# VDS를 사용한 배포

## Virtual Desktop Service

NetApp
April 28, 2022

# 목차

# VDS를 사용한 배포

# Azure를 지원합니다

## Azure 가상 데스크톱

### Avd 배포 가이드

#### 개요

이 가이드에서는 Azure에서 VDS(NetApp Virtual Desktop Service)를 사용하여 Azure AVD(Virtual Desktop) 구축을 생성하는 단계별 지침을 제공합니다.

이 가이드는 다음 사이트에서 시작됩니다. https://cwasetup.cloudworkspace.com/

이 POC(개념 증명) 가이드는 테스트 Azure 구독에서 AVD를 빠르게 배포하고 구성하는 데 도움이 되도록 설계되었습니다. 이 가이드에서는 운영 환경 없이 깨끗한 Azure Active Directory 테넌트로 녹색 필드 배포를 가정합니다.

특히 기존 AD 또는 Azure AD 환경에 대한 프로덕션 배포는 매우 일반적인 작업이지만 이 POC 가이드에서는 이러한 프로세스를 고려하지 않습니다. 복잡한 POC 및 생산 배포는 NetApp VDS 영업/서비스 팀과 함께 시작되어야 하며 셀프 서비스 방식으로 수행되지 않습니다.

이 POC 문서는 전체 AVD 배포를 안내하며 VDS 플랫폼에서 사용 가능한 배포 후 구성의 주요 영역을 간략하게 설명합니다. 완료되면 호스트 풀, 앱 그룹 및 사용자를 포함한 AVD 환경을 완벽하게 구축하고 사용할 수 있습니다. 선택적으로 자동 애플리케이션 전송, 보안 그룹, 파일 공유 권한, Azure Cloud Backup, 지능형 비용 최적화를 구성할 수 있습니다. VDS는 GPO를 통해 일련의 모범 사례 설정을 배포합니다. 이러한 컨트롤을 선택적으로 비활성화하는 방법에 대한 지침도 POC에 관리되지 않는 로컬 장치 환경과 유사한 보안 컨트롤이 필요하지 않은 경우에 포함됩니다.

#### Avd 기본 사항

Azure Virtual Desktop은 클라우드에서 실행되는 포괄적인 데스크톱 및 앱 가상화 서비스입니다. 다음은 몇 가지 주요 기능과 특징을 간략하게 소개합니다.

- 게이트웨이, 브로커링, 라이센스 등록 및 로그인을 비롯하여 Microsoft의 서비스로서 제공되는 플랫폼 서비스입니다. 따라서 호스팅 및 관리가 필요한 인프라가 최소화됩니다.
- Azure Active Directory를 ID 공급자로 활용하여 조건부 액세스와 같은 추가 Azure 보안 서비스를 계층화할 수 있습니다.
- 사용자는 Microsoft 서비스에 대한 SSO(Single Sign-On) 환경을 경험할 수 있습니다.
- 사용자 세션은 독점적인 역방향 연결 기술을 통해 세션 호스트에 연결됩니다. 즉, 인바운드 포트를 열 필요가 없습니다. 대신 상담원이 AVD 관리 평면에 대한 아웃바운드 연결을 생성하고 최종 사용자 장치에 연결합니다.
- 역방향 연결을 사용하면 공용 인터넷에 노출되지 않고 가상 시스템을 실행할 수 있으므로 원격 연결을 유지하는 동안에도 격리된 워크로드가 가능합니다.
- Avd에는 Windows 10 멀티 세션에 대한 액세스가 포함되어 있어 Windows 10 Enterprise 환경에서 고밀도 사용자 세션의 효율성을 높일 수 있습니다.
- FSLogix 프로필 컨테이너화 기술은 사용자 세션 성능, 스토리지 효율성을 향상시키고 비영구 환경에서 Office 환경을 개선하는 기술을 포함합니다.

- Avd는 전체 데스크톱 및 RemoteApp 액세스를 지원합니다. 지속 또는 비지속, 전용 및 멀티 세션 환경 모두
- AVD는 RDS CAL의 필요성을 대체하고 Azure에서 세션 호스트 VM의 시간당 비용을 대폭 절감하는 "Windows 10 Enterprise E3 per User"를 활용할 수 있기 때문에 Windows 라이선스 비용을 절감할 수 있습니다.

가이드 범위

이 가이드는 Azure 및 VDS 관리자의 관점에서 NetApp VDS 기술을 사용하여 AVD를 구축하는 방법을 설명합니다. 사전 구성이 필요 없는 Azure 테넌트와 구독을 가져오며 이 가이드를 통해 AVD의 종단 간 설정을 수행할 수 있습니다

이 가이드에서는 다음 단계를 다룹니다.

1. Azure 테넌트, Azure 구독 및 Azure 관리자 계정 권한의 사전 요구 사항을 확인합니다
2. 필요한 검색 세부 정보를 수집합니다
3. Azure용 VDS 설정 마법사를 사용하여 Azure 환경을 구축합니다
4. 표준 Windows 10 EVD 이미지로 첫 번째 호스트 풀을 생성합니다
5. Azure AD 사용자에게 가상 데스크톱 할당
6. 사용자에게 데스크톱 환경을 제공하기 위한 기본 앱 그룹에 사용자를 추가합니다. 필요한 경우 RemoteApp 서비스를 제공하기 위한 추가 호스트 풀을 생성합니다
7. 클라이언트 소프트웨어 및/또는 웹 클라이언트를 통해 최종 사용자로 연결합니다
8. 플랫폼 및 클라이언트 서비스에 로컬 및 도메인 관리자로 연결합니다
9. 선택적으로 VDS admins 및 amp; AVD 최종 사용자를 위한 VDS의 다중 요소 인증을 활성화합니다
10. 필요에 따라 앱 라이브러리 채우기, 앱 설치 자동화, 사용자 및 보안 그룹의 앱 마스킹을 비롯한 전체 애플리케이션 자격 워크플로를 살펴봅니다
11. 필요에 따라 Active Directory 보안 그룹, 폴더 권한 및 응용 프로그램 권한을 그룹별로 생성하고 관리합니다.
12. 워크로드 스케줄링 및 라이브 확장을 비롯한 비용 최적화 기술을 선택적으로 구성합니다
13. 필요에 따라 향후 구축을 위해 가상 머신 이미지를 생성, 업데이트 및 Sysprep 합니다
14. 선택적으로 Azure Cloud Backup을 구성합니다
15. 필요에 따라 기본 보안 제어 그룹 정책을 사용하지 않도록 설정합니다

**Azure** 필수 구성 요소

VDS는 네이티브 Azure 보안 컨텍스트를 사용하여 AVD 인스턴스를 구축합니다. VDS 설정 마법사를 시작하기 전에 몇 가지 Azure 필수 구성 요소를 설정해야 합니다.

배포 중에 Azure 테넌트 내에서 기존 관리자 계정의 인증을 통해 서비스 계정 및 사용 권한이 VDS에 부여됩니다.

빠른 사전 요구 사항 체크리스트

- Azure AD 인스턴스가 있는 Azure 테넌트(Microsoft 365 인스턴스일 수 있음)
- Azure 구독
- Azure 가상 시스템에 사용 가능한 Azure 할당량
- 글로벌 관리자 및 구독 소유권 역할이 있는 Azure 관리자 계정

자세한 사전 요구 사항은 에 설명되어 있습니다 "PDF입니다"

**Azure AD**의 **Azure** 관리자

이 기존 Azure 관리자는 타겟 테넌트의 Azure AD 계정이어야 합니다. Windows Server AD 계정은 VDS 설정으로 배포할 수 있지만 Azure AD와의 동기화를 설정하는 데 추가 단계가 필요합니다(이 가이드의 범위 외).

사용자 > 모든 사용자 아래의 Azure Management Portal에서 사용자 계정을 찾아 확인할 수 있습니다.[]

글로벌 관리자 역할

Azure 관리자에게는 Azure 테넌트에서 글로벌 관리자 역할이 할당되어야 합니다.

**Azure AD**에서 역할을 확인하려면 다음 단계를 수행하십시오**.**

1. 에서 Azure Portal에 로그인합니다 https://portal.azure.com/
2. Azure Active Directory를 검색하여 선택합니다
3. 오른쪽 다음 창에서 관리 섹션의 사용자 옵션을 클릭합니다
4. 확인 중인 관리자 사용자의 이름을 클릭합니다
5. 디렉터리 역할을 클릭합니다. 맨 오른쪽 창에 글로벌 관리자 역할이 나열되어야 합니다[]

이 사용자에게 전역 관리자 역할이 없는 경우 다음 단계를 수행하여 추가할 수 있습니다**(**로그인 계정은 글로벌 관리자여야 이 단계를 수행할 수 있음**).**

1. 위의 5단계의 사용자 디렉토리 역할 세부 정보 페이지에서 상세 페이지 상단의 할당 추가 버튼을 클릭합니다.
2. 역할 목록에서 글로벌 관리자를 클릭합니다. 추가 버튼을 클릭합니다.[]

**Azure** 구독 소유권

Azure 관리자는 배포를 포함할 구독의 구독 소유자여야 합니다.

관리자가 구독 소유자인지 확인하려면 다음 단계를 수행하십시오**.**

1. 에서 Azure Portal에 로그인합니다 https://portal.azure.com/
2. 를 검색하고 구독 을 선택합니다
3. 오른쪽 다음 창에서 구독 이름을 클릭하여 구독 세부 정보를 확인합니다
4. 왼쪽에서 두 번째 창에서 IAM(액세스 제어) 메뉴 항목을 클릭합니다
5. 역할 할당 탭을 클릭합니다. Azure 관리자는 소유자 섹션에 나열되어야 합니다.[]

**Azure Administrator**가 나열되지 않은 경우 다음 단계를 수행하여 계정을 구독 소유자로 추가할 수 있습니다**.**

1. 페이지 맨 위에 있는 추가 단추를 클릭하고 역할 할당 추가 옵션을 선택합니다
2. 오른쪽에 대화 상자가 나타납니다. 역할 드롭다운에서 "소유자"를 선택한 다음 선택 상자에 관리자 사용자 이름을 입력합니다. 관리자의 전체 이름이 나타나면 선택합니다
3. 대화 상자 아래쪽에 있는 저장 단추를 클릭합니다[]

**Azure** 컴퓨팅 코어 할당량

CWA 설정 마법사와 VDS 포털은 새 가상 머신을 생성하고 Azure 구독에 사용 가능한 할당량이 있어야 성공적으로 실행할 수 있습니다.

할당량을 확인하려면 다음 단계를 수행하십시오**.**

1. 구독 모듈로 이동하여 “사용량 + 할당량”을 클릭합니다.
2. "공급자" 드롭다운에서 모든 공급자를 선택하고 "공급자" 드롭다운에서 "Microsoft.Compute 을 선택합니다
3. “Locations(위치)” 드롭다운에서 대상 지역을 선택합니다
4. 가상 시스템 제품군별로 사용 가능한 할당량 목록이 표시됩니다[]할당량을 늘려야 하는 경우 Request crease(증가 요청) 를 클릭하고 표시되는 메시지에 따라 용량을 추가합니다. 초기 배포의 경우 특히 "표준 DSv3 제품군 vCPU"에 대한 증가된 견적을 요청합니다.

