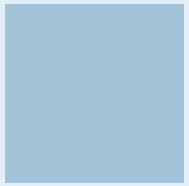
CLOUD ON
Azure Managed Service

Azure Virtual Desktop

CloudON for Infrastructure (AVD) : 2wk Assessment



씨앤토트

Contents

CLOUD MANAGED SERVICE

1. AVD 개요

CLOUD ON
Azure Managed Service

Azure Virtual Desktop(AVD) 서비스는 Microsoft 클라우드 기반으로 제공되는 Virtual Desktop Infrastructure(VDI) 서비스입니다.

- Microsoft Azure 플랫폼 상에서 제공되는 클라우드 VDI 서비스
- 스마트폰, 태블릿, PC 등의 다양한 디바이스에서 접속 가능한 Windows OS PC 환경 제공
- 에이전트 또는 웹 클라이언트를 통한 접속 방식 제공
- Windows 365 Cloud PC와 달리 중앙에서 VDI 리소스 관리가 가능한 서비스
- 연결 브로커와 같은 VDI 관리 인프라는 Microsoft에서 관리
- 기업 환경에서 사용 중인 마스터 이미지를 업로드하여 사용 가능
- 데스크톱 가상화 뿐만 아니라 애플리케이션 가상화 기능도 제공
- 비용 절감을 위한 멀티세션 Windows 11 또는 Windows 10 환경 제공
- 클라우드 인프라를 활용함으로써 빠른 배포 및 확장 용이
- 시간대별 또는 사용자 수요 변화에 따라 자동 확장 기능 제공

2. AVD 사용 환경 - 사용자

CLOUD ON
Azure Managed Service

팬데믹 이후로 하이브리드 근무 형태가 많이 도입되었습니다만, 다음과 같은 사용자 유형 및 요구 사항이 여전히 존재합니다.

원격 근무 및 하이브리드 근무

- 코로나 바이러스 확산 이후 재택 근무의 활성화
- 약 2년 이상의 팬데믹 기간 동안 하이브리드 형태의 근무 환경에 대한 요구 증대
- Z세대의 직장을 대하는 가치관의 변화

탄력적인 노동력

- 프리랜서 및 개인 사업자를 통한 노동력 확보
- 자유로운 출퇴근 시간 변경 등의 탄력적인 근무 환경 도입
- 단기 임시직 또는 파트너 사사의 협업을 위한 PC 환경 제공

조직 확장 및 변화

- 회사 합병을 통한 기업 비즈니스 확장
- 급변하는 기업 비즈니스 환경에 대응하기 위한 빈번한 조직 변경
- 스타트업 활성화에 따른 Agile 조직으로의 변화

자신의 PC 사용 (BYOD)

- 다양한 종류의 디바이스 확산
- 개인 사용 디바이스를 업무 환경에서 활용하고자 하는 요구 사항 증대 (Bring-Your-Own-Device)
- 업무 환경에서 개인 사용 디바이스의 네트워크 접속 허용 정책 수립

글로벌 및 특수 워크로드

- 네트워크 지연이 높은 해외 지점 근무자 및 출장자를 위한 VDI VM 제공
- 디자인 및 3D 모델링 등의 고성능 GPU 작업 수요
- 일부 App만 사용할 필요가 있는 경우

보안 및 규정 준수

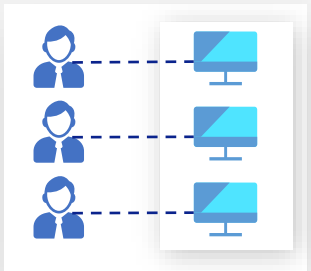
- 망분리 요구 사항으로 2대의 PC(물리 또는 가상)를 사용해야 하는 규정 준수
- 인터넷 연결이 차단된 폐쇄망 형태의 PC 환경 구현
- 인터넷 전용 PC 환경 제공

2. AVD 사용 환경 - 데스크톱 유형

CLOUD ON
Azure Managed Service

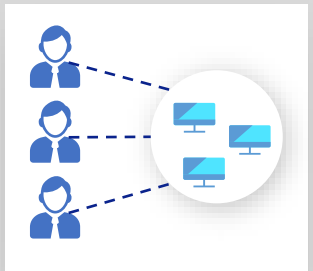
AVD 사용자의 요구 사항에 따라 개인 또는 풀(Pool) 방식의 데스크톱과 세션 방식의 서버 데스크톱 환경을 제공합니다.

개인 데스크톱



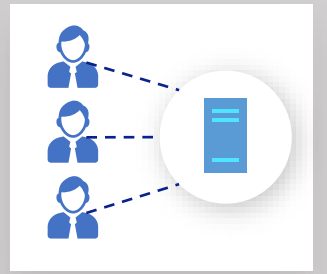
- 개인 사용자의 상태 및 데이터 저장
- 데스크톱에 대한 관리자 권한 제공
- 애플리케이션 호환성이 높음
- 비용 효율성이 낮음

풀 방식 데스크톱



- 개인 사용자의 데이터는 별도의 개인용 공유 폴더에 저장
- 단일세션 방식의 경우, 데스크톱에 대한 관리자 권한 제공
- 멀티세션 방식의 경우, 데스크톱에 대한 사용자 권한 제공
- 관리 효율성이 높음

세션 방식 서버 데스크톱



- 개인 사용자의 데이터는 별도의 개인용 공유 폴더에 저장
- 데스크톱에 대한 사용자 권한 제공
- 애플리케이션 호환성이 낮음
- 사용자에게 특정 애플리케이션만 제공 가능
- 비용 효율성이 높음

3. AVD 사전 요구 사항 #1

CLOUD ON
Azure Managed Service

AVD를 사용하기 위해 사전에 확인해야 할 사항이 몇가지 있습니다.

- Azure 계정 - 구독(Subscription)이 활성화 되어 있어야 함
- AVD 사용자가 인증 받기 위한 서비스 - Azure Active Directory(Azure AD)
- AVD VM이 참가할 도메인 - Active Directory Domain Services(AD DS) 또는 Azure Active Directory Domain Services(Azure AD DS)
- AVD VM에서 사용할 운영 체제 버전 (#2 장표 참조)
- AVD 서비스에 연결하기 위한 필수 URL 허용 (#3 장표 참조)
- AVD VM에 접속하기 위한 클라이언트 - Remote Desktop client
  - ❖ Windows 데스크톱 클라이언트 : Windows 11, Windows 10, Windows 10 IoT Enterprise, Windows 7 (단, Windows 8 또는 Windows 8.1은 지원하지 않음)
  - ❖ 웹 클라이언트 : Microsoft Edge, Apple Safari, Mozilla Firefox, Google Chrome (단, 모바일 OS는 지원하지 않음)
  - ❖ macOS 클라이언트 : macOS 10.12 이상
  - ❖ iOS 클라이언트 : iOS 14.0 이상 (iPhone, iPad, iPod touch와 호환 가능)
  - ❖ Android 클라이언트 : Android 4.1 이상, ChromeOS 53 이상이 설치된 Chromebooks
  - ❖ Thin 클라이언트 : 10ZiG, Dell, HP, IGEL, NComputing, Stratodesk
- AVD VM에서 인터넷 접속을 위한 라우팅 구성 - Azure 상에 DMZ 구성 여부

3. AVD 사전 요구 사항 #2

CLOUD ON
Azure Managed Service

AVD VM에 사용 가능한 운영체제 및 라이선스는 다음과 같습니다.

- AVD 서비스를 통해 가상 데스크톱 및 원격 앱을 제공하기 위해 세션 호스트에 사용할 수 있는 운영 체제는 아래와 같이 사용 가능합니다.

AVD VM 사용 가능 운영 체제	AVD 사용자 액세스 권한 라이선스
 • Windows 11 Enterprise multi-session • Windows 11 Enterprise • Windows 10 Enterprise multi-session, 버전 1909 이상 • Windows 10 Enterprise, 버전 1909 이상 • Windows 7 Enterprise	• Microsoft 365 E3/E5 • Microsoft 365 A3/A5/Student Use Benefit • Microsoft 365 F3 • Microsoft 365 Business Premium • Windows Enterprise E3/E5 • Windows Education A3/A5 • Windows VDA E3/E5 • 외부 사용자는 라이선스 권한 대신 사용자당 액세스 가격 책정을 사용할 수 있습니다.
 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2	• Software Assurance(사용자당 또는 디바이스당)가 포함된 Remote Desktop Services(RDS) Client Access License(CAL) • RDS User Subscription Licenses • Windows Server 운영 체제에 대해서는 사용자당 액세스 가격 책정을 사용할 수 없습니다.

3. AVD 사전 요구 사항 #3

CLOUD ON
Azure Managed Service

AVD를 사용하려면 세션 호스트 VM에서 액세스할 수 있도록 특정 URL을 허용해야 합니다.

- 다음 표는 세션 호스트 VM이 AVD에 액세스해야 하는 URL 목록입니다. 하기 URL외에 Azure AD 인증을 위한 URL도 허용해야 합니다.

주소	아웃바운드 TCP 포트	목적	서비스 태그
login.microsoftonline.com	443	Microsoft Online Services에 대한 인증	
*.wvd.microsoft.com	443	서비스 트래픽	WindowsVirtualDesktop
*.prod.warm.ingest.monitor.core.windows.net	443	에이전트 트래픽	AzureMonitor
catalogartifact.azureedge.net	443	Azure Marketplace	AzureFrontDoor.Frontend
gcs.prod.monitoring.core.windows.net	443	에이전트 트래픽	AzureCloud
kms.core.windows.net	1688	Windows 정품 인증	인터넷
azkms.core.windows.net	1688	Windows 정품 인증	인터넷
mrsglobalsteus2prod.blob.core.windows.net	443	에이전트 및 SXS(병력) 스택 업데이트	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Azure Portal 지원	AzureCloud
169.254.169.254	80	Azure Instance Metadata Service 엔드포인트	해당 없음
168.63.129.16	80	세션 호스트 상태 모니터링	해당 없음
oneocsp.microsoft.com	80	인증서	해당 없음
www.microsoft.com	80	인증서	해당 없음

◆ 참조 링크: https://learn.microsoft.com/ko-kr/azure/virtual-desktop/safe-url-list?tabs=azure

◆ 참조 링크: https://learn.microsoft.com/ko-kr/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide#microsoft-365-common-and-office-online

3. AVD 사전 요구 사항 #4

CLOUD ON
Azure Managed Service

AVD에 연결하기 위해서 모든 원격 데스크톱 클라이언트는 특정 URL에 액세스할 수 있어야 합니다.

