로 운영할 수 있다면 그만큼 Workspace 이용시간이 적다는 의미이고, 그렇다면 Workspace 환경 안에서 업무를 하지 않도록 일하는 방식을 바꾸는게 맞습니다. (가령 월간 접속이력을 검토하기 위해서 1달에 3~4시간 정도만 Workspace를 이용하는 등)

또한 Workspace를 이용하는 사용자들이 업무가 종료된다고 습관적으로 Workspace를 종료하지는 않습니다. 퇴근 시에 PC를 종료하지 않고 대부분 항상 켜둔 상태로 PC를 잠그거나 Sleep 모드로 두는데, Sleep 모드에서도 Workspace의 세션이 종료되지 않고 계속 유지되어 밤새도록 켜져있는 것을 자주 확인했습니다.

AutoStop 구동방식에 대한 자동화를 구현하더라도 자동화를 구현하기 위해 들어가는 개발 리소스 비용 대비 AlwaysOn 방식으로 구동시키는 것이 최초 로그인 시간, 로그인 오류, 비용 이슈 등을 모두 감안하더라도 압도적인 ROI를 보입니다.
AutoStop이 비용 효율적이라고 생각되신다면 한달씩 동작모드를 변경해서 이용해서 비용을 비교 해 보시기를 권장 드립니다.

프로게이머에게 월간 정액이 아닌 시간 요금제 서비스를 제공할 필요는 없지 않을까 생각됩니다.