검색 세부 정보를 수집합니다

CWA 설정 마법사를 통해 작업하면 몇 가지 질문에 답해야 합니다. NetApp VDS는 배포 전에 이러한 선택 사항을 기록하는 데 사용할 수 있는 링크된 PDF를 제공합니다. 항목 포함:

| 항목 | 설명 |
| --- | --- |
| VDS 관리자 자격 증명 | 기존 VDS 관리자 자격 증명이 이미 있는 경우 이를 수집합니다. 그렇지 않으면 배포 중에 새 관리자 계정이 생성됩니다. |
| Azure 지역 | 서비스의 성능 및 가용성을 기준으로 타겟 Azure Region을 결정합니다. 여기 "Microsoft 도구" 지역에 따라 최종 사용자 경험을 추정할 수 있습니다. |
| Active Directory 유형입니다 | VM은 도메인에 가입해야 하지만 Azure AD에 직접 연결할 수 없습니다. VDS 배포는 새 가상 컴퓨터를 구축하거나 기존 도메인 컨트롤러를 사용할 수 있습니다. |
| 파일 관리 | 성능은 특히 사용자 프로필 스토리지와 관련된 디스크 속도에 따라 크게 달라집니다. VDS 설정 마법사는 간단한 파일 서버를 배포하거나 ANF(Azure NetApp Files)를 구성할 수 있습니다. 거의 모든 운영 환경 ANF가 권장되지만 POC의 경우 파일 서버 옵션이 충분한 성능을 제공합니다. Azure에서 기존 스토리지 리소스 사용을 포함하여 배포 후 스토리지 옵션을 수정할 수 있습니다. 자세한 내용은 ANF 가격을 참조하십시오. https://azure.microsoft.com/en-us/pricing/details/netapp/ |
| 가상 네트워크 범위 | 배포에는 라우팅 가능/20개의 네트워크 범위가 필요합니다. VDS 설정 마법사를 사용하여 이 범위를 정의할 수 있습니다. 이 범위는 Azure 또는 사내(두 네트워크가 VPN 또는 ExpressRoute를 통해 연결된 경우)의 기존 vNets와 겹치지 않는 것이 중요합니다. |

**VDS** 설정 섹션

에 로그인합니다 https://cwasetup.cloudworkspace.com/ 필수 구성 요소 섹션에 있는 Azure 관리자 자격 증명을 사용합니다.

**IaaS** 및 플랫폼

[]

**Azure AD** 도메인 이름입니다

Azure AD 도메인 이름은 선택한 테넌트에 의해 상속됩니다.

위치

해당 **Azure Region** 을 선택합니다. 여기 "Microsoft 도구" 지역에 따라 최종 사용자 경험을 추정할 수 있습니다.

**Active Directory** 유형입니다

VDS는 기존 도메인 컨트롤러를 활용하기 위해 도메인 컨트롤러 기능 또는 설정을 위해  새 가상 시스템으로 프로비저닝할 수 있습니다. 이 가이드에서는 구독 아래에서 하나 또는 두 개의 VM(이 프로세스 중에 선택한 사항에 따라)을 생성하는 새 Windows Server Active Directory를 선택합니다.

기존 AD 배포에 대한 자세한 문서를 찾을 수 있습니다 "여기".

**Active Directory** 도메인 이름입니다

- 도메인 이름** 을 입력합니다. 위에서 Azure AD 도메인 이름을 미러링하는 것이 좋습니다.

파일 관리

VDS는 단순 파일 서버 가상 컴퓨터를 프로비저닝하거나 Azure NetApp Files를 설정 및 구성할 수 있습니다. 운영 환경에서 사용자당 30GB를 할당하는 것이 권장되며 최적의 성능을 위해서는 사용자당 5-15의 IOPS를 할당해야 합니다.

POC(비운영) 환경에서 파일 서버는 저렴한 비용으로 간편하게 구축할 수 있는 옵션이지만, Azure Managed Disks의 사용 가능한 성능은 소규모 운영 구축 환경의 IOPS 소비로 인해 압도될 수 있습니다.

예를 들어, Azure의 4TB 표준 SSD 디스크는 최대 500 IOPS를 지원하므로 사용자당 최대 100명의 총 사용자를 5 IOPS로 지원할 수 있습니다. ANF Premium을 사용할 경우 동일한 크기의 스토리지 설정이 16,000 IOPS를 지원하고 32x IOPS를 더 많이 지원합니다.

프로덕션 AVD 배포의 경우 **Azure NetApp Files**는 **Microsoft**의 권장 사항입니다.

배포하려는 구독에 Azure NetApp Files가 있어야 합니다. NetApp 계정 담당자에게 문의하거나 https://aka.ms/azurenetappfiles 링크를 사용하십시오

또한 NetApp을 구독 공급자로 등록해야 합니다. 이 작업은 다음을 수행하여 수행할 수 있습니다.

- Azure 포털에서 구독 으로 이동합니다
  - 리소스 공급자 를 클릭합니다
  - NetApp 필터링
  - 공급자를 선택하고 등록 을 클릭합니다

**RDS** 라이센스 번호입니다

NetApp VDS는 RDS 및/또는 AVD 환경을 배포하는 데 사용할 수 있습니다. AVD를 배포할 때 이 필드는 빈 상태로 유지됩니다**.

**ThinPrint**

NetApp VDS는 RDS 및/또는 AVD 환경을 배포하는 데 사용할 수 있습니다. AVD를 배포할 때 이 토글이  꺼짐(왼쪽 토글)으로 유지될 수 있습니다.

알림 이메일

VDS는 배포 알림 및 지속적인 상태 보고서를 제공된** 이메일로 전송합니다. 나중에 변경할 수 있습니다.

**VM** 및 네트워크

VDS 환경을 지원하기 위해 실행해야 하는 다양한 서비스가 있습니다. 이러한 서비스를 통칭하여 “VDS 플랫폼”이라고 합니다. 구성에 따라 CWMGR, 하나 또는 두 개의 RDS 게이트웨이, 하나 또는 두 개의 HTML5 게이트웨이, FTPS 서버 및 하나 또는 두 개의 Active Directory VM이 포함될 수 있습니다.

대부분의 AVD 구축 환경에서는 Microsoft가 AVD 게이트웨이를 PaaS 서비스로 관리하므로 단일 가상 머신 옵션을 활용합니다.

RDS 사용 사례가 포함될 작고 단순한 환경의 경우 이러한 모든 서비스를 단일 가상 시스템 옵션으로 압축하여 VM 비용(제한된 확장성)을 줄일 수 있습니다. 100명 이상의 사용자가 있는 RDS 사용 사례에서는 RDS 및/또는 HTML5 게이트웨이 확장성을 높이기 위해 다중 가상 시스템 옵션을 사용하는 것이 좋습니다[]

플랫폼 **VM** 구성

NetApp VDS는 RDS 및/또는 AVD 환경을 배포하는 데 사용할 수 있습니다. AVD를 구축할 때는 단일 가상 머신을 선택하는 것이 좋습니다. RDS 배포의 경우 Broker 및 게이트웨이와 같은 추가 구성 요소를 배포 및 관리해야 합니다. 프로덕션 환경에서는 이러한 서비스를 전용 가상 시스템에서 실행해야 합니다. AVD의 경우 이러한 모든 서비스는 Azure에서 포함된 서비스로 제공되므로 단일 가상 머신 구성을 사용하는 것이 좋습니다.

단일 가상 머신

이는 AVD(RDS 또는 두 가지 조합을 사용하는 것이 아님)만 사용하는 구축 환경에 권장되는 선택입니다. 단일 가상 시스템 배포에서 다음 역할은 모두 Azure의 단일 VM에서 호스팅됩니다.

- CW Manager(CW 관리자)
- HTML5 게이트웨이
- RDS 게이트웨이
- 원격 앱
- FTPS 서버(옵션)
- 도메인 컨트롤러 역할입니다

이 구성에서 RDS 사용 사례에 권장되는 최대 사용자 수는 100명입니다. 로드 밸런싱된 RDS/HTML5 게이트웨이는 이 구성에서 옵션이 아니며 향후 확장을 위한 중복성과 옵션을 제한합니다. Microsoft는 게이트웨이를 PaaS 서비스로 관리하기 때문에 이 제한은 AVD 배포에는 적용되지 않습니다.

이 환경이 멀티 테넌시를 위해 설계되는 경우 단일 가상 시스템 구성은 지원되지 않으며 AVD 또는 AD Connect도 지원되지 않습니다.

여러 개의 가상 머신

VDS 플랫폼을 여러 가상 시스템으로 분할할 때 Azure의 전용 VM에서 다음 역할이 호스팅됩니다.

- 원격 데스크탑 게이트웨이

  VDS 설정은 하나 또는 두 개의 RDS 게이트웨이를 배포하고 구성하는 데 사용할 수 있습니다. 이러한 게이트웨이는 열린 인터넷에서 구축 내의 세션 호스트 VM으로 RDS 사용자 세션을 중계합니다. RDS 게이트웨이는 중요한 기능을 처리하여 개방형 인터넷으로부터 직접 공격으로부터 RDS를 보호하고 환경 내/외부로 모든 RDS 트래픽을 암호화합니다. 두 개의 원격 데스크탑 게이트웨이를 선택하면 VDS Setup에서 두 개의 VM을 배포하고 들어오는 RDS 사용자 세션의 로드 밸런싱을 위해 구성합니다.

- HTML5 게이트웨이

  VDS Setup(VDS 설정)을 사용하여 하나 또는 두 개의 HTML5 게이트웨이를 배포 및 구성할 수 있습니다. 이러한 게이트웨이는 VDS 및 웹 기반 VDS 클라이언트(H5 Portal)의 _Connect to Server_feature에서 사용하는 HTML5 서비스를 호스팅합니다. HTML5 포털 2개를 선택한 경우 VDS Setup은 2개의 VM을 배포하고 들어오는 HTML5 사용자 세션의 로드 균형을 유지하도록 구성합니다.

  > ⓘ 다중 서버 옵션을 사용하는 경우(사용자가 설치된 VDS 클라이언트를 통해서만 연결할 수 있는 경우에도) VDS에서 _Connect to Server_functionality를 활성화하려면 하나 이상의 HTML5 게이트웨이를 사용하는 것이 좋습니다.

- 게이트웨이 확장성 참고 사항

  RDS 사용 사례의 경우, 각 RDS 또는 HTML5 게이트웨이에서 약 500명의 사용자를 지원하는 추가 게이트웨이 VM을 사용하여 환경의 최대 크기를 확장할 수 있습니다. 최소 NetApp 프로페셔널 서비스 지원을 통해 추가 게이트웨이를 추가할 수 있습니다

이 환경이 멀티 테넌시를 위해 설계된 경우에는 여러 가상 시스템을 선택해야 합니다.

시간대

최종 사용자의 환경은 현지 시간대를 반영하지만 기본 시간대를 선택해야 합니다. 환경의 기본 관리 중에서 시간대를 선택합니다.

가상 네트워크 범위

VM을 용도에 따라 다른 서브넷으로 분리하는 것이 가장 좋습니다. 먼저 네트워크 범위를 정의하고 A/20 범위를 추가합니다.

VDS Setup(VDS 설정)은 성공을 입증할 범위를 감지하고 제안합니다. 모범 사례에 따라 서브넷 IP 주소는 전용 IP 주소 범위에 속해야 합니다.

이러한 범위는 다음과 같습니다.

- 192.168.0.0 ~ 192.168.255.255
- 172.16.0.0 ~ 172.31.255.255
- 10.0.0.0 ~ 10.255.255.255

필요한 경우 검토 및 조정한 다음 유효성 검사 를 클릭하여 다음 각 서브넷에 대한 서브넷을 확인합니다.