- 다음 표는 원격 데스크톱 클라이언트에서 액세스해야 하는 URL 목록입니다. 하기 URL외에 Azure AD 인증을 위한 URL도 허용해야 합니다.

주소	아웃바운드 TCP 포트	목적	클라이언트
login.microsoftonline.com	443	Microsoft Online Services에 대한 인증	모두
*.wvd.microsoft.com	443	서비스 트래픽	모두
*.servicebus.windows.net	443	데이터 문제 해결	모두
go.microsoft.com	443	Microsoft FWLinks	모두
aka.ms	443	Microsoft URL 단축키	모두
learn.microsoft.com	443	설명서	모두
privacy.microsoft.com	443	개인정보처리방침	모두
query.prod.cms.rt.microsoft.com	443	클라이언트 업데이트	Windows Desktop

◆ 참조 링크: https://learn.microsoft.com/ko-kr/azure/virtual-desktop/safe-url-list?tabs=azure

◆ 참조 링크: https://learn.microsoft.com/ko-kr/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide#microsoft-365-common-and-office-online

4. AVD 가격 구성 요소

CLOUD ON
Azure Managed Service

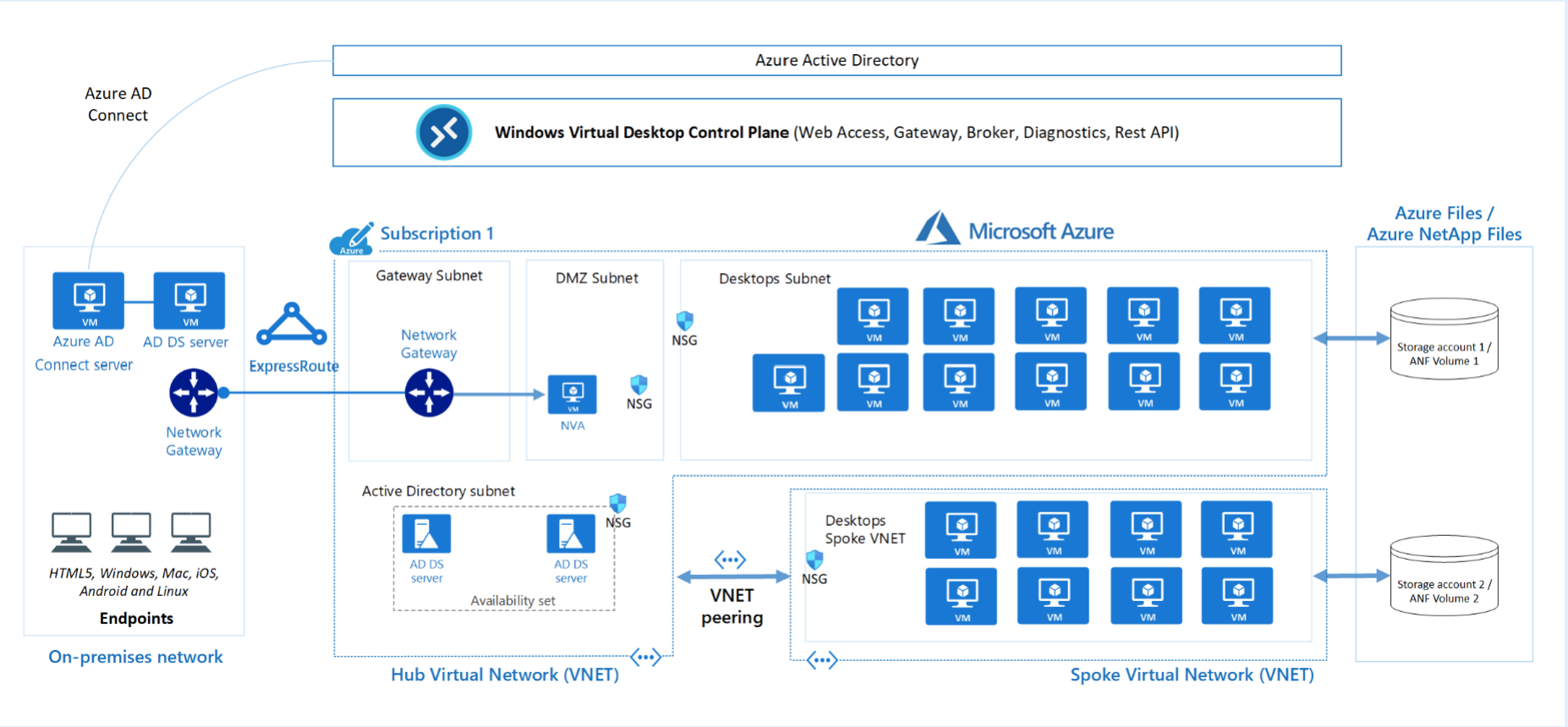
AVD 사용 비용은 사용자 액세스 권한 비용과 Azure 인프라 비용 2가지로 구성됩니다.

- AVD 가격을 구성하는 2가지 요소
  1. 사용자 액세스 권한
     - 라이선스 자격 : 적격한 Windows, Microsoft 365 및 Microsoft RDS CAL이 있는 경우, 추가 비용이 발생하지 않음
     - 사용자당 액세스 가격 : AVD 액세스에 대해 외부 사용자에게만 적용하는 새로운 월별 사용자당 가격 옵션
  2. Azure 인프라 비용
     - 가상 머신(Virtual Machines) : 종량제(PAYG) 또는 예약 인스턴스(Reserved Instance, RI) 방식으로 Linux 컴퓨팅 요금 청구
     - 스토리지 : 운영 체제 스토리지, 데이터 디스크, 사용자 프로필 스토리지 등
     - 네트워킹 : VPN 게이트웨이 또는 전용선, 아웃바운드 트래픽, Azure Firewall 등
     - 관리 기능 : Azure Automation, Logic Apps, Azure Monitor 등

5. AVD 아키텍처 - 기업용

CLOUD ON
Azure Managed Service

AVD 기업용 아키텍처는 1,000대 이상 규모의 가상 데스크톱 구현을 예시로 구성한 것입니다.



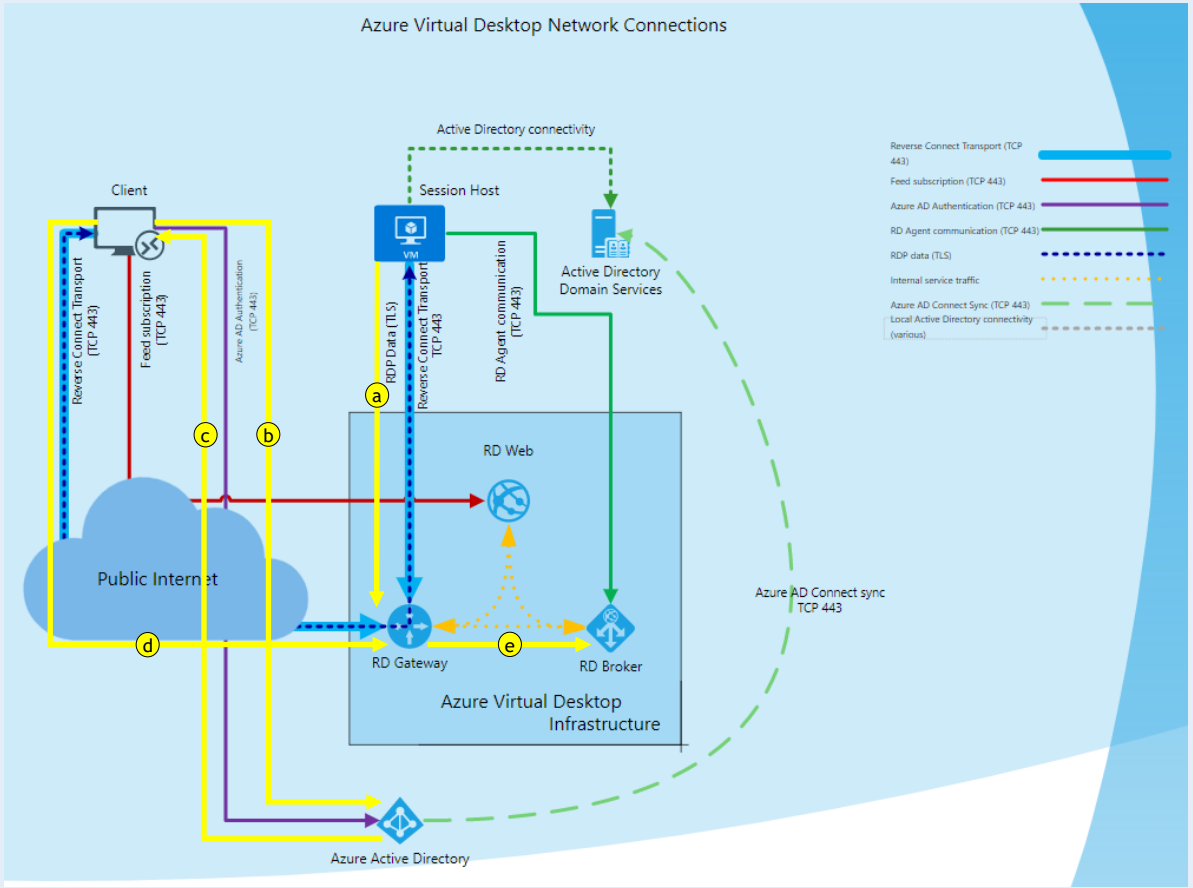
<Azure Virtual Desktop 기업용 아키텍처>

- Azure ExpressRoute는 온-프레미스 네트워크를 Azure로 확장하고, Azure AD Connect는 고객의 AD DS를 Azure AD와 통합합니다.
- Windows Virtual Desktop Control Plane은 웹 액세스, 게이트웨이, 브로커, 진단 및 Rest API와 같은 확장성 구성 요소를 처리합니다.
- 기업 고객은 AD DS 및 Azure AD, Azure 구독, 가상 네트워크, Azure Files 또는 Azure NetApp Files, AVD 호스트 풀 및 작업 영역을 관리합니다.
- 용량 확장을 위해, 허브-스포크 아키텍처에서 가상 네트워크 피어링을 통해 연결합니다.

5. AVD 아키텍처 - 네트워크 연결 #1

CLOUD ON
Azure Managed Service

AVD에서 사용되는 네트워크 연결에 대한 개략적인 개요는 아래와 같습니다.



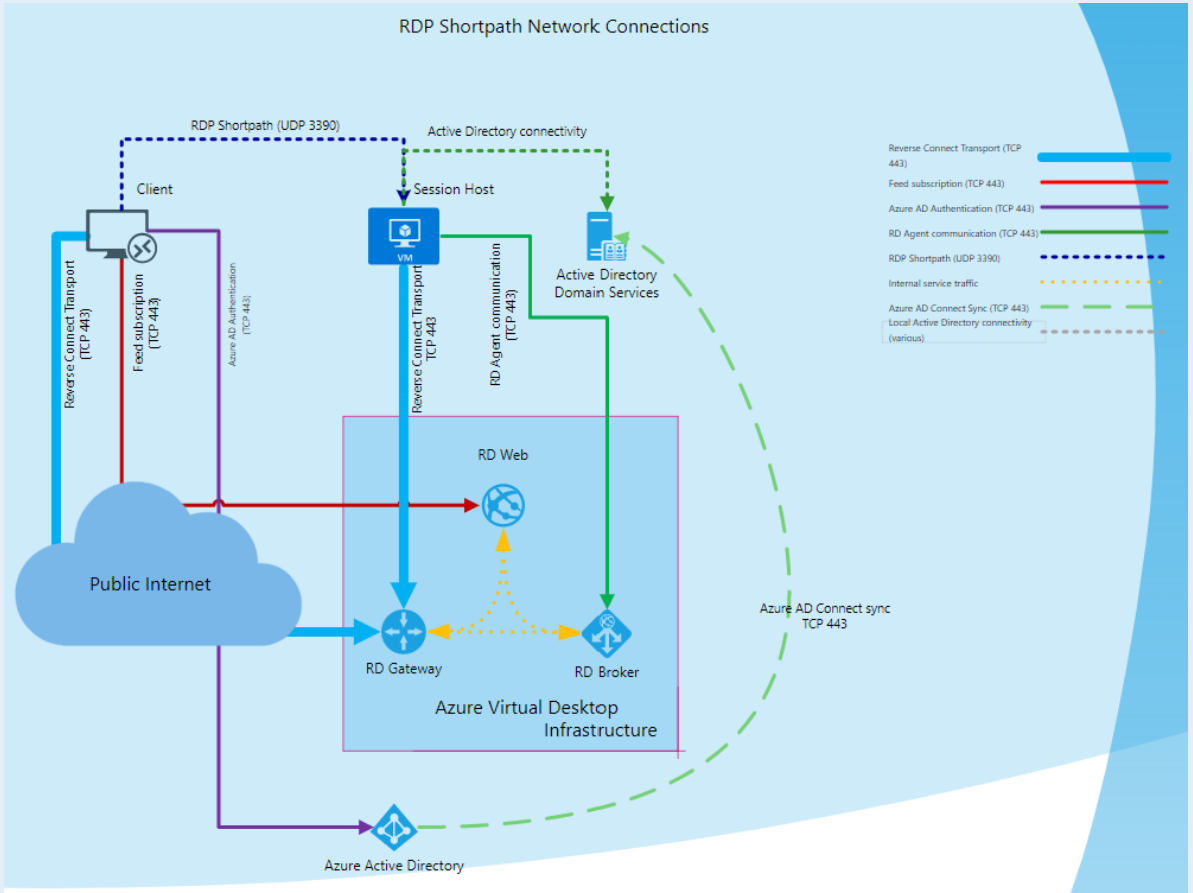
<Azure Virtual Desktop 네트워크 연결 이해 #1>

0. AVD 환경 배포 후 AVD VM이 시작될 때, AVD 인프라에 대한 아웃바운드 HTTPS 연결을 사용하여 영구 통신 채널을 설정합니다. (ⓐ)
1. 사용자는 지원되는 Azure Virtual Desktop(AVD) 클라이언트를 사용하여 Azure Virtual Desktop 작업 영역을 구독합니다. (ⓑ)
2. Azure Active Directory에서 사용자를 인증하고 사용자가 사용할 수 있는 리소스를 열거하는데 사용되는 토큰을 반환합니다. (ⓒ)
3. AVD 클라이언트가 AVD 피드 구독 서비스에 토큰을 전달합니다.
4. AVD 피드 구독 서비스는 토큰의 유효성을 검사한 후, 사용 가능한 데스크톱 및 RemoteApp의 목록을 디지털로 서명된 연결 구성 형식으로 AVD 클라이언트에 다시 전달합니다.
5. AVD 클라이언트는 사용 가능한 리소스에 대한 연결 구성을 .rdp 파일 세트에 저장합니다.
6. 사용자가 연결할 리소스를 선택하면 AVD 클라이언트는 연관된 .rdp 파일을 사용하여 가장 가까운 AVD 게이트웨이 인스턴스로 보안 TLS 1.2 연결을 설정한 후 연결 정보를 전달합니다. (ⓓ)
7. AVD 게이트웨이는 요청의 유효성을 검사하고 AVD 브로커에게 연결을 조율하도록 요청합니다. (ⓔ)
8. AVD 브로커는 세션 호스트를 식별하고 이전에 설정된 영구 통신 채널을 사용하여 연결을 초기화합니다.
9. 원격 데스크톱 스택은 AVD 클라이언트에서 사용하는 것과 동일한 AVD 게이트웨이 인스턴스에 대한 TLS 1.2 연결을 시작합니다.
10. 클라이언트 및 세션 호스트 둘 다 게이트웨이에 연결되면 게이트웨이는 두 엔드포인트 간에 원시 데이터 전달을 시작합니다. 그러면 RDP에 대한 기본 역방향 연결 전송이 설정됩니다.
11. 기본 역방향 연결 전송이 설정된 후 클라이언트는 RDP 핸드셰이크를 시작합니다.

5. AVD 아키텍처 - 네트워크 연결 #2

CLOUD ON
Azure Managed Service

RDP Shortpath는 AVD 클라이언트와 세션 호스트 간에 직접 UDP 기반 전송을 설정하는 기능입니다.



<Azure Virtual Desktop 네트워크 연결 이해 #2>

<관리 네트워크에서 RDP Shortpath가 작동하는 방식>

모든 연결은 AVD Gateway를 통해 TCP 기반 역방향 연결 전송을 설정하여 시작됩니다. 그런 다음 AVD 클라이언트와 세션 호스트는 초기 RDP 전송을 설정하고 기능 교환을 시작합니다. 이러한 기능들은 다음 프로세스를 사용하여 협상됩니다:

1. 세션 호스트는 IPv4 및 IPv6 주소 목록을 클라이언트에 보냅니다.
2. 클라이언트는 백그라운드 스레드를 시작하여 세션 호스트의 IP 주소 중 하나에 직접 병렬 UDP 기반 전송을 설정합니다.
3. 클라이언트가 제공된 IP 주소를 검색하는 동안 사용자 연결에 지연이 없도록 하기 위해 역방향 연결 전송을 통해 초기 연결을 계속 설정합니다.
4. 클라이언트가 세션 호스트에 직접 연결되어 있는 경우 클라이언트는 보안 TLS 연결을 설정합니다.
5. RDP Shortpath 전송을 설정한 후 원격 그래픽, 입력 및 디바이스 리디렉션을 포함한 모든 DVC(동적 가상 채널)가 새 전송으로 이동됩니다. 그러나 방화벽이나 네트워크 토폴로지에 따라 클라이언트가 직접 UDP 연결을 설정하지 못하는 경우 RDP는 역방향 연결 전송을 계속합니다.

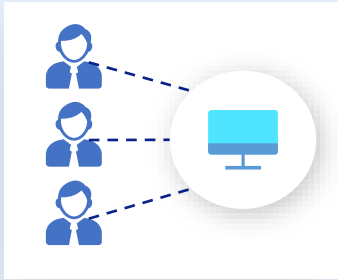
사용자가 관리 네트워크용 RDP Shortpath와 공용 네트워크를 모두 사용할 수 있는 경우 발견된 첫 번째 알고리즘이 사용됩니다. 먼저 설정되는 연결이 사용자가 해당 세션에 사용할 연결입니다.

6. AVD에 적용된 기술 - 멀티세션

CLOUD ON
Azure Managed Service

Windows 10/11 Enterprise 멀티세션은 여러 동시 대화형 세션을 허용하는 새로운 원격 데스크톱 세션 호스트입니다.