- 테넌트: 세션 호스트 서버 및 데이터베이스 서버가 상주할 범위입니다
- 서비스: Azure NetApp Files와 같은 PaaS 서비스가 존재하는 범위입니다
- 플랫폼: 플랫폼 서버가 상주할 범위입니다
- 디렉터리: AD 서버가 상주할 범위입니다

검토

마지막 페이지에서는 선택 사항을 검토할 수 있는 기회를 제공합니다. 검토를 마치면 확인 버튼을 클릭합니다. VDS Setup(VDS 설정)은 모든 항목을 검토하고 배포가 제공된 정보로 진행될 수 있는지 확인합니다. 이 검증에는 2-10분이 소요될 수 있습니다. 진행 상황을 따라 로그 로고(오른쪽 위)를 클릭하여 검증 작업을 볼 수 있습니다.

검증이 완료되면 Validate 버튼 대신 녹색 Provision 버튼이 나타납니다. 구축을 위한 프로비저닝 프로세스를 시작하려면 프로비저닝 을 클릭합니다.

상태

프로비저닝 프로세스는 Azure 워크로드와 선택한 항목에 따라 2~4시간이 소요됩니다. 상태 페이지를 클릭하여 로그의 진행 상황을 따르거나 배포 프로세스가 완료되었음을 알려주는 이메일이 도착할 때까지 기다릴 수 있습니다. 배포는 VDS 및 원격 데스크톱 또는 AVD 구현을 모두 지원하는 데 필요한 가상 머신과 Azure 구성 요소를 구축합니다. 여기에는 원격 데스크톱 세션 호스트와 파일 서버 역할을 모두 수행할 수 있는 단일 가상 머신이 포함됩니다. AVD 구현에서 이 가상 시스템은 파일 서버로만 작동합니다.

#### **AD Connect**를 설치하고 구성합니다

설치가 성공적으로 완료된 직후 AD Connect를 도메인 컨트롤러에 설치 및 구성해야 합니다. 단일 플랫폼 VM 설정에서 CWMGR1 시스템은 DC입니다. AD의 사용자는 Azure AD와 로컬 도메인 간에 동기화해야 합니다.

**AD Connect**를 설치하고 구성하려면 다음 단계를 수행하십시오**.**

1. 도메인 관리자로 도메인 컨트롤러에 연결합니다.
   a. Azure Key Vault에서 자격 증명을 가져옵니다(참조) "주요 Vault 지침은 여기 를 참조하십시오")
2. AD Connect를 설치하고 도메인 관리자(엔터프라이즈 관리자 역할 권한 사용) 및 Azure AD Global Admin으로 로그인합니다

#### **AVD** 서비스를 활성화하는 중입니다

구축이 완료되면 다음 단계는 AVD 기능을 활성화하는 것입니다. AVD 활성화 프로세스를 수행하려면 Azure 관리자가 Azure AD 도메인을 등록하고 Azure AVD 서비스를 사용하여 액세스하기 위한 구독을 등록하는 몇 가지 단계를 수행해야 합니다. 마찬가지로 Microsoft는 VDS가 Azure의 자동화 애플리케이션에 대해 동일한 권한을 요청해야 합니다. 아래 단계를 통해 해당 프로세스를 단계별로 안내합니다.

#### **AVD** 호스트 풀을 생성합니다

AVD 가상 머신에 대한 최종 사용자 액세스는 가상 머신이 포함된 호스트 풀 및 사용자 액세스 유형과 사용자 액세스 유형이 포함된 애플리케이션 그룹에 의해 관리됩니다.

를 클릭하여 첫 번째 호스트 풀을 구성합니다

1. AVD 호스트 풀 섹션 헤더의 오른쪽에 있는 추가 버튼을 클릭합니다.[]
2. 호스트 풀의 이름과 설명을 입력합니다.

3. 호스트 풀 유형을 선택합니다
   a. 풀링된**: 여러 사용자가 동일한 애플리케이션이 설치된 동일한 가상 시스템 풀에 액세스합니다.
   b. **Personal**는 사용자가 자신의 세션 호스트 VM을 할당할 수 있는 호스트 풀을 생성합니다.
4. 로드 밸런서 유형을 선택합니다
   a. 깊이 우선: 풀의 두 번째 가상 머신에서 시작하기 전에 첫 번째 공유 가상 머신을 최대 사용자 수로 채웁니다
   b. **breadth first**: 라운드 로빈 방식으로 풀에 있는 모든 가상 머신에 사용자를 배포합니다
5. 이 풀에 가상 머신을 생성할 Azure 가상 머신 템플릿을 선택합니다. VDS는 구독에서 사용할 수 있는 모든 템플릿을 표시하지만 최상의 환경을 위해 최신 Windows 10 다중 사용자 빌드를 선택하는 것이 좋습니다. 현재 빌드는 Windows-10-20h1-EVD입니다. (필요에 따라 프로비저닝 수집 기능을 사용하여 골드 이미지를 생성하여 사용자 지정 가상 머신 이미지에서 호스트를 구축할 수 있습니다.)
6. Azure 시스템 크기를 선택합니다. 평가를 위해 D 시리즈(다중 사용자용 표준 장비 유형) 또는 E 시리즈(중부하 멀티 유저 시나리오를 위한 향상된 메모리 구성)를 권장합니다. 다른 시리즈 및 크기를 실험하려면 VDS에서 나중에 시스템 크기를 변경할 수 있습니다
7. 드롭다운 목록에서 가상 머신의 관리되는 디스크 인스턴스에 대해 호환되는 스토리지 유형을 선택합니다
8. 호스트 풀 생성 프로세스의 일부로 생성할 가상 머신의 수를 선택합니다. 나중에 풀에 가상 머신을 추가할 수 있지만 VDS는 요청한 가상 머신 수를 빌드하고 생성된 가상 머신을 호스트 풀에 추가합니다
9. 호스트 풀 추가 버튼을 클릭하여 생성 프로세스를 시작합니다. AVD 페이지에서 진행률을 추적하거나 작업 섹션의 배포/배포 이름 페이지에서 프로세스 로그의 세부 정보를 확인할 수 있습니다
10. 호스트 풀이 생성되면 AVD 페이지의 호스트 풀 목록에 표시됩니다. 호스트 풀의 이름을 클릭하면 해당 가상 머신, 앱 그룹 및 활성 사용자 목록이 포함된 세부 정보 페이지가 표시됩니다

> VDS의 Avd 호스트는 사용자 세션 연결을 허용하지 않는 설정으로 생성됩니다. 이는 사용자 연결을 수락하기 전에 사용자 지정을 허용하도록 설계되었습니다. 이 설정은 세션 호스트의 설정을 편집하여 변경할 수 있습니다. []

사용자에 대해 **VDS** 데스크톱을 활성화합니다

위에서 설명한 대로 VDS는 배포 중에 최종 사용자 작업 영역을 지원하는 데 필요한 모든 요소를 생성합니다. 구축이 완료되면 다음 단계는 AVD 환경에 도입할 각 사용자에 대해 작업 공간 액세스를 활성화하는 것입니다. 이 단계에서는 가상 데스크톱의 기본인 프로파일 구성과 최종 사용자 데이터 계층 액세스를 생성합니다. VDS는 이 구성을 재사용하여 Azure AD 최종 사용자를 AVD 앱 풀에 연결합니다.

최종 사용자의 작업 영역을 활성화하려면 다음 단계를 따르십시오**.**

1. 에서 VDS에 로그인합니다 https://manage.cloudworkspace.com 프로비저닝 중에 생성한 VDS 기본 관리자 계정을 사용합니다. 계정 정보가 기억나지 않는 경우 NetApp VDS에 문의하여 계정 정보를 검색할 수 있도록 도움을 받으십시오
2. 작업 영역 메뉴 항목을 클릭한 다음 프로비저닝 중에 자동으로 만들어진 작업 영역의 이름을 클릭합니다
3. 사용자 및 그룹 탭을 클릭합니다[]
4. 활성화할 각 사용자에 대해 사용자 이름을 스크롤한 다음 기어 아이콘을 클릭합니다
5. "클라우드 작업 공간 사용" 옵션을 선택합니다[]
6. 구현 프로세스가 완료되려면 30~90초 정도 걸립니다. 사용자 상태가 보류 중 에서 사용 가능 으로 변경됩니다

Azure AD 도메인 서비스를 활성화하면 Azure에서 관리되는 도메인이 생성되고 생성된 각 AVD 가상 머신이 해당 도메인에 연결됩니다. 가상 시스템에 대한 기존 로그인이 작동하려면 Azure AD 사용자의 암호 해시를 NTLM 및 Kerberos 인증을 지원하도록 동기화해야 합니다. 이 작업을 수행하는 가장 쉬운 방법은 Office.com 또는 Azure 포털에서 사용자 암호를 변경하는 것입니다. 이렇게 하면 암호 해시 동기화가 강제로 수행됩니다. 도메인 서비스 서버의 동기화 주기는 최대 20분 정도 걸릴 수 있습니다.

사용자 세션을 활성화합니다

기본적으로 세션 호스트는 사용자 연결을 수락할 수 없습니다. 이 설정은 새 사용자 세션을 방지하기 위해 프로덕션에서 사용할 수 있기 때문에 일반적으로 "드레인 모드"라고 하며, 이를 통해 호스트는 결국 모든 사용자 세션을 제거할 수 있습니다. 호스트에서 새 사용자 세션이 허용되는 경우 이 작업은 일반적으로 세션 호스트를 "순환"으로 배치하는 것을 말합니다.

운영 환경에서 새 호스트를 드레인 모드로 시작하는 것이 좋습니다. 일반적으로 호스트가 운영 워크로드에 대비하기 전에 완료해야 하는 구성 작업이 있기 때문입니다.

테스트 및 평가 시 즉시 호스트를 배수 모드에서 벗어나와 사용자가 연결하고 기능을 확인할 수 있습니다. . 세션 호스트에서 사용자 세션을 활성화하려면 다음 단계를 수행하십시오.

1. 작업 영역 페이지의 AVD 섹션으로 이동합니다.
2. “AVD 호스트 풀” 아래에서 호스트 풀 이름을 클릭합니다.[]
3. 세션 호스트의 이름을 클릭하고 "새 세션 허용" 확인란을 선택한 다음 "세션 호스트 업데이트"를 클릭합니다. 회전해야 하는 모든 호스트에 대해 반복합니다.[]
4. 각 호스트 라인 항목의 기본 AVD 페이지에도 "새 세션 허용"의 현재 통계가 표시됩니다.

기본 앱 그룹

데스크톱 응용 프로그램 그룹은 기본적으로 호스트 풀 생성 프로세스의 일부로 생성됩니다. 이 그룹은 모든 그룹 구성원에 대한 대화형 데스크톱 액세스를 제공합니다. 그룹에 구성원을 추가하려면 다음을 수행합니다.

1. 앱 그룹 이름을 클릭합니다[]
2. 추가된 사용자 수를 표시하는 링크를 클릭합니다[]
3. 앱 그룹 이름 옆에 있는 확인란을 선택하여 앱 그룹에 추가할 사용자를 선택합니다
4. 사용자 선택 버튼을 클릭합니다
5. 앱 그룹 업데이트 버튼을 클릭합니다

추가 **AVD** 앱 그룹 생성

호스트 풀에 추가 앱 그룹을 추가할 수 있습니다. 이러한 앱 그룹은 호스트 풀 가상 머신의 특정 애플리케이션을 RemoteApp를 사용하는 앱 그룹 사용자에게 게시합니다.