- 이전에는 Windows Server에서만 제공하였던 기능
- IT 부서에서는 멀티세션의 비용적인 이점을 활용 가능
- 별도로 RDS CAL 라이선스를 구매할 필요없이 사용자당 Windows 라이선스 이용
- Windows 10/11 Enterprise 멀티세션의 ProductType은 Windows Server와 동일
- 실제 서비스 목적으로 Azure 외부에서 Windows 10/11 Enterprise 멀티세션을 실행하는 것은 라이선스 계약 위반
- Windows 10/11 Enterprise 멀티세션은 원격 데스크톱 IP 가상화를 지원하지 않음
- Windows 10/11 Enterprise 멀티세션 이미지는 Azure 갤러리에서 구할 수 있음
- Windows 10/11 Enterprise 멀티세션 이미지 커스터마이징 과정:
  ① Azure에서 Windows 10/11 Enterprise VM 생성
  ② 생성된 VM의 VHD를 다운로드
  ③ 다운로드한 VHD를 Hyper-V 위에 1세대 VM으로 생성
  ④ LOB 애플리케이션을 설치한 후, sysprep 수행
  ⑤ VHD 이미지를 Azure 상에 업로드 후, AVD에서 해당 이미지 사용하여 호스트풀 배포



<멀티세션 VM 추천 사항>

워크로드 유형	vCPU당 최대 사용자 수	최소 vCPU /RAM /OS 스토리지	Azure 인스턴스 예제	최소 프로필 스토리지
Light	6	8개 / 16GB / 32GB	D8s_v5, D8s_v4, F8s_v2, D8as_v4, D16s_v5, D16s_v4, F16s_v2, D16as_v4	30GB
Medium	4			
Heavy	2			
Power	1	16개 / 56GB / 340GB	D16ds_v5, D16s_v4, D16as_v4, NV6, NV16as_v4	

- 모든 VM은 최소 4개 이상의 vCPU가 있어야 함
- 32개 vCPU를 초과하는 VM은 권장하지 않음. 16개 vCPU VM이 가성비가 제일 좋음

6. AVD에 적용된 기술 - FSLogix

CLOUD ON
Azure Managed Service

FSLogix는 AVD와 같은 원격 컴퓨팅 환경에서 사용자 프로필 로밍을 지원하는 솔루션입니다.

- FSLogix를 2018년에 인수한 이후, 사용자 프로필 솔루션을 FSLogix 프로필 컨테이너로 변경하고 있음
- FSLogix 핵심 기술
  - *프로필 컨테이너*
    - ❖ 로밍 프로필 및 폴더 리디렉션 대체
    - ❖ Office 365 컨테이너 포함 (Office 캐시 데이터 로밍)
  - *앱 마스킹*
    - ❖ 애플리케이션에 대한 접근 권한을 사용자당, IP 주소 등으로 조정 가능
  - *Java 리디렉션*
    - ❖ 개별 앱 또는 웹사이트에 특정 버전의 Java를 각각 매핑
- FSLogix는 Microsoft 365 및 RDS 고객에게 추가 비용 없이 제공
- FSLogix 프로필 컨테이너는 Azure Files 또는 Azure NetApp Files와 같은 클라우드 스토리지에 저장

<FSLogix 프로필 컨테이너가 저장될 Azure 스토리지 솔루션 비교>

기능	Azure Files	Azure NetApp Files
사용 사례	범용 가상 컴퓨터	Ultra급 성능 또는 NetApp 온-프레미스에서 마이그레이션
플랫폼 서비스	Azure 자체 솔루션	Azure 자체 솔루션
국가별 가용성	모든 리전	한국 포함 31개 리전
중복	로컬 중복/영역 중복/지역 중복/지역 영역 중복	지역 간 복제를 사용하여 로컬 중복/지역 중복
계층 및 성능	Standard(트랜잭션 최적화) Premium 공유당 최대 100K IOPS, 공유당 10GBps, 약 3ms의 대기 시간	Standard Premium Ultra 볼륨당 최대 4.5GBps, 약 1ms의 대기 시간
용량	공유당 100TiB, 범용 계정당 최대 5PiB	볼륨당 100TiB, 구독당 최대 12.5PiB
필요한 인프라	최소 공유 크기 1GiB	최소 용량 풀 4TiB, 최소 볼륨 크기 100GiB
프로토콜	SMB 3.0/2.1, NFSv4.1(미리 보기), REST	NFSv3, NFSv4.1(미리 보기), SMB 3.x/2.x

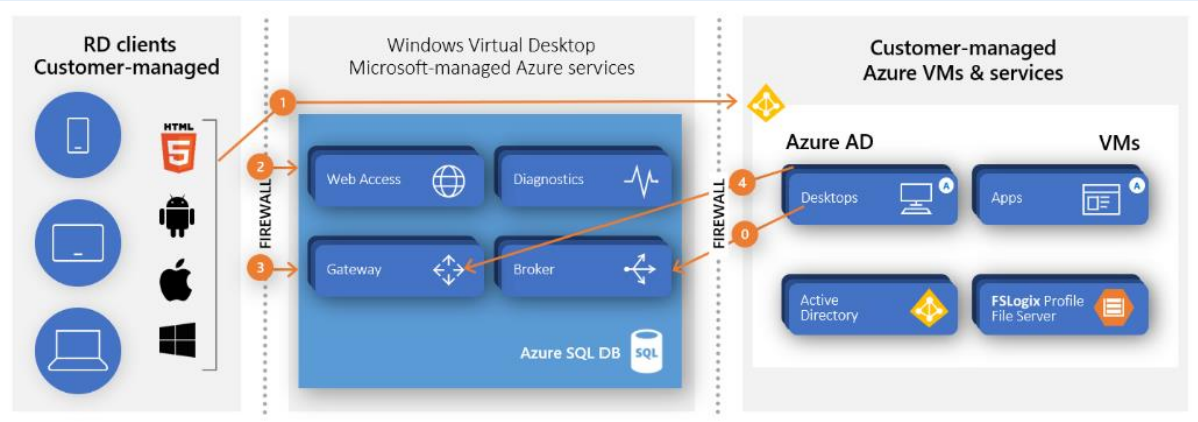
6. AVD에 적용된 기술 - 역방향 연결

CLOUD ON
Azure Managed Service

AVD 역방향 연결 기술은 인바운드 포트를 열어야 하는 필요성을 제거하여 공격 지점을 감소시킵니다.

- AVD는 원격 세션을 설정하고 RDP 트래픽을 운반하기 위해 역방향 연결 전송 사용
- 온-프레미스 기반의 원격 데스크톱 서비스 배포와 달리, 역방향 연결 전송은 들어오는 RDP 연결을 수신하기 위해 TCP 수신기를 사용하지 않음
- AVD VM이 시작될 때, AVD 인프라에 대한 아웃바운드 HTTPS 연결을 사용하여 영구 통신 채널을 설정함

<역방향 연결 네트워크 흐름>



1. 사용자가 RD 클라이언트를 시작하면, Azure AD에 연결하여 로그인을 한 후, Azure AD는 토큰을 반환합니다.
2. RD 클라이언트는 웹액세스에 토큰을 제출하고, 브로커는 DB에 쿼리하여 사용자에게 인가된 리소스를 확인합니다.
3. 사용자가 리소스를 선택하면, RD 클라이언트는 게이트웨이에 연결합니다.
4. 브로커는 세션 호스트 에이전트로부터 게이트웨이로의 연결을 조율합니다.
5. RDP 트래픽은 연결 3과 4를 통해 RD 클라이언트와 세션 호스트 VM 간에 이동합니다.

(* 상기 내용은 christiaanbrinkhoff.com 사이트의 자료를 인용함)

6. AVD에 적용된 기술 - 자동 크기 조정

CLOUD ON
Azure Managed Service

자동 크기 조정 또는 크기 조정 도구를 사용하여 호스트풀의 세션 호스트 VM을 늘리거나 줄여서 배포 비용을 최적화 합니다.

자동 크기 조정(Autoscale)

- AVD 자동 크기 조정을 이용하여 세션 호스트 VM을 늘리거나 줄일 수 있습니다.
- 다음 항목 기반으로 크기 조정 계획 수립이 가능합니다:
  - 하루 중 시간
  - 특정 요일
  - 세션 호스트당 세션 제한
- 호스트풀당 하나의 크기 조정 계획만 연결 가능합니다.
- 크기 조정 계획은 사용하도록 설정하는 즉시 적용됩니다.
- 제한 사항
  - AVD(classic)은 자동 크기 조정을 지원하지 않습니다.
  - 자동 크기 조정은 Azure Stack HCI용 AVD를 지원하지 않습니다.
  - 자동 크기 조정은 현재 한국 리전을 포함한 일부 Azure 리전에서는 지원하지 않습니다.

크기 조정(Scaling) 도구

- Azure Automation과 Logic Apps 서비스를 이용하여 사용량의 변화에 따라 세션 호스트 VM을 늘리거나 줄일 수 있습니다.
- 크기 조정 도구를 이용한 작업
  - 사용량이 많은 시간과 적은 시간을 기준으로 VM이 시작 및 중지되도록 예약
  - CPU 코어당 세션 수를 기준으로 VM을 늘림 (풀 방식의 멀티세션 VM에 한함)
  - 사용량이 적은 시간에는 VM을 줄여서 실행 중인 세션 호스트 VM의 수를 최소로 유지
- 크기 조정 도구는 Azure Automation 계정, PowerShell Runbook, 웹후크 및 Logic Apps의 조합을 사용하여 작동합니다. Logic Apps가 웹후크를 호출하여 Runbook을 실행하고, Runbook은 Job을 생성합니다.
- Runbook에서 Job의 최대 실행 시간은 3시간입니다.

7. 금융분야 규정 - 전자금융감독규정

CLOUD ON
Azure Managed Service

전자금융감독규정은 금융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정하고 있습니다.