Avd는 최종 사용자가 데스크톱 앱 그룹 유형 또는 RemoteApp 앱 그룹 유형에만 할당할 수 있지만 동일한 호스트 풀에 둘 다 할당할 수는 없도록 하므로 사용자를 적절하게 격리해야 합니다. 사용자가 데스크톱 및 스트리밍 앱에 액세스해야 하는 경우 앱을 호스트하기 위해 두 번째 호스트 풀이 필요합니다.

새 앱 그룹을 만들려면:

1. 앱 그룹 섹션 헤더에서 추가 버튼을 클릭합니다[]
2. 앱 그룹의 이름과 설명을 입력합니다
3. 사용자 추가 링크를 클릭하여 그룹에 추가할 사용자를 선택합니다. 이름 옆의 확인란을 클릭하여 각 사용자를 선택한 다음 사용자 선택 단추를 클릭합니다[]
4. RemoteApps 추가 링크를 클릭하여 응용 프로그램을 이 앱 그룹에 추가합니다. Avd는 가상 머신에 설치된 애플리케이션 목록을 검색하여 가능한 애플리케이션 목록을 자동으로 생성합니다. 응용 프로그램 이름 옆의 확인란을 클릭하여 응용 프로그램을 선택한 다음 RemoteApps 선택 단추를 클릭합니다.[]
5. 앱 그룹 추가 버튼을 클릭하여 앱 그룹을 생성합니다

#### 최종 사용자 **AVD** 액세스

최종 사용자는 웹 클라이언트 또는 다양한 플랫폼에 설치된 클라이언트를 사용하여 AVD 환경에 액세스할 수 있습니다

- 웹 클라이언트: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web
- 웹 클라이언트 로그인 URL: http://aka.ms/AVDweb
- Windows 클라이언트: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10
- Android 클라이언트: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android
- macOS 클라이언트: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos
- iOS 클라이언트: https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios
- IGEL 씬 클라이언트: https://www.igel.com/igel-solution-family/windows-virtual-desktop/

최종 사용자 이름과 암호를 사용하여 로그인합니다. 원격 응용 프로그램 및 데스크톱 연결(RADC), 원격 데스크톱 연결(mstsc) 및 Windows 응용 프로그램용 CloudWorksapce 클라이언트는 현재 AVD 인스턴스에 로그인하는 기능을 지원하지 않습니다.

#### 사용자 로그인을 모니터링합니다

호스트 풀 세부 정보 페이지에는 AVD 세션에 로그인할 때 활성 사용자 목록도 표시됩니다.

#### 관리자 연결 옵션

VDS 관리자는 다양한 방식으로 환경에서 가상 컴퓨터에 연결할 수 있습니다.

### 서버에 연결합니다

포털 전체에서 VDS 관리자는 “서버에 연결” 옵션을 찾을 수 있습니다. 기본적으로 이 기능은 로컬 관리자 자격 증명을 동적으로 생성하여 웹 클라이언트 연결에 삽입하여 관리자를 가상 머신에 연결합니다. 관리자는 연결하기 위해 자격 증명을 알 필요가 없으며 이 자격 증명도 제공되지 않습니다.

이 기본 동작은 다음 섹션에 설명된 대로 관리자별로 비활성화할 수 있습니다.

### 기술/레벨 **3** 관리자 계정

CWA 설정 프로세스에서 "Level III" 관리자 계정이 생성되었습니다. 사용자 이름의 형식은 username.tech@domain.xyz 입니다

일반적으로 ".tech" 계정이라고 하는 이러한 계정은 도메인 수준 관리자 계정입니다. VDS 관리자는 CWMGR1(플랫폼)

서버에 연결할 때 그리고 선택적으로 환경의 다른 모든 가상 컴퓨터에 연결할 때 .tech 계정을 사용할 수 있습니다.

자동 로컬 관리자 로그인 기능을 비활성화하고 레벨 III 계정을 강제로 사용하려면 이 설정을 변경합니다. VDS > Admins > Admin Name(관리자 이름) > Check “Tech Account Enabled(기술 계정 활성화)”로 이동합니다. 이 상자를 선택하면 VDS 관리자가 로컬 관리자로 가상 시스템에 자동으로 로그인되지 않고 .tech 자격 증명을 입력하라는 메시지가 표시됩니다.

이러한 자격 증명 및 기타 관련 자격 증명은 _Azure Key Vault_에 자동으로 저장되며 Azure Management Portal()에서 액세스할 수 있습니다 https://portal.azure.com/.

배포 후 작업(선택 사항

멀티팩터 인증**(MFA)**

NetApp VDS에는 SMS/이메일 MFA가 무료로 포함되어 있습니다. 이 기능은 VDS Admin 계정 및/또는 최종 사용자 계정을 보호하는 데 사용할 수 있습니다."MFA 기사"

응용 프로그램 권한 워크플로

VDS는 응용 프로그램 카탈로그라고 하는 미리 정의된 응용 프로그램 목록에서 최종 사용자에게 응용 프로그램에 대한 액세스를 할당하는 메커니즘을 제공합니다. 애플리케이션 카탈로그는 관리되는 모든 구축에 걸쳐 제공됩니다.

> 자동으로 배포된 TSD1 서버는 응용 프로그램 권한을 지원하기 위해 그대로 유지되어야 합니다. 특히 이 가상 시스템에 대해 "데이터로 변환" 기능을 실행하지 마십시오.

애플리케이션 관리는 다음 문서에 자세히 설명되어 있습니다. ""

**Azure AD** 보안 그룹

VDS에는 Azure AD 보안 그룹이 백업한 사용자 그룹을 생성, 채우기 및 삭제하는 기능이 포함되어 있습니다. 이러한 그룹은 다른 보안 그룹과 마찬가지로 VDS 외부에서 사용할 수 있습니다. VDS에서 이러한 그룹을 사용하여 폴더 권한 및 응용 프로그램 권한을 할당할 수 있습니다.

사용자 그룹을 생성합니다

사용자 그룹 생성은 작업 영역 내의 사용자 및 그룹 탭에서 수행됩니다.

그룹별로 폴더 권한을 할당합니다

회사 공유의 폴더를 보고 편집할 수 있는 권한을 사용자 또는 그룹에 할당할 수 있습니다.

""

그룹별로 응용 프로그램을 할당합니다

응용 프로그램을 사용자에게 개별적으로 할당하는 것 외에도 응용 프로그램을 그룹에 프로비저닝할 수 있습니다.

1. 사용자 및 그룹 세부 정보로 이동합니다.[]
2. 새 그룹을 추가하거나 기존 그룹을 편집합니다.[]
3. 사용자 및 응용 프로그램을 그룹에 할당합니다.[]

## 비용 최적화 옵션을 구성합니다

작업 영역 관리는 AVD 구현을 지원하는 Azure 리소스 관리에도 확장됩니다. VDS를 사용하면 워크로드 스케줄과 라이브 확장을 모두 구성하여 최종 사용자 작업에 따라 Azure 가상 컴퓨터를 켜거나 끌 수 있습니다. 이러한 기능을 통해 Azure 리소스 활용률과 최종 사용자의 실제 사용 패턴에 따른 지출을 일치시킬 수 있습니다. 또한 개념 증명 AVD 구현을 구성한 경우 VDS 인터페이스에서 전체 배포를 전환할 수 있습니다.

### 워크로드 스케줄링

워크로드 스케줄링은 관리자가 최종 사용자 세션을 지원하기 위해 작업 공간 가상 머신에 대한 설정 스케줄을 생성할 수 있는 기능입니다. 특정 요일의 예약된 기간이 끝나면 VDS는 Azure에서 가상 컴퓨터를 중지/할당 해제하여 매시간 요금이 중지되도록 합니다.

워크로드 예약을 활성화하려면 다음을 수행합니다**.**

1. 에서 VDS에 로그인합니다 https://manage.cloudworkspace.com VDS 자격 증명을 사용합니다.
2. 작업 영역 메뉴 항목을 클릭한 다음 목록에서 작업 영역의 이름을 클릭합니다. []
3. Workload Schedule 탭을 클릭합니다. []
4. Workload Schedule 헤더에서 Manage 링크를 클릭합니다. []
5. 상태 드롭다운 메뉴에서 항상 켜짐(기본값), 항상 꺼짐 또는 예약됨의 기본 상태를 선택합니다.
6. 예약을 선택한 경우 예약 옵션에는 다음이 포함됩니다.
   a. 매일 할당된 간격으로 실행합니다. 이 옵션은 해당 주의 7일 모두에 대해 동일한 시작 시간 및 종료 시간으로 일정을 설정합니다. []
   b. 지정된 요일에 지정된 간격으로 실행합니다. 이 옵션은 선택한 요일에 대해서만 동일한 시작 타이 및 종료 시간으로 일정을 설정합니다. 선택하지 않은 요일 때문에 VDS가 해당 요일에 가상 컴퓨터를 켜지 않습니다. []
   c. 다양한 시간 간격과 요일로 실행합니다. 이 옵션은 선택한 각 날짜에 대해 다른 시작 시간 및 종료 시간으로 일정을 설정합니다. []
   d. 일정 설정이 완료되면 Update schedule(일정 업데이트) 단추를 클릭합니다. []

### 실시간 배율 조정

라이브 확장은 동시 사용자 로드에 따라 공유 호스트 풀의 가상 머신을 자동으로 켜고 끕니다. 각 서버가 가득 차면 호스트 풀 로드 밸런서가 사용자 세션 요청을 보낼 때 추가 서버가 준비되도록 켜집니다. 라이브 배율을 효과적으로 사용하려면 로드 밸런서 유형으로 "깊이 우선"을 선택합니다.

라이브 배율 활성화하기**:**

1. 에서 VDS에 로그인합니다 https://manage.cloudworkspace.com VDS 자격 증명을 사용합니다.
2. 작업 영역 메뉴 항목을 클릭한 다음 목록에서 작업 영역의 이름을 클릭합니다. []
3. Workload Schedule 탭을 클릭합니다. []
4. Live Scaling(라이브 배율) 섹션에서 Enabled(활성화) 라디오 단추를 클릭합니다. []
5. 서버당 최대 사용자 수를 클릭하고 최대 수를 입력합니다. 가상 머신 크기에 따라 이 수는 일반적으로 4에서 20 사이입니다. []
6. 선택 사항 – 추가 전원 켜짐 서버 사용 을 클릭하고 호스트 풀에 대해 설정할 추가 서버를 여러 대 입력합니다. 이 설정은 활성 충전 서버 외에 지정된 수의 서버를 활성화해 같은 시간 창에 로그인하는 대규모 사용자 그룹의 버퍼 역할을 합니다. []

현재 라이브 확장은 모든 공유 리소스 풀에 적용됩니다. 가까운 미래에 각 풀에는 독립적인 라이브 스케일링 옵션이 있습니다.

전체 배포의 전원을 끕니다

산발적이고 비생산적 기반으로만 평가 배포를 사용하려는 경우 사용하지 않을 때 구축 시 모든 가상 시스템을 끌 수 있습니다.

배포 기능을 설정하거나 해제하려면(즉, 구축 시 가상 시스템 끄기) 다음 단계를 따르십시오.

1. 에서 VDS에 로그인합니다 https://manage.cloudworkspace.com VDS 자격 증명을 사용합니다.
2. 배포 메뉴 항목을 클릭합니다. []커서를 대상 배치 줄 위로 이동하여 구성 기어 아이콘을 표시합니다. []
3. 기어를 클릭한 다음 중지를 선택합니다. []
4. 다시 시작하거나 시작하려면 1-3단계를 수행한 다음 시작 을 선택합니다. []

구축 환경의 모든 가상 머신을 중지하거나 시작하는 데 몇 분 정도 걸릴 수 있습니다.

**VM** 이미지 생성 및 관리

VDS에는 향후 배포를 위해 가상 컴퓨터 이미지를 만들고 관리하는 기능이 포함되어 있습니다. 이 기능에 도달하려면 VDS > 배포자 > 배포 이름 > 프로비저닝 컬렉션 으로 이동합니다. "VDI 이미지 수집" 기능은 여기에 설명되어 있습니다. ""

**Azure Cloud Backup Service**를 구성합니다

VDS는 가상 컴퓨터 백업을 위한 Azure PaaS 서비스인 Azure Cloud Backup을 기본적으로 구성 및 관리할 수 있습니다. 백업 정책은 유형 또는 호스트 풀별로 개별 시스템 또는 시스템 그룹에 할당할 수 있습니다. 자세한 내용은 여기에서 확인할 수 있습니다. ""

앱 관리/정책 모드를 선택합니다

기본적으로 VDS는 최종 사용자 작업 공간을 잠그는 여러 GPO(그룹 정책 개체)를 구현합니다. 이러한 정책은 핵심 데이터 계층 위치(예: c:\)에 대한 액세스와 최종 사용자로 응용 프로그램 설치를 수행하는 기능을 모두 차단합니다.

이 평가는 Window Virtual Desktop의 기능을 시연하기 위한 것이므로 GPO를 제거하여 물리적 작업 영역과 동일한 기능과 액세스를 제공하는 "기본 작업 영역"을 구현할 수 있습니다. 이렇게 하려면 “기본 작업 영역” 옵션의 단계를 따릅니다.

또한 전체 가상 데스크톱 관리 기능 집합을 활용하여 "제어된 작업 공간"을 구현할 수도 있습니다. 이러한 단계에는 최종 사용자 응용 프로그램 사용 권한에 대한 응용 프로그램 카탈로그를 생성 및 관리하고 관리자 수준 권한을 사용하여 응용 프로그램과 데이터 폴더에 대한 액세스를 관리하는 것이 포함됩니다. "제어된 작업 공간" 섹션의 단계에 따라 AVD 호스트 풀에 이 유형의 작업 공간을 구현합니다.

제어된 **AVD** 작업 공간(기본 정책)

VDS 배포의 기본 모드는 제어된 작업 공간을 사용하는 것입니다. 정책이 자동으로 적용됩니다. 이 모드를 사용하려면 VDS 관리자가 응용 프로그램을 설치해야 하며 최종 사용자는 세션 바탕 화면의 바로 가기를 통해 응용 프로그램에 액세스할 수 있습니다. 이와 유사하게 매핑된 공유 폴더를 생성하고 표준 부팅 및/또는 데이터 드라이브 대신 매핑된 드라이브 문자만 볼 수 있는 권한을 설정하여 데이터 폴더에 대한 액세스가 최종 사용자에게 할당됩니다. 이 환경을 관리하려면 아래 단계에 따라 응용 프로그램을 설치하고 최종 사용자 액세스를 제공합니다.

### 기본 **AVD** 작업 공간으로 돌아갑니다

기본 작업 영역을 만들려면 기본적으로 만들어지는 기본 GPO 정책을 비활성화해야 합니다.

이 작업을 수행하려면 다음 일회성 프로세스를 따르십시오**.**

1. 에서 VDS에 로그인합니다 https://manage.cloudworkspace.com 기본 관리자 자격 증명을 사용합니다.
2. 왼쪽에서 배포 메뉴 항목을 클릭합니다. []
3. 배포 이름을 클릭합니다. []
4. Platform Servers(플랫폼 서버) 섹션(오른쪽 중간 페이지)에서 기어가 나타날 때까지 CWMGR1의 줄 오른쪽으로 스크롤합니다. []
5. 기어를 클릭하고 연결 을 선택합니다. []
6. 프로비저닝 중에 생성한 "Tech" 자격 증명을 입력하여 HTML5 액세스를 사용하여 CWMGR1 서버에 로그온합니다. []
7. 시작(Windows) 메뉴를 클릭하고 Windows 관리 도구 를 선택합니다. []
8. 그룹 정책 관리 아이콘을 클릭합니다. []
9. 왼쪽 창의 목록에서 AADDC Users 항목을 클릭합니다. []
10. 오른쪽 창의 목록에서 “Cloud Workspace Users(클라우드 작업 영역 사용자)” 정책을 마우스 오른쪽 단추로 클릭한 다음 “Link Enabled(링크 사용)” 옵션의 선택을 취소합니다. 확인 을 클릭하여 이 작업을 확인합니다. [] []
11. 메뉴에서 작업, 그룹 정책 업데이트 를 선택한 다음 해당 컴퓨터에 정책 업데이트를 적용할지 확인합니다. []
12. 9단계와 10단계를 반복하되 "AADDC 사용자" 및 "클라우드 작업 영역 회사"를 선택하여 링크를 비활성화합니다. 이 단계를 수행한 후에는 그룹 정책을 강제로 업데이트할 필요가 없습니다. [] []
13. 그룹 정책 관리 편집기 및 관리 도구 창을 닫고 로그오프합니다. []이 단계에서는 최종 사용자를 위한 기본적인 작업 공간 환경을 제공합니다. 확인하려면 최종 사용자 계정 중 하나로 로그인합니다. 세션 환경에는 숨겨진 시작 메뉴, C:\ 드라이브에 대한 잠긴 액세스, 숨겨진 제어판 등의 제어된 작업 공간 제한 사항이 없어야 합니다.

> ⓘ 배포 중에 생성된 .tech 계정은 VDS와 관계없이 응용 프로그램을 설치하고 폴더의 보안을 변경할 수 있는 모든 권한을 가집니다. 그러나 Azure AD 도메인의 최종 사용자가 비슷한 전체 액세스 권한을 가지도록 하려면 각 가상 시스템의 로컬 관리자 그룹에 추가해야 합니다.

### **Avd** 배포 가이드 **-** 기존 **AD** 보완

#### 개요

VDS Setup(VDS 설정)은 새 배포를 기존 AD 구조에 연결할 수 있습니다. 이 지침은 해당 옵션에 대해 자세히 설명합니다. 이 문서는 독립 실행형 문서가 아니라 에서 다룬 새 AD 옵션 대신 사용할 수 있는 자세한 설명입니다 "Avd 배포 가이드"

#### **Active Directory** 유형입니다

다음 섹션에서는 VDS 배포에 대한 Active Directory 배포 유형을 정의합니다. 이 가이드에서는 이미 존재하는 AD 구조를 활용하는 기존 Windows Server Active Directory를 선택합니다.

#### 기존 **AD** 네트워크

VDS 설정은 기존 AD 구조와 Azure AD 간의 연결을 나타낼 수 있는 vNets 목록을 표시합니다. 선택한 VNET에는 Azure에서 구성한 Azure 호스팅 DC가 있어야 합니다. 또한 VNET에는 Azure 호스팅 DC를 가리키는 사용자 지정

DNS 설정이 있습니다.

[]

#### 기존 **Active Directory** 도메인 이름입니다

사용할 기존 도메인 이름을 입력합니다. 참고: Active Directory 모듈의 Azure Portal에 있는 도메인은 DNS 문제를 일으킬 수 있으므로 사용하지 마십시오. 이 방법의 주요 예는 사용자가 데스크톱 내에서 해당 웹 사이트(<yourdomain>.com)에 액세스할 수 없다는 것입니다.

#### 기존 **AD** 사용자 이름 및 암호

기존 AD 구조를 사용하여 배포를 촉진하는 데 필요한 자격 증명을 제공하는 방법에는 세 가지가 있습니다.

1. Active Directory 도메인 관리자 사용자 이름 및 암호를 제공합니다

   이 방법은 배포를 용이하게 하는 데 사용되는 도메인 관리자 자격 증명을 제공하는 가장 쉬운 방법입니다.

   > ⓘ 이 계정은 일회성 목적으로 만들 수 있으며 배포 프로세스가 완료되면 삭제할 수 있습니다.

2. 계정 일치 필수 권한을 생성합니다

   이 방법은 고객 관리자가 여기에서 권한 구조를 수동으로 생성한 후 여기에 CloudWorkspaceSVC 계정에 대한 자격 증명을 입력하고 계속 진행하는 것입니다.

3. 수동 배포 프로세스

   최소 권한 계정 보안 주체를 사용하여 AD 액세스를 구성하는 데 도움이 필요하면 NetApp VDS 지원에 문의하십시오.

#### 다음 단계

이 문서에서는 기존 AD 환경에 배포할 수 있는 고유한 단계를 설명합니다. 이 단계가 완료되면 표준 배포 가이드로 돌아갈 수 있습니다 "여기".

### **VDS** 구성 요소 및 권한

#### **Avd** 및 **VDS** 보안 엔터티 및 서비스

Azure Virtual Desktop(AVD)은 자동 작업을 수행하려면 Azure AD 및 로컬 Active Directory의 보안 계정 및 구성 요소가 필요합니다. NetApp의 VDS(Virtual Desktop Service)는 구축 프로세스 중에 관리자가 AVD 환경을 제어할 수 있도록 구성 요소 및 보안 설정을 생성합니다. 이 문서에서는 두 환경 모두에서 관련된 VDS 계정, 구성 요소 및 보안 설정을 설명합니다.

배포 자동화 프로세스의 구성 요소 및 권한은 주로 최종 배포 환경의 구성 요소와 다릅니다. 따라서 이 문서는 배포 자동화 섹션과 배포된 환경 섹션의 두 가지 주요 섹션으로 구성됩니다.

[너비 = 75%]

#### **Avd** 배포 자동화 구성 요소 및 권한

VDS 배포는 여러 Azure 및 NetApp 구성 요소와 보안 권한을 활용하여 배포 및 작업 공간을 모두 구현합니다.

엔터프라이즈 애플리케이션

VDS는 테넌트의 Azure AD 도메인에서 엔터프라이즈 응용 프로그램 및 응용 프로그램 등록을 활용합니다. 엔터프라이즈 응용 프로그램은 Azure Resource Manager, Azure Graph 및 (AVD Fall Release를 사용하는 경우) AVD API 끝점에 대한 호출을 위한 전달자입니다. 이 끝점은 연결된 서비스 대표자에게 부여된 위임 역할 및 권한을 사용하여 Azure AD 인스턴스 보안 컨텍스트의 AVD API 끝점입니다. 앱 등록은 VDS를 통해 테넌트에 대한 AVD 서비스의 초기화 상태에 따라 생성될 수 있습니다.

이러한 VM을 생성 및 관리하기 위해 VDS는 Azure Subscription에 다음과 같은 몇 가지 지원 구성 요소를 생성합니다.

클라우드 작업 공간

이것은 초기 엔터프라이즈 응용 프로그램 관리자가 VDS 설치 마법사의 배포 프로세스 중에 동의하며 사용됩니다.

Cloud Workspace Enterprise Application은 VDS 설정 프로세스 중에 특정 권한 집합을 요청합니다. 이러한 권한은 다음과 같습니다.