제14조의2(클라우드컴퓨팅서비스 이용절차 등)

① 금융회사 또는 전자금융업자는 “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률“ 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.

1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가
2. <별표 2의2>의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가
3. <별표 2의3>에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항제1호에 따라 다음 각 호의 어느 하나에 해당한다고 평가하는 경우에는 클라우드컴퓨팅서비스를 실제로 이용하려는 날의 7영업일 이전에 금융감독원장이 정하는 양식에 따라 제4항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다. 이 경우 “금융회사의 정보처리 업무 위탁에 관한 규정” 제7조 제1항부터 제3항까지의 규정에 따라 보고한 것으로 본다.

1. 고유식별정보 또는 개인신용정보를 처리하는 경우
2. 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 경우

④ …

⑤ …

(참조 링크: 전자금융감독규정 (law.go.kr) / 전자금융감독규정시행세칙 (law.go.kr))

제15조(해킹 등 방지대책)

① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch) 사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)
4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

② …

③ …

➔ 전자금융감독규정시행세칙

제2조의2(망분리 적용 예외)

① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 다음 각 호와 같다.

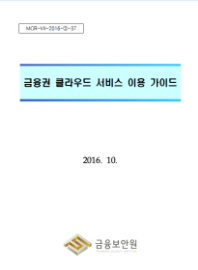
1. 내부 통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결해야 하는 경우
2. 규정 제12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로부터 내부 업무용시스템으로 원격접속 하는 경우

7. 금융분야 규정 - 클라우드 이용 가이드

CLOUD ON
Azure Managed Service

2016년 10월 이후로 금융권에서도 퍼블릭 클라우드 이용이 가능해졌으며, 2019년부터 본격적인 클라우드 도입이 진행되고 있습니다.

2016.10.

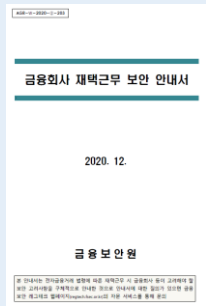


- 금융보안원에서 “금융권 클라우드 서비스 이용 가이드” 발간 (클라우드 규제 개선 관련 “전자금융감독규정” 개정 - 제14조의2 신설)
- 비중요 정보처리시스템에 한하여 클라우드를 사용 가능
- 비중요 정보처리시스템만 위치한 전산실에 대해서는 “전자금융감독규정” 예외 인정 (국내 DC, 무선통신망 설치 금지, 외부통신망과의 분리)
- 고유식별정보 또는 개인신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템 지정 불가
- 홍보용 홈페이지, 인터넷메일시스템 등의 15가지의 비중요 정보처리시스템 지정 가능 예시 제공

2019.01.

- 금융보안원에서 “금융분야 클라우드컴퓨팅서비스 이용 가이드” 발간 (“전자금융감독규정” 개정 - 제14조의2 개정)
- 금융회사의 클라우드컴퓨팅서비스 이용을 위한 세부절차 안내 (사전 준비 > 계약 체결 > 보고 및 이용 > 이용 종료)
- 이용 대상 정보처리업무 선정 및 중요도 평가 후, 업무연속성 계획 및 안전성 확보조치 방안을 수립하고 업무 위수탁 기준을 보완해야 함
- 클라우드서비스 제공자의 건전성 및 안전성을 평가해야 하며, 정보보호심의위원회의 심의 의결해야 함
- 중요 업무의 경우, 클라우드 서비스를 실제로 이용하려는 날의 7영업일 이전에 금융감독원에 보고해야 함 (비중요 업무시스템은 요청 시 제공 의무)
- 중요 정보처리시스템은 국내에 설치하여야 하고, 해당 전산실 내에 무선통신망 설치 금지

2020.12.



- 금융보안원에서 “금융회사 재택근무 보안 안내서” 발간 (“전자금융감독규정시행세칙” 개정 - 제2조의2 개정)
- 재택근무 수행 필요성이 급증함에 따라 “전자금융감독규정 시행세칙”을 개정하여 재택근무를 위한 원격접속 시 정보보호 통제사항을 규정
- 원격접속을 통해 내부망에 접속하는 방식은 “간접 접속”과 “직접 접속”으로 접속 방식 선택 가능
- “간접 접속” 방식으로는 가상화 데스크톱 기반(VDI) 방식과 원격접속 프로그램 방식이 있음
- 외부 단말기에 화면 캡처 방지 등의 보안 관리를 해야 하며, 간접 접속의 경우 파일 송수신 차단 및 내부망 접속 시 인터넷 연결 차단 등의 추가 보안통제 적용 필요

2022.11.

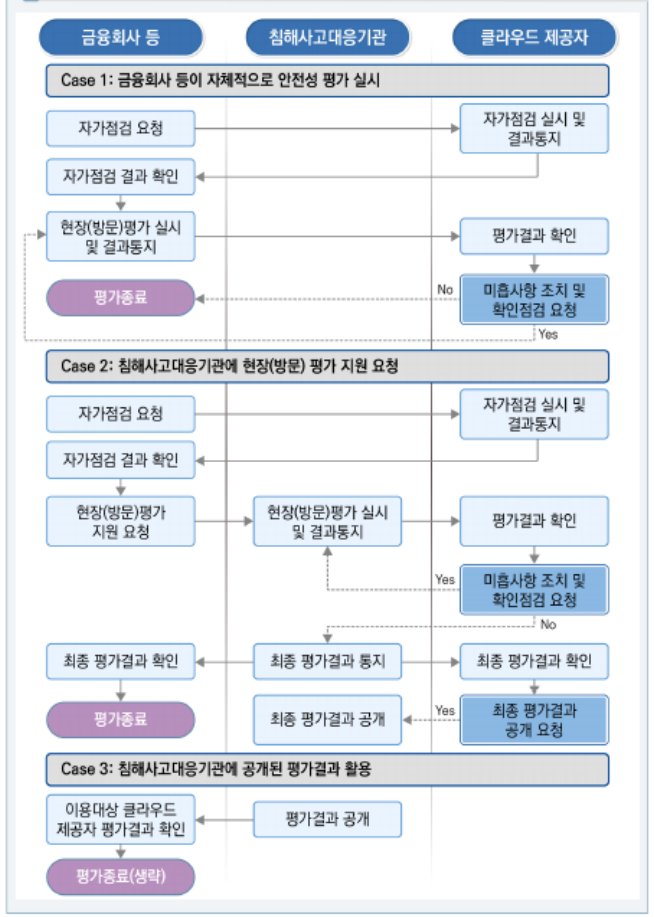
- 2022.04.14.에 발표한 “클라우드 및 망분리 규제 개선방안”에 따라 “전자금융감독규정” 개정안 변경 예정
- 클라우드 이용절차 명료화 및 비중요업무에 대한 절차 간소화, 클라우드 이용 시 사후보고로 전환, 연구와 개발 목적의 경우에는 망분리 규제 완화 등

7. 금융분야 규정 - 안전성 평가

CLOUD ON
Azure Managed Service

금융회사는 계약 준비단계에서 클라우드서비스 제공자를 대상으로 안전성 평가를 진행해야 합니다.

참고 클라우드서비스 제공기준 평가 절차 통합 Flow



- 일반적으로 금융보안원과 같은 침해사고대응기관을 통해 안전성 평가를 진행함
- 안전성 평가 항목 (IaaS 기준 기본 보호조치 109개, 금융부문 추가 보호조치 32개)
  - 기본 보호조치 항목은 과기정통부 주관 클라우드서비스 보안인증제(CSAP)의 일반적 평가·인증 통제항목 준용
  - 국내·외 클라우드 보안인증(4개) 중의 하나를 취득·유지하고 있는 클라우드서비스 제공자의 해당 서비스에 대해서는 '기본 보호조치' 항목 평가 생략 가능

참고 CSAP의 평가·인증 통제항목

통제분야	통제항목수	
	IaaS	SaaS
1. 정보보호 정책 및 조직	5개	5개
2. 인적보안	12개	5개
3. 자산관리	10개	3개
4. 서비스 공급망 관리	4개	3개
5. 침해사고 관리	7개	7개
6. 서비스 연속성 관리	7개	6개
7. 준거성	4개	3개
8. 물리적 보안	12개	-
9. 가상화 보안	10개	6개
10. 접근통제	10개	10개
11. 네트워크 보안	6개	5개
12. 데이터 보호 및 암호화	10개	8개
13. 시스템 개발 및 도입 보안	12개	10개
합계	**109개**	**71개**

구분	인증제도명	평가생략 근거
국내	클라우드 서비스 보안인증제(CSAP)	• 과기정통부 주관, KISA가 평가·인증 • 국내 주요 클라우드 사업자가 인증 취득 • 평가항목수가 최대 120여개
해외	FedRAMP(High) (미국)	• 정부(FedRAMP 관리국) 주관 • 평가항목 수가 최대 400여개
	CSA STAR Certification(Gold) (Global)	• 400여개의 클라우드 사업자가 회원인 글로벌 클라우드 보안협회(CSA*) 주관 * CSA : Cloud Security Alliance • 평가항목 수가 최대 300여개
	MTCS(Level 3) (싱가포르)	• 정보통신미디어개발청(IMDA) 주관

※ 위 리스트는 상기 기준에 부합하여 평가 생략이 가능한 인증 제도를 열거한 것이며, 동 기준에 부합하는 국내·외 클라우드 보안인증제가 추가로 확인되는 경우, 지속 업데이트할 계획

8. AVD 활용 시나리오 - 분류

CLOUD ON
Azure Managed Service

금융권에서 도입한 AVD 활용 시나리오는 망분리 PC 및 재택근무 용도, 원격 App 사용 등이 있습니다.