- 로그인한 사용자로 디렉터리에 액세스(위임됨)
- 디렉토리 데이터 읽기 및 쓰기(위임됨)
- 로그인 및 사용자 프로필 읽기(위임됨)
- 로그인(위임됨)
- 사용자의 기본 프로필 보기(위임됨)
- 조직 사용자로 Azure Service Management 액세스(위임됨)

**Cloud Workspace API**를 참조하십시오

Azure PaaS 기능에 대한 일반 관리 통화를 처리합니다. Azure PaaS 기능의 예로는 Azure Compute, Azure Backup, Azure Files 등이 있습니다. 이 서비스 담당자는 초기 배포 중에 대상 Azure 구독에 대한 소유자 권한과 지속적인 관리를 위한 참가자 권한이 필요합니다(참고: Azure Files를 사용하려면 Azure File 객체에 대한 사용자별 권한을 설정하려면 가입 소유자 권한이 필요합니다.

Cloud Workspace API Enterprise Application은 VDS 설정 프로세스 중에 특정 권한 집합을 요청합니다. 이러한 권한은 다음과 같습니다.

- 구독자(또는 Azure 파일이 사용되는 경우 구독 소유자)
- Azure AD 그래프
  - 모든 응용 프로그램 읽기 및 쓰기(응용 프로그램)
  - 이 앱이 만들거나 소유하는 앱 관리(응용 프로그램)
  - 디바이스 읽기 및 쓰기(애플리케이션)
  - 로그인한 사용자로 디렉터리에 액세스(위임됨)
  - 디렉토리 데이터 읽기(애플리케이션)
  - 디렉토리 데이터 읽기(위임됨)
  - 디렉토리 데이터 읽기 및 쓰기(애플리케이션)

    - 디렉토리 데이터 읽기 및 쓰기(위임됨)
    - 도메인 읽기 및 쓰기(응용 프로그램)
    - 모든 그룹 읽기(위임됨)
    - 모든 그룹 읽기 및 쓰기(위임됨)
    - 모든 숨겨진 멤버십 읽기(응용 프로그램)
    - 숨겨진 구성원 읽기(위임됨)
    - 로그인 및 사용자 프로필 읽기(위임됨)
    - 모든 사용자의 전체 프로필 읽기(위임됨)
    - 모든 사용자의 기본 프로필 읽기(위임됨)
- Azure 서비스 관리
    - 조직 사용자로 Azure Service Management 액세스(위임됨)

**NetApp VDS**

NetApp VDS 구성 요소는 VDS 컨트롤 플레인을 통해 AVD 역할, 서비스 및 리소스의 배포 및 구성을 자동화하는 데 사용됩니다.

사용자 지정 역할

Automation Contributor 역할은 최소한의 권한을 가진 방법을 통해 배포를 용이하게 하기 위해 생성됩니다. CWMGR1 VM은 이 역할을 통해 Azure 자동화 계정에 액세스할 수 있습니다.

자동화 계정

자동화 계정은 구축 중에 생성되며 프로비저닝 프로세스 중에 필요한 구성 요소입니다. 자동화 계정에는 변수, 자격 증명, 모듈 및 원하는 상태 설정이 포함되어 있으며 키 볼트를 참조합니다.

원하는 상태 구성

CWMGR1의 구성을 빌드하는 데 사용되는 방법입니다. 구성 파일은 VM에 다운로드되고 VM의 로컬 구성 관리자를 통해 적용됩니다. 구성 요소의 예는 다음과 같습니다.

- Windows 기능 설치
- 소프트웨어 설치 중
- 소프트웨어 구성을 적용하는 중입니다
- 적절한 권한 집합이 적용되었는지 확인합니다
- Let’s Encrypt 인증서 적용
- DNS 레코드가 올바른지 확인합니다
- CWMGR1이 도메인에 가입되어 있는지 확인합니다

모듈**:**

- ActiveDirectoryDsc: Active Directory의 배포 및 구성을 위한 원하는 상태 구성 리소스입니다. 이러한 리소스를 사용하여 새 도메인, 자식 도메인 및 고가용성 도메인 컨트롤러를 구성하고 도메인 간 트러스트를 설정하고 사용자,

그룹 및 OU를 관리할 수 있습니다.

- AZ.Accounts: Azure 모듈의 자격 증명 및 공통 구성 요소를 관리하는 데 사용되는 Microsoft 제공 모듈입니다
- AZ.Automation: Azure Automation commandlet을 위한 Microsoft 제공 모듈입니다
- Az.Compute:A Azure Compute commandlet용 Microsoft 제공 모듈입니다
- AZ.KeyVault: Azure Key Vault commandlet용 Microsoft 제공 모듈입니다
- AZ.Resources: Azure Resource Manager commandlet을 위한 Microsoft 제공 모듈입니다
- cChoco: Chocolatey를 사용하여 패키지를 다운로드하고 설치하기 위한 원하는 상태 구성 리소스입니다
- cjAz: NetApp이 작성한 이 모듈은 Azure 자동화 모듈에 자동화 도구를 제공합니다
- cjAzACS: NetApp이 만든 이 모듈에는 사용자 환경 자동화 기능과 PowerShell 프로세스가 포함되어 있으며, 사용자가 작성한 컨텍스트 내에서 실행됩니다.
- cjAzBuild: NetApp이 만든 이 모듈에는 시스템 컨텍스트에서 실행되는 빌드 및 유지 관리 자동화 및 PowerShell 프로세스가 포함되어 있습니다.
- cNtfsAccessControl: NTFS 액세스 제어 관리에 필요한 상태 구성 리소스입니다
- ComputerManagementDsc: 가상 메모리, 이벤트 로그, 시간대 및 전원 설정과 같은 항목을 구성할 뿐만 아니라 도메인 가입 및 일정 작업 등의 컴퓨터 관리 작업을 허용하는 원하는 상태 구성 리소스입니다.
- cUserRightsAssignment: 로그온 권한 및 권한과 같은 사용자 권한을 관리할 수 있는 원하는 상태 구성 리소스입니다
- NetworkingDsc: 네트워킹에 필요한 상태 구성 리소스입니다
- xCertificate: Windows Server에서 인증서 관리를 간소화하기 위해 필요한 상태 구성 리소스입니다.
- xDnsServer: Windows Server DNS 서버의 구성 및 관리에 필요한 상태 구성 리소스입니다
- xNetworking: 네트워킹과 관련하여 원하는 상태 구성 리소스입니다.
- "xRemoteDesktopAdmin": 이 모듈은 로컬 또는 원격 컴퓨터에서 원격 데스크톱 설정 및 Windows 방화벽을 구성하기 위해 원하는 상태 구성 리소스가 포함된 리포지토리를 사용합니다.
- xRemoteDesktopSessionHost: 원격 데스크톱 세션 호스트(RDSH) 인스턴스의 생성 및 구성을 지원하는 원하는 상태 구성 리소스(xRDSessionDeployment, xRDSessionCollection, xRDSessionCollectionConfiguration 및 xRDRemoteApp
- xSmbShare: SMB 공유를 구성 및 관리하기 위한 원하는 상태 구성 리소스입니다
- xSystemSecurity: UAC 및 IE Esc를 관리하기 위해 필요한 상태 구성 리소스

> ⓘ 또한 Azure Virtual Desktop은 엔터프라이즈 애플리케이션 및 Azure Virtual Desktop 및 Azure Virtual Desktop Client에 대한 앱 등록, AVD 테넌트, AVD 호스트 풀, AVD 앱 그룹 및 AVD 등록 가상 머신을 비롯한 Azure 구성 요소도 설치합니다. VDS Automation 구성 요소가 이러한 구성 요소를 관리하는 동안 AVD는 기본 구성 및 속성 집합을 제어하므로 자세한 내용은 AVD 설명서를 참조하십시오.

하이브리드 **AD** 구성 요소

사내 또는 퍼블릭 클라우드에서 실행되는 기존 AD와 원활하게 통합하려면 기존 AD 환경에 추가 구성 요소 및 권한이 필요합니다.

도메인 컨트롤러

기존 도메인 컨트롤러는 AD Connect 및/또는 사이트 간 VPN(또는 Azure ExpressRoute)을 통해 AVD 배포에 통합될 수 있습니다.

**AD** 연결

AVD PaaS 서비스를 통해 성공적인 사용자 인증을 지원하기 위해 AD 연결을 사용하여 Azure AD와 도메인 컨트롤러를 동기화할 수 있습니다.

보안 그룹

VDS는 CW-Infrastructure라는 Active Directory 보안 그룹을 사용하여 도메인 연결 및 GPO 정책 첨부 등의 Active Directory 종속 작업을 자동화하는 데 필요한 권한을 포함합니다.

서비스 계정

VDS는 VDS Windows 서비스 및 IIS 응용 프로그램 서비스의 ID로 사용되는 CloudworkspaceSVC라는 Active Directory 서비스 계정을 사용합니다. 이 계정은 비대화형 계정이며(RDP 로그인을 허용하지 않음) CW-Infrastructure 계정의 기본 구성원입니다

**VPN** 또는 **ExpressRoute**를 선택합니다

사이트 간 VPN 또는 Azure ExpressRoute를 사용하여 Azure VM을 기존 도메인에 직접 연결할 수 있습니다. 이 구성은 프로젝트 요구 사항에 따라 필요할 때 사용할 수 있는 선택적 구성입니다.

로컬 **AD** 권한 위임

NetApp은 하이브리드 AD 프로세스를 간소화할 수 있는 옵션 툴을 제공합니다. NetApp의 선택적 툴을 사용하는 경우 다음을 수행해야 합니다.

- 워크스테이션 OS가 아닌 서버 OS에서 실행합니다
- 도메인에 가입되거나 도메인 컨트롤러인 서버에서 실행합니다
- 툴을 실행하는 서버(도메인 컨트롤러에서 실행되지 않는 경우)와 도메인 컨트롤러 모두에 PowerShell 5.0 이상이 설치되어 있어야 합니다
- 도메인 관리자 권한이 있는 사용자가 실행하거나 로컬 관리자 권한이 있고 도메인 관리자 자격 증명을 제공할 수 있는 사용자(RunAs와 함께 사용)가 실행해야 합니다.

수동으로 생성하든 NetApp 툴로 적용하든 필요한 사용 권한은 다음과 같습니다.

- CW - 인프라 그룹
  - Cloud Workspace Infrastructure(* CW-Infrastructure*) 보안 그룹에는 Cloud Workspace OU 수준 및 모든 하위 개체에 대한 모든 권한이 부여됩니다
  - 배포 코드>.cloudworkspace.app DNS Zone – CW-Infrastructure 그룹에 CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree가 부여되었습니다. ExtendedRight, Delete, GenericWrite 가 있습니다
  - DNS 서버 – CW 인프라 그룹에 ReadProperty, GenericExecute 권한이 부여되었습니다
  - 생성된 VM(CWMGR1, AVD 세션 VM)에 대한 로컬 관리자 액세스(관리되는 AVD 시스템의 그룹 정책에 의해 수행)

- CW-CWMGRAccess 그룹 이 그룹은 모든 템플릿, 단일 서버, 새로운 기본 Active Directory 템플릿에 대해 CWMGR1에 대한 로컬 관리 권한을 제공합니다. 기본 제공 그룹 서버 운영자 원격 데스크톱 사용자 및 네트워크 구성 운영자를 활용합니다.

#### Avd 환경 구성 요소 및 권한

배포 자동화 프로세스가 완료되면 배포 및 작업 영역의 지속적인 사용 및 관리가 아래에 정의된 대로 별도의 구성 요소와 사용 권한이 필요합니다. 위의 구성 요소와 사용 권한 중 다수는 여전히 관련이 있지만 이 섹션은 배포된 의 구조를 정의하는 데 중점을 둡니다.

VDS 배포 및 작업 공간의 구성 요소는 다음과 같은 여러 논리 범주로 구성할 수 있습니다.