인터넷 PC 또는 내부망 PC

1. 망분리 환경에서 인터넷이 가능한 PC 또는 인터넷이 차단된 내부망 PC 제공 (VDI)
2. 네트워크 회선 증설이 필요한 물리 PC 대신에 가상 PC 제공
3. 망연계 솔루션과의 연동 필요
4. 근무 시간에만 운영
5. 사용 시간 기반의 비용 발생
6. 신규 수요 발생 시, 가상 PC 확장이 용이

재택근무 용도 VDI

1. 금융회사 재택근무 허용에 따른 간접 접속 방식의 VDI 제공
2. 외부 단말기에서 접속 가능한 관리되는 가상 PC 제공
3. 회사 보안 정책 적용 및 준수 (VPN 연결)
4. VPN 연결 시, 외부 단말기의 인터넷을 차단하는 보안 솔루션 필요
5. 재택 상황 발생 시에만 운영
6. 사용 시간 기반의 비용 발생

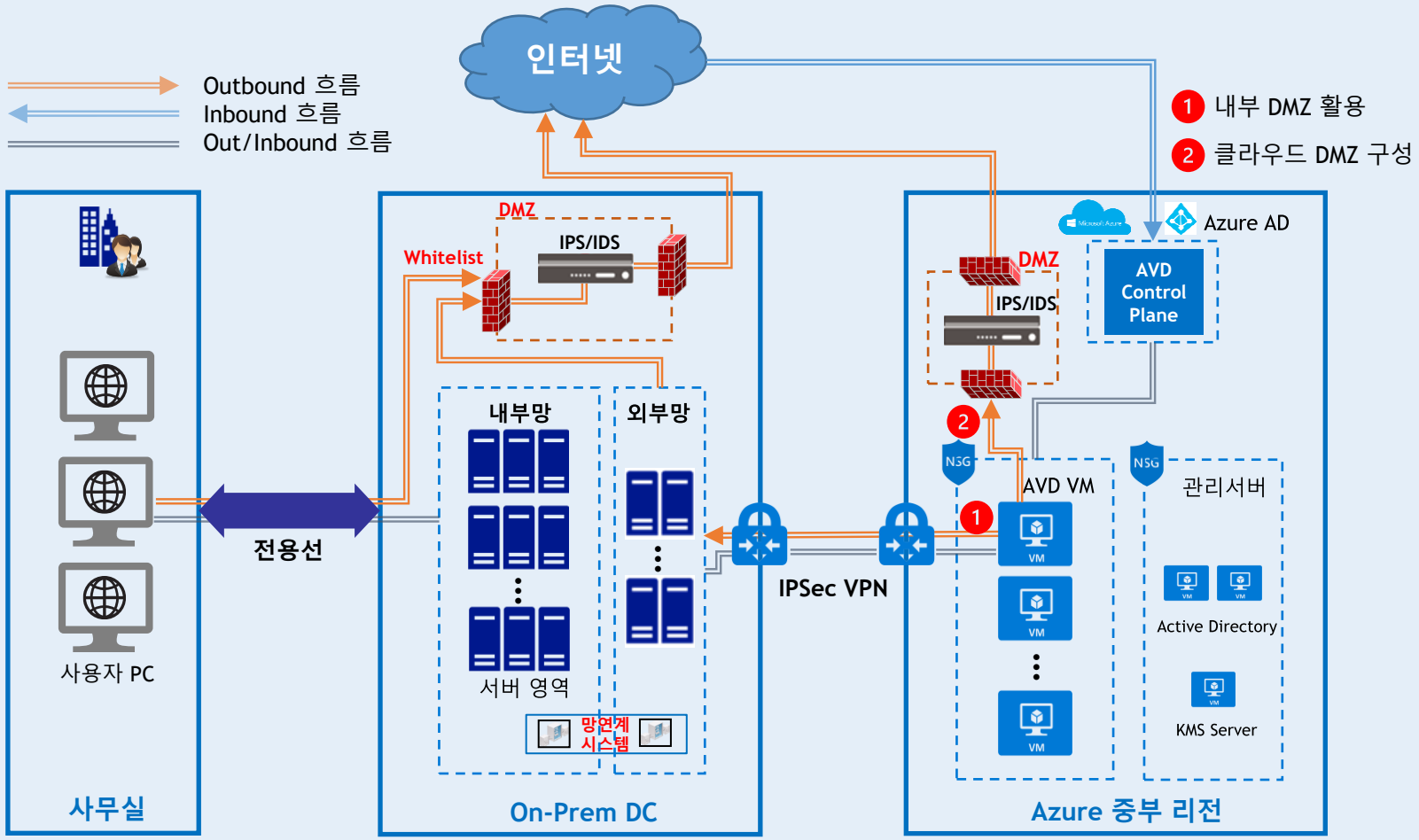
원격 App 제공 PC

1. 데스크톱 환경 대신에 필요한 App만 제공하는 환경
2. 개인 사용자의 데이터는 별도의 개인용 폴더에 저장
3. 원격 App에 대한 표준 사용자 권한만 제공
4. 키보드 보안 프로그램 등은 지원하지 않음 (멀티세션 OS)
5. 근무 시간에만 운영
6. 사용 시간 기반의 비용 발생
7. 멀티세션 데스크톱을 제공함으로써 비용 절감 효과 극대화

8. AVD 활용 시나리오 - 인터넷 PC

CLOUD ON
Azure Managed Service

금융회사 내의 망분리 적용이 된 인터넷 PC 환경을 AVD로 대체하여 구성 가능합니다.



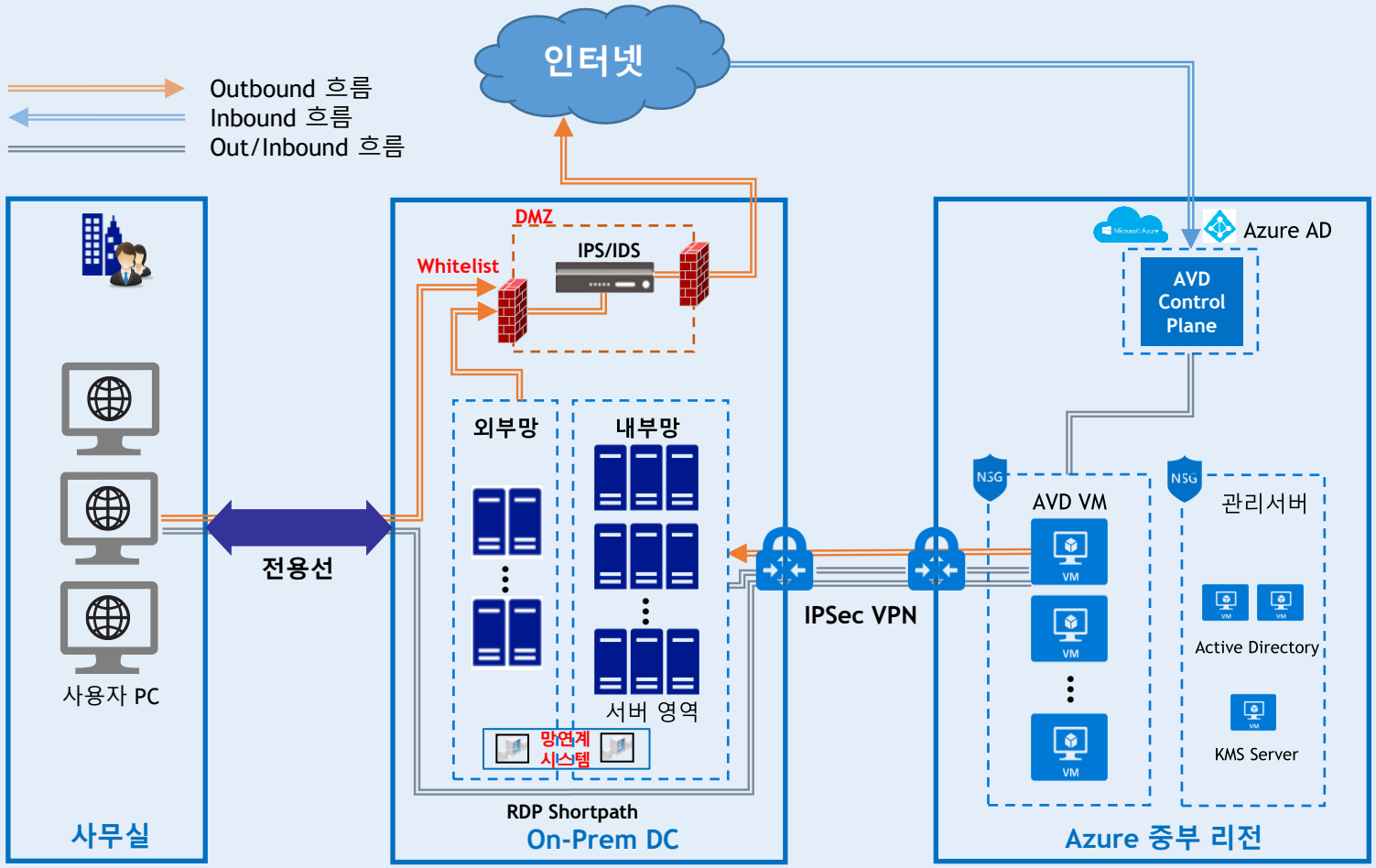
고려 사항

1. 인터넷 연결을 위한 DMZ를 Azure 상에 구현할 지, On-premise DMZ를 이용할 지를 결정
2. 클라우드 DMZ를 구성할 경우, 인터넷 트래픽 모니터링을 위한 보안 솔루션 검증 필요 (DDoS/IPS/IDS/Firewall/DLP/Contents Filtering 등)
3. AVD VM에 설치될 내부 보안 소프트웨어 및 애플리케이션과의 호환성 확보 필요 (망연계 솔루션 포함)
4. AVD VM 화면 전송 및 Azure AD와의 통신을 위한 Microsoft 서비스와의 인터넷 연결 필요
5. 인터넷 사이트 연결 시, 외부 보안 프로그램과의 호환성 확보
6. Azure AD Domain Services 사용 여부
7. 비용 절감을 위한 Windows 10/11 멀티세션 사용 여부

8. AVD 활용 시나리오 - 내부망 PC

CLOUD ON
Azure Managed Service

금융회사 내의 망분리 적용이 된 내부망 PC 환경을 AVD로 대체하여 구성 가능합니다.