- 최종 사용자 클라이언트
- VDS 컨트롤 플레인 구성 요소
- Microsoft Azure AVD-PaaS 구성 요소
- VDS 플랫폼 구성 요소
- Azure 테넌트의 VDS 작업 영역 구성 요소입니다
- 하이브리드 AD 구성 요소

#### 최종 사용자 클라이언트

사용자는 AVD 데스크톱 및/또는 다양한 엔드포인트 유형에 연결할 수 있습니다. Microsoft는 Windows, macOS, Android 및 iOS용 클라이언트 응용 프로그램을 게시했습니다. 또한 웹 클라이언트를 클라이언트 없이 액세스할 수 있습니다.

AVD에 대한 엔드포인트 클라이언트를 게시한 Linux 씬 클라이언트 공급업체도 있습니다. 이러한 항목은 에 나와 있습니다 https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

#### VDS 컨트롤 플레인 구성 요소

#### VDS REST API

VDS는 완전 문서화된 REST API를 기반으로 구축되므로 웹 앱에서 사용할 수 있는 모든 작업은 API를 통해서도 사용할 수 있습니다. API 설명서는 다음과 같습니다. https://api.cloudworkspace.com/5.4/swagger/ui/index#

#### VDS 웹 앱입니다

VDS 관리자는 VDS 웹 앱을 통해 ADS 응용 프로그램을 상호 작용할 수 있습니다. 이 웹 포털은 다음과 같습니다. https://manage.cloudworkspace.com

#### 컨트롤 플레인 데이터베이스

VDS 데이터 및 설정은 NetApp에서 호스팅 및 관리하는 제어 플레인 SQL 데이터베이스에 저장됩니다.

#### VDS 통신

#### Azure 테넌트 구성 요소입니다

VDS 배포 자동화는 VM, 네트워크 서브넷, 네트워크 보안 그룹 및 Azure 파일 컨테이너 또는 Azure NetApp Files 용량

풀을 비롯한 다른 AVD 구성 요소를 포함하는 단일 Azure 리소스 그룹을 생성합니다. 참고 – 기본값은 단일 리소스 그룹이지만 필요한 경우 VDS에는 추가 리소스 그룹에 리소스를 생성할 수 있는 도구가 있습니다.

**Microsoft Azure AVD-PaaS** 구성 요소

**Avd REST API**

Microsoft AVD는 API를 통해 관리할 수 있습니다. VDS는 이러한 API를 광범위하게 활용하여 AVD 환경을 자동화하고 관리합니다. 문서 위치: https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/

세션 브로커

브로커는 사용자에 대해 승인된 리소스를 확인하고 사용자와 게이트웨이 간의 연결을 조정합니다.

**Azure** 진단

Azure 진단은 AVD 구축을 지원하도록 특별히 제작되었습니다.

**Avd** 웹 클라이언트

Microsoft는 사용자가 로컬에 설치된 클라이언트 없이 AVD 리소스에 연결할 수 있는 웹 클라이언트를 제공합니다.

세션 게이트웨이

로컬로 설치된 RD 클라이언트는 게이트웨이에 연결하여 AVD 환경과 안전하게 통신합니다.

**VDS** 플랫폼 구성 요소

**CWMGR1**

CMWGR1은 각 배포에 대한 VDS 제어 VM입니다. 기본적으로 이 VM은 대상 Azure 구독에서 Windows 2019 Server VM으로 생성됩니다. CWMGR1에 설치된 VDS 및 타사 구성 요소 목록은 로컬 배포 섹션을 참조하십시오.

AVD VM을 Active Directory 도메인에 연결해야 합니다. 이 프로세스를 용이하게 하고 VDS 환경 관리를 위한 자동화 도구를 제공하기 위해 위에서 설명한 CWMGR1 VM에 여러 구성 요소가 설치되며 AD 인스턴스에 여러 구성 요소가 추가됩니다. 구성 요소는 다음과 같습니다.

- * Windows 서비스 * - VDS는 Windows 서비스를 사용하여 배포 내에서 자동화 및 관리 작업을 수행합니다.
  - * CW Automation Service * 는 각 AVD 구축 시 CWMGR1에 배포된 Windows 서비스로서, 해당 환경에서 사용자 대면 자동화 작업을 많이 수행합니다. 이 서비스는 * CloudWorkspaceSVC * AD 계정으로 실행됩니다.
  - * CW VM Automation Service * 는 가상 머신 관리 기능을 수행하는 각 AVD 구축 시 CWMGR1에 구축된 Windows 서비스입니다. 이 서비스는 * CloudWorkspaceSVC * AD 계정으로 실행됩니다.
  - * CW 에이전트 서비스 * 는 CWMGR1을 포함하여 VDS 관리 하에 각 가상 머신에 배포된 Windows 서비스입니다. 이 서비스는 가상 시스템의 * LocalSystem * 컨텍스트에서 실행됩니다.
  - * CWManagerX API * 는 각 AVD 배포의 CWMGR1에 설치된 IIS 앱 풀 기반 수신기입니다. 이는 글로벌 컨트롤 플레인에서 들어오는 인바운드 요청을 처리하며 * CloudWorkspaceSVC * AD 계정으로 실행됩니다.
- * SQL Server 2017 Express * – VDS는 CWMGR1 VM에 SQL Server Express 인스턴스를 만들어 자동화 구성 요소에서 생성된 메타데이터를 관리합니다.
- * IIS(인터넷 정보 서비스) * – CWMGR1에서 IIS를 활성화하여 CWManagerX 및 CWApps IIS 응용 프로그램을

호스팅합니다(RDS RemoteApp 기능이 활성화된 경우에만). VDS를 사용하려면 IIS 버전 7.5 이상이 필요합니다.

- * HTML5 포털(옵션) * – VDS는 Spark Gateway 서비스를 설치하여 배포 및 VDS 웹 응용 프로그램에서 VM에 HTML5 액세스를 제공합니다. 이 응용 프로그램은 Java 기반 응용 프로그램이며 이 액세스 방법을 원하지 않는 경우 비활성화 및 제거할 수 있습니다.
- * RD 게이트웨이(옵션) * – VDS는 CWMGR1에서 RD 게이트웨이 역할을 활성화하여 RDS 수집 기반 리소스 풀에 대한 RDP 액세스를 제공합니다. 이 역할은 AVD 역방향 연결 액세스만 원하는 경우 비활성화/제거할 수 있습니다.
- * RD 웹(옵션) * – VDS는 RD 웹 역할을 활성화하고 CWApps IIS 웹 응용 프로그램을 만듭니다. AVD 액세스만 원하는 경우 이 역할을 비활성화할 수 있습니다.
- * DC 구성 * – 배포 및 VDS 사이트별 구성 및 고급 구성 작업을 수행하는 데 사용되는 Windows 응용 프로그램입니다.
- * 테스트 VDC 도구 * – 가상 머신 및 클라이언트 레벨 구성 변경에 대한 직접 작업 실행을 지원하는 Windows 애플리케이션으로, 문제 해결을 위해 API 또는 웹 애플리케이션 작업을 수정해야 하는 드문 경우에 사용됩니다.
- * Let's Encrypt 와일드카드 인증서(선택 사항) * – VDS에서 생성 및 관리 – TLS를 통한 HTTPS 트래픽이 필요한 모든 VM은 야간에 인증서로 업데이트됩니다. 또한 갱신은 자동화된 작업으로 처리됩니다(인증서는 90일이므로 갱신은 바로 전에 시작됩니다). 고객은 원하는 경우 자신만의 와일드카드 인증서를 제공할 수 있습니다. VDS는 또한 자동화 작업을 지원하기 위해 여러 Active Directory 구성 요소가 필요합니다. 이 설계 의도는 자동화된 관리를 위한 환경을 지원하는 동시에 최소한의 AD 구성 요소 및 권한 추가를 활용하는 것입니다. 이러한 구성 요소는 다음과 같습니다.
- * Cloud Workspace OU(Organizational Unit) * – 이 조직 단위는 필수 하위 구성 요소에 대한 기본 AD 컨테이너 역할을 합니다. CW-Infrastructure 및 Client DHP Access 그룹에 대한 사용 권한은 이 수준과 하위 구성 요소에서 설정됩니다. 이 OU에 만든 하위 OU에 대해서는 부록 A를 참조하십시오.
- * Cloud Workspace Infrastructure Group(CW-Infrastructure) * 은 VDS 서비스 계정(* CloudWorkspaceSVC *)에 필요한 위임된 권한을 할당할 수 있도록 로컬 AD에서 생성된 보안 그룹입니다.
- * 클라이언트 DHP 액세스 그룹(ClientDHPAccess) * 은 VDS가 회사 공유, 사용자 홈 및 프로필 데이터가 상주하는 위치를 제어할 수 있도록 로컬 AD에 생성된 보안 그룹입니다.
- * CloudWorkspaceSVC * 서비스 계정(Cloud Workspace Infrastructure Group 회원)
- * 배포 코드>.cloudworkspace.app domain * 용 DNS 존(이 도메인은 세션 호스트 VM의 자동 생성된 DNS 이름을 관리함) – 배포 구성을 통해 생성됩니다.
- * Cloud Workspace 조직 단위의 다양한 하위 OU에 연결된 NetApp 고유 GPO *. 이러한 GPO는 다음과 같습니다.
  - * Cloud Workspace GPO(Cloud Workspace OU에 연결) * – CW-Infrastructure 그룹의 구성원에 대한 액세스 프로토콜과 메서드를 정의합니다. 또한 AVD 세션 호스트의 로컬 Administrators 그룹에 그룹을 추가합니다.
  - * Cloud Workspace 방화벽 GPO * (전용 고객 서버, 원격 데스크톱 및 스테이징 OU에 연결) - 플랫폼 서버에서 세션 호스트와의 연결을 확인하고 격리하는 정책을 만듭니다.
  - * Cloud Workspace RDS * (전용 고객 서버, 원격 데스크톱 및 스테이징 OU) - 세션 품질, 안정성, 연결 해제 시간 제한에 대한 정책 설정 제한. RDS 세션의 경우 TS 라이선스 서버 값이 정의됩니다.
  - * Cloud Workspace Companies * (기본적으로 연결되지 않음) – 관리 도구 및 영역에 대한 액세스를 방지하여 사용자 세션/작업 영역을 "잠금"하는 GPO(옵션)입니다. 제한된 활동 작업 공간을 제공하도록 연결/활성화할 수 있습니다.

요청 시 기본 그룹 정책 설정 구성을 제공할 수 있습니다.

**VDS** 작업 영역 구성 요소

데이터 계층

**Azure NetApp Files**

VDS 설정에서 Azure NetApp Files를 데이터 계층 옵션으로 선택하면 Azure NetApp Files 용량 풀 및 관련 볼륨이 생성됩니다. 볼륨은 사용자 프로필(FSLogix 컨테이너 사용), 사용자 개인 폴더 및 기업 데이터 공유 폴더에 대한 공유 파일 스토리지를 호스팅합니다.

**Azure** 파일

CWS 설정에서 Azure 파일을 데이터 계층 옵션으로 선택한 경우 Azure 파일 공유 및 연결된 Azure 저장소 계정이 생성됩니다. Azure File Share는 사용자 프로필(FSLogix 컨테이너 사용), 사용자 개인 폴더 및 회사 데이터 공유 폴더에 대한 공유 파일 스토리지를 호스팅합니다.