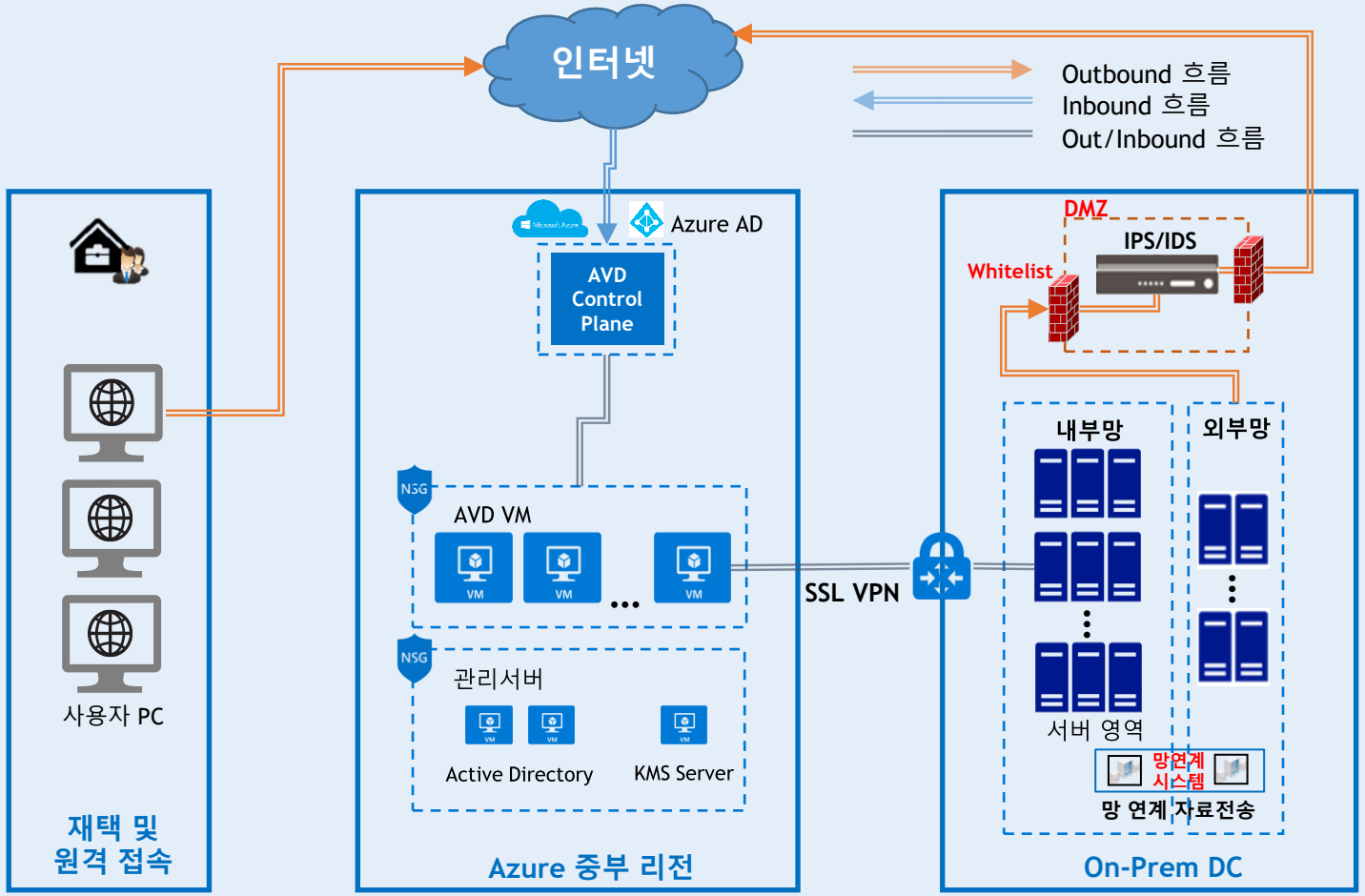
고려 사항

1. Azure 데이터센터에서는 인터넷 연결 차단
2. 인터넷 연결이 가능한 사용자 PC에 화면 캡처 방지 등의 보안 솔루션 설치 필요
3. AVD VM에 설치될 내부 보안 소프트웨어 및 애플리케이션과의 호환성 확보 필요 (망연계 솔루션 포함)
4. Azure AD와의 통신을 위한 Microsoft 서비스와의 인터넷 연결 필요
5. 사용자 PC와 AVD VM은 내부망 네트워크를 통한 연결 기능 활용 (RDP Shortpath)

8. AVD 활용 시나리오 - 재택근무 용도 PC

CLOUD ON
Azure Managed Service

금융권의 재택근무 허용에 따라 간접 접속 방식의 VDI 환경으로 AVD를 도입 사용 가능합니다.



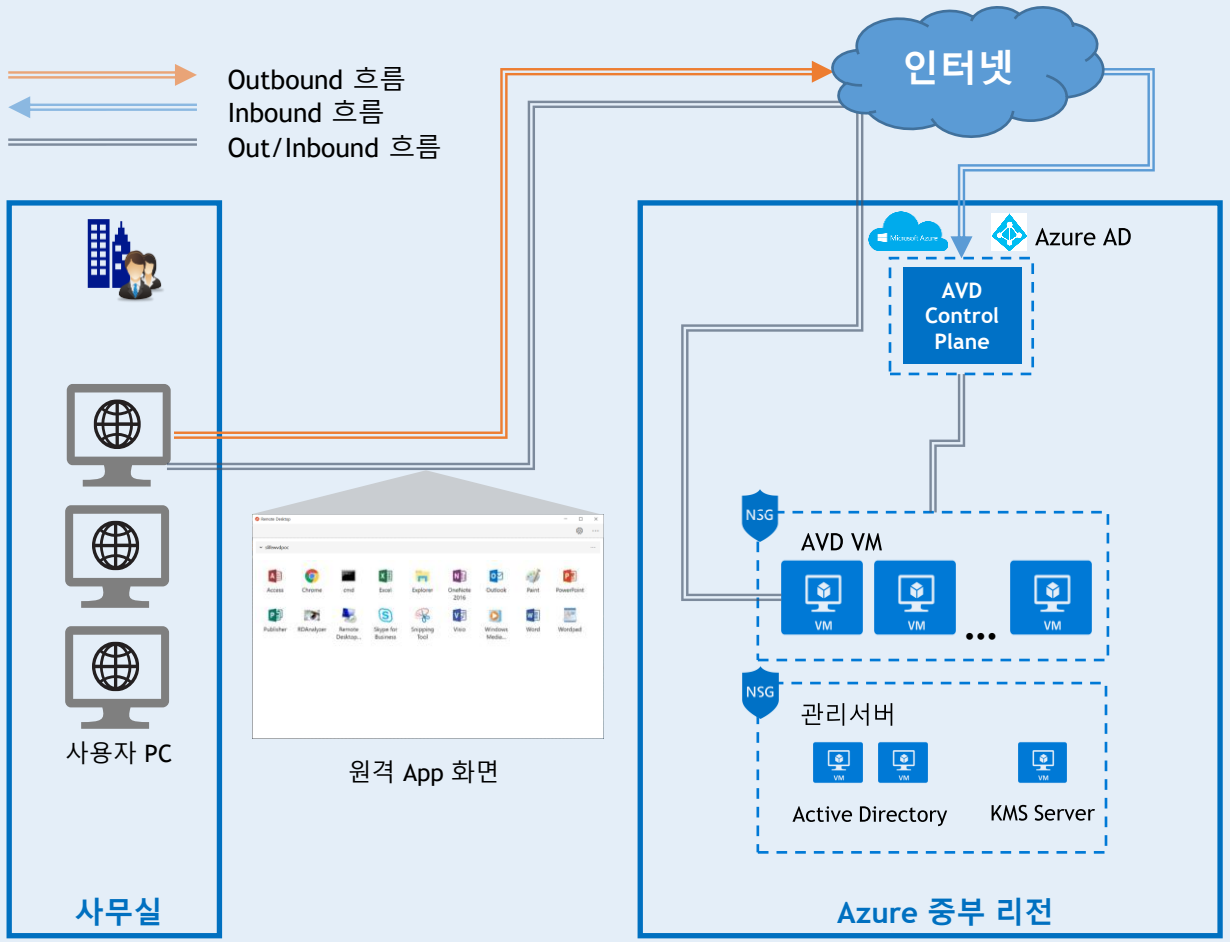
고려 사항

1. 외부 단말기(사용자 PC 또는 태블릿)에서 보안 대책이 수립되어 있어야 함 (업무망으로 VPN 연결 시, 사용자 PC에서 인터넷 사용 차단 등)
2. AVD VM과의 연결을 위한 SSL VPN 솔루션 필요 (F5 등)
3. AVD VM에 설치될 내부 보안 소프트웨어 및 애플리케이션과의 호환성 확보 필요
4. Azure AD Domain Services 사용 여부
5. 비용 절감 및 운영 효율화를 위한 VM 관리 필요

8. AVD 활용 시나리오 - 원격 App 제공 PC

CLOUD ON
Azure Managed Service

AVD 사용자에게 바탕화면이 아닌 필요한 App 아이콘만 제공하여 필요한 업무만 수행할 수 있도록 합니다.



고려 사항

1. 사용자에게 필요한 App들을 지정
2. 원격 App은 멀티세션 OS에서만 제공되는 기능이므로, App 및 OS에 대한 표준 사용자 권한만 제공됨
3. 개인 사용자의 데이터 저장 위치 지정 필요
4. 키보드 보안 프로그램 등은 지원하지 않음 (멀티세션 OS)
5. 비용 절감 및 운영 효율화를 위한 VM 관리 필요

9. 요약

퍼블릭 데스크톱 서비스인 AVD를 도입하여 다양한 사용자의 요구 사항 수용, 관리 부담 감소, 그리고 비용 절감 효과를 기대할 수 있습니다.

사용자 경험 향상

- 스마트폰 및 태블릿 등의 다양한 단말기 지원
- 재택근무자의 간접 접속 방식을 위한 VDI 원격 근무 환경 제공
- GPU 등의 특정 워크로드를 지원하는 컴퓨팅 리소스 이용

관리 용이성

- 퍼블릭 클라우드의 인프라 확장 용이성을 활용
- VDI 인프라 관리 부담 최소화
- 특정 사용자에게 필요한 App만 제공 가능
- 망분리 환경을 위한 VDI 환경 제공

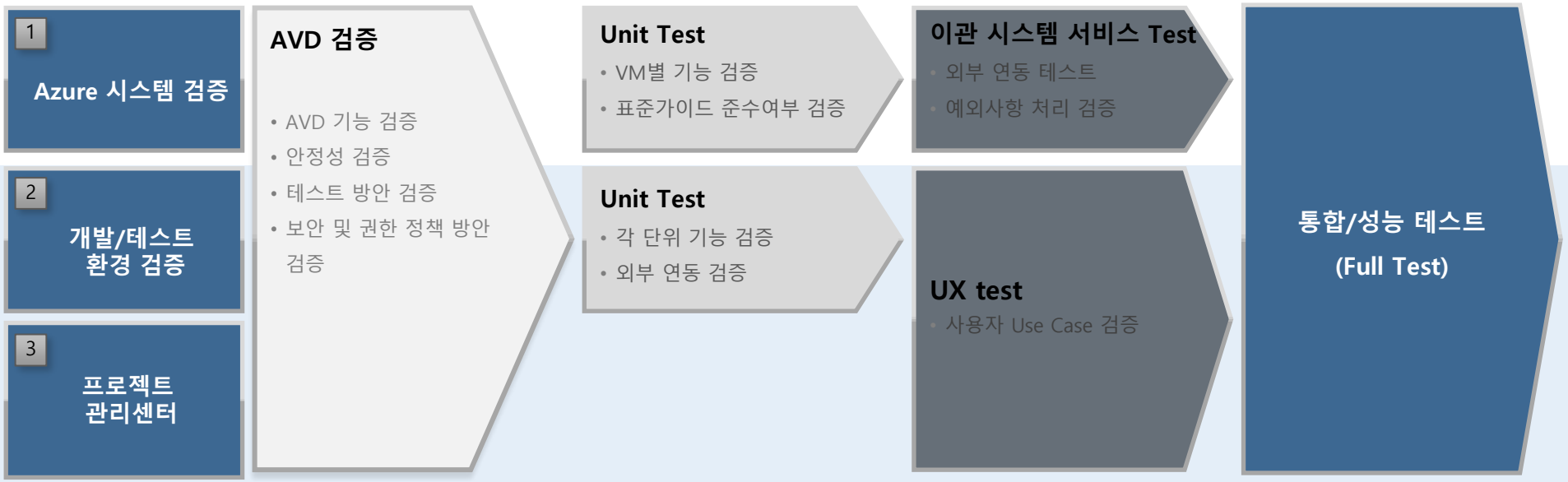
비용 절감

- 컴퓨팅 리소스에 대해 사용량 기반 과금으로 비용 절감
- Azure 상에서만 제공되는 Windows 10/11 멀티세션 활용
- Azure Hybrid Benefit과 Azure Savings Plan을 이용

10. CloudON for Infrastructure (AVD) : 2wk Assessment 개요

CLOUD ON
Azure Managed Service

다음과 같은 전체 일정 및 지원항목을 통해 고객의 성공적인 AVD 구축을 위한 환경을 분석하고 해당 내용을 프로젝트에 반영하여 고객이 만족하는 최적의 구성을 구현합니다.



11. CloudON for Infrastructure (AVD) : 2wk Assessment 특장점

CLOUD ON
Azure Managed Service

안정적인 가상화 프로젝트 구축을 위해 씨앤토트는 고객사의 Vision과 목표를 명확하게 이해하고 있으며, 고객사의 시스템을 성공적으로 구축하기 위해 씨앤토트의 준비된 사업수행 역량과 유사 프로젝트 수행 경험을 바탕으로 다음과 같이 제안합니다.

고객사 요청 사항에 맞는 Cloud 시스템 구축

- TCO 절감효과를 확보할 수 있는 Cloud 솔루션 제안
- 전문화된 가상화 솔루션 구축 리소스로 안정적인 구축 및 사후 유지보수 및 운영지원
- 고객사의 상황에 맞는 유기적인 Cloud 아키텍쳐 제안

검증된 Cloud 시스템 구축 경험

- 검증된 cloud AVD 구축경험
- 목표 시스템 에 대한 최적화된 제안시스템 구축
- 유사 시스템 구축 경험과 Know-how
- 다양한 형태의 Cloud 프로젝트 수행으로 검증된 기술력

표준화 및 확장성을 고려한 유연한 설계 및 개발

- 업계 표준을 고려한 표준화 방안 수립 및 적용
- 다양한 요구 및 환경 수용이 용이한 가상화 구조 제안
- 오픈소스를 이용한 향 후 가상화 방안 준비
- 다양한 활용성을 고려한 유연한 구조의 아키텍쳐 설계

강력한 수행 조직 구성 및 철저한 유지 관리

- 다양한 분야에서의 Platform 구축경험을 보유하고 관련 프로젝트 수행경험이 풍부한 PM투입
- PL급 이상 핵심인력을 컨소시엄별 고급 기술자로 제안
- 아키텍처 전문인력 투입
- 체계적이고 과학적인 프로젝트 관리
- 다양한 분야의 프로젝트에서 검증된 운영능력 보유

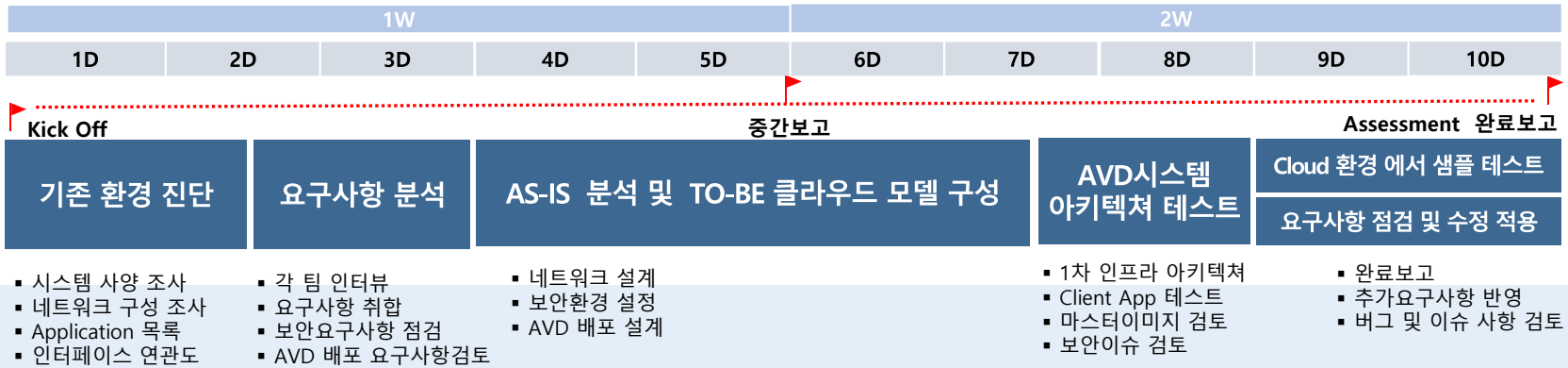
12. CloudON for Infrastructure (AVD) : 2wk Assessment 일정

CLOUD ON
Azure Managed Service

분석 단계는 다음과 같은 2 Week 일정으로 진행됩니다.

진행일정

수행



세부일정

구분	Test 일자	Cut-Over	대상 업무	담당
환경분석 및 진단	4D		Infra Assessment, Risk Assessment, 보안성 검토, TCO분석	씨앤토트
AVD설계	2D		전체 아키텍쳐 설계 및 검토	씨앤토트
AVD 시스템테스트	4D		AVD 전환 가능여부를 위한 미니 테스트	씨앤토트
APP 호환성검증	4D		Client APP 기능 테스트 및 이슈 분석	씨앤토트
보안 및 추가 검증	2D		보안사항 점검 및 Cloud 보안성 반영 검토	씨앤토트

씨앤토트

AVD 도입을 위한
씨앤토트만의 5종 프로모션

혜택 01

Assessment

AVD를 위한 사전진단
CloudON Assessment 제공
(1~3days)

혜택 02

무상 PoC

AVD 시뮬레이션 및 검토를
위한 PoC 진행 (5days)

혜택 03

USD 1,500

Azure 크레딧 지원!
(PoC/Test 사용을 위한
무료 크레딧)

혜택 04

Workshop

클라우드 환경의
문턱을 낮춰주는
맞춤형 팀 워크샵 (1~2days)

혜택 05

50% 할인!

매니지드서비스 CloudON
최초 1년 할인 혜택

CLOUD ON
Azure Managed Service

THANK YOU

cloudon@cnthoth.com
www.cnthoth.com