관리 디스크가 있는 파일 서버입니다

VDS 설정에서 파일 서버를 데이터 계층 옵션으로 선택한 경우 Windows Server VM이 관리되는 디스크로 생성됩니다. 파일 서버는 사용자 프로필(FSLogix 컨테이너 사용), 사용자 개인 폴더 및 기업 데이터 공유 폴더에 대한 공유 파일 스토리지를 호스팅합니다.

**Azure** 네트워킹

**Azure** 가상 네트워크

VDS는 Azure 가상 네트워크 및 지원 서브넷을 생성합니다. VDS는 CWMGR1, AVD 호스트 컴퓨터, Azure 도메인 컨트롤러 및 서브넷 간 피어링을 위한 별도의 서브넷이 필요합니다. AD 컨트롤러 서브넷은 일반적으로 이미 존재하므로 VDS가 배포된 서브넷은 기존 서브넷을 통해 살펴봐야 합니다.

네트워크 보안 그룹

CWMGR1 VM에 대한 액세스를 제어하기 위해 네트워크 보안 그룹이 생성됩니다.

- 테넌트: 세션 호스트 및 데이터 VM에서 사용할 IP 주소를 포함합니다
- 서비스: PaaS 서비스에서 사용할 IP 주소 포함(예: Azure NetApp Files)
- 플랫폼: NetApp 플랫폼 VM(CWMGR1 및 모든 게이트웨이 서버)으로 사용할 IP 주소를 포함합니다.
- Directory(디렉터리): Active Directory VM으로 사용할 IP 주소를 포함합니다

**Azure AD**

VDS 자동화 및 오케스트레이션은 가상 시스템을 대상 Active Directory 인스턴스에 배포한 다음 시스템을 지정된 호스트 풀에 연결합니다. Avd 가상 시스템은 AD 구조(조직 단위, 그룹 정책, 로컬 컴퓨터 관리자 권한 등)와 AVD 구조(호스트 풀, 작업 영역 앱 그룹 구성원)의 구성원 모두 컴퓨터 수준에서 관리되며 Azure AD 엔터티 및 권한에 의해 관리됩니다. VDS는 AVD 작업에 대한 VDS Enterprise Application/Azure Service Principal 및 로컬 AD 및 로컬 컴퓨터 작업에 대한 로컬 AD 서비스 계정(CloudWorkspaceSVC)을 사용하여 이 “이중 제어” 환경을 처리합니다.

AVD 가상 머신을 생성하고 AVD 호스트 풀에 추가하는 구체적인 단계는 다음과 같습니다.

- Azure 템플릿에서 가상 머신 생성 AVD와 연결된 Azure 구독에 표시(Azure Service Principal 권한 사용)

- VDS 배포 중에 지정된 Azure VNET를 사용하여 새 가상 머신에 대한 DNS 주소 확인/구성(로컬 AD 권한 필요(위의 모든 권한을 CW-Infrastructure에 위임함) 표준 VDS 명명 체계 *_{companycode}TS{sequencenumber}_ * 를 사용하여 가상 머신 이름을 설정합니다. 예: XYZTS3. (로컬 AD 권한 필요(사내에서 만든 OU 구조(원격 데스크톱/회사 코드/공유)(위와 동일한 권한/그룹 설명)
- 지정된 AD(Active Directory Organizational Unit)에 가상 컴퓨터를 배치합니다(OU 구조에 위임된 권한 필요(위의 수동 프로세스 중에 지정됨)).
- 내부 AD DNS 디렉터리를 새 컴퓨터 이름/IP 주소로 업데이트(로컬 AD 권한 필요)
- 새 가상 시스템을 로컬 AD 도메인에 연결(로컬 AD 권한 필요)
- VDS 로컬 데이터베이스를 새 서버 정보로 업데이트(추가 권한이 필요하지 않음)
- 지정된 AVD 호스트 풀에 VM 연결(AVD 서비스 담당자 권한 필요)
- 새 가상 머신에 초콜릿 구성 요소를 설치합니다( * CloudWorkspaceSVC * 계정에 대한 로컬 컴퓨터 관리 권한 필요).
- AVD 인스턴스에 대해 FSLogix 구성 요소 설치(로컬 AD의 AVD OU에 대한 로컬 컴퓨터 관리 권한 필요)
- AD Windows 방화벽 GPO를 업데이트하여 새 VM에 대한 트래픽을 허용합니다(AVD OU 및 연결된 가상 시스템과 관련된 정책에 대해 AD GPO 생성/수정 필요). 로컬 AD의 AVD OU에 AD GPO 정책을 생성/수정해야 합니다. VDS를 통해 VM을 관리하지 않는 경우 설치 후 기능을 끌 수 있습니다.)
- 새 가상 머신에 "새 연결 허용" 플래그 설정(Azure Service Principal 권한 필요)

**Azure AD**에 **VM**을 가입하는 중입니다

Azure 테넌트의 가상 시스템은 도메인에 가입해야 하지만 VM은 Azure AD에 직접 가입할 수 없습니다. 따라서 VDS는 VDS 플랫폼에서 도메인 컨트롤러 역할을 배포한 다음 AD Connect를 사용하여 해당 DC를 Azure AD와 동기화합니다. 대체 구성 옵션에는 AADDS(Azure AD Domain Services) 사용, AD Connect를 사용한 하이브리드 DC(사내 또는 기타 VM)로 동기화, 사이트 간 VPN 또는 Azure ExpressRoute를 통한 하이브리드 DC에 VM 직접 연결 등이 있습니다.

**Avd** 호스트 풀

호스트 풀은 Azure Virtual Desktop 환경 내에서 하나 이상의 동일한 가상 머신(VM)의 모음입니다. 각 호스트 풀에는 사용자가 실제 데스크톱에서와 같이 상호 작용할 수 있는 앱 그룹이 포함될 수 있습니다.

세션 호스트입니다

호스트 풀 내에서 하나 이상의 동일한 가상 시스템이 있습니다. 이 호스트 풀에 연결되는 이러한 사용자 세션은 AVD 로드 밸런싱 장치 서비스에 의해 로드 밸런싱됩니다.

앱 그룹

기본적으로 배포 시 _Desktop users_app 그룹이 만들어집니다. 이 앱 그룹 내의 모든 사용자에게 전체 Windows 데스크톱 환경이 제공됩니다. 또한 앱 그룹을 생성하여 스트리밍 앱 서비스를 제공할 수 있습니다.

로그 분석 작업 영역

Log Analytics 작업 영역은 배포, DSC 프로세스 및 기타 서비스의 로그를 저장하기 위해 생성됩니다. 배포 후에는 이 기능을 삭제할 수 있지만 다른 기능을 사용할 수 있으므로 권장하지 않습니다. 로그는 기본적으로 30일 동안 보관되며, 보존 비용이 청구되지 않습니다.

가용성 세트

Availability Set는 배포 프로세스의 일부로 설정되어 공유 VM(공유 AVD 호스트 풀, RDS 리소스 풀)을 장애 도메인 간에 분리할 수 있습니다. 원하는 경우 구축 후 삭제할 수 있지만 공유 VM에 대한 추가 내결함성을 제공하는 옵션을 비활성화할 수 있습니다.

#### Azure 복구 볼트

복구 서비스 저장소는 배포 중에 VDS Automation에 의해 생성됩니다. 배포 프로세스 중에 Azure Backup이 CWMGR1에 적용되므로 이 기능은 기본적으로 활성화되어 있습니다. 이 기능은 원하는 경우 비활성화 및 제거할 수 있지만 환경에서 Azure Backup이 활성화된 경우 다시 생성됩니다.

#### Azure 키 볼트

Azure Key Vault는 배포 프로세스 중에 생성되며 배포 중에 Azure Automation 계정이 사용하는 인증서, API 키 및 자격 증명을 저장하는 데 사용됩니다.

##### 부록 A – 기본 Cloud Workspace 조직 구성 단위 구조

- 클라우드 작업 공간
  - Cloud Workspace 회사
  - Cloud Workspace 서버
    - 전용 고객 서버
    - 검토할 수 있습니다
- CWMGR 서버
- 게이트웨이 서버
- FTP 서버
- 템플릿 VM
  - 원격 데스크탑
  - 스테이징
    - Cloud Workspace 서비스 계정
  - 클라이언트 서비스 계정
  - 인프라 서비스 계정
    - Cloud Workspace 기술 사용자
  - 그룹
  - 기술 3 정비사

### Avd 및 VDS v5.4 사전 요구 사항

#### Avd 및 VDS 요구 사항 및 참고 사항

이 문서에서는 VDS(NetApp Virtual Desktop Service)를 사용하여 Azure AVD(Virtual Desktop)를 구축하는 데 필요한 요소에 대해 설명합니다. "빠른 점검 목록"에서는 효율적인 배포를 위해 필요한 구성 요소 및 배포 전 단계에 대한 간단한 목록을 제공합니다. 이 가이드의 나머지 부분에서는 선택한 구성에 따라 각 요소에 대해 더 자세히 설명합니다.

### **Azure** 요구사항

- Azure AD 테넌트
- AVD 지원을 위한 Microsoft 365 라이선스
- Azure 구독
- Azure 가상 시스템에 사용 가능한 Azure 할당량
- 글로벌 관리자 및 구독 소유권 역할이 있는 Azure 관리자 계정
- AD Connect 설정에 대해 '엔터프라이즈 관리자' 역할이 있는 도메인 관리자 계정

### 배포 전 정보

- 총 사용자 수를 결정합니다
- Azure 지역 결정
- Active Directory 유형을 확인합니다
- 스토리지 유형을 확인합니다
- 세션 호스트 VM 이미지 또는 요구 사항을 식별합니다
- 기존 Azure 및 사내 네트워킹 구성을 평가합니다

#### **VDS** 배포 세부 요구 사항

### 최종 사용자 연결 요구 사항

다음 원격 데스크톱 클라이언트는 **Azure Virtual Desktop**을 지원합니다**.**

- Windows 데스크톱
- 웹
- macOS
- iOS
- IGEL 고려 클라이언트(Linux)
- Android(Preview)

> Azure Virtual Desktop은 RemoteApp 및 데스크탑 연결(RADC) 클라이언트 또는 원격 데스크톱 연결(MSCSC) 클라이언트를 지원하지 않습니다.

> Azure Virtual Desktop은 현재 Windows Store에서 원격 데스크톱 클라이언트를 지원하지 않습니다. 이 클라이언트에 대한 지원은 향후 릴리즈에서 추가될 예정입니다.

- 원격 데스크톱 클라이언트는 다음 URL에 액세스할 수 있어야 합니다. *

| 주소 | 아웃바운드 **TCP** 포트 | 목적 | 클라이언트 |
| --- | --- | --- | --- |
| .AVD.microsoft.com 으로 문의하십시오 | 443 | 서비스 트래픽 | 모두 |
| * .servicebus.windows.net 443 데이터 문제 해결 | 모두 | go.microsoft.com | 443 |
| Microsoft FWLinks를 참조하십시오 | 모두 | aka.ms | 443 |
| Microsoft URL 바로가기 | 모두 | docs.microsoft.com | 443 |
| 문서화 | 모두 | privacy.microsoft.com | 443 |
| 개인 정보 보호 정책 | 모두 | query.prod.cms.rt.microsoft.com | 443 |

이러한 URL을 여는 것은 안정적인 클라이언트 환경을 위해 필수적입니다. 이러한 URL에 대한 액세스를 차단하는 것은 지원되지 않으며 서비스 기능에 영향을 줍니다. 이러한 URL은 클라이언트 사이트 및 리소스에만 해당되며 Azure Active Directory와 같은 다른 서비스의 URL은 포함하지 않습니다.

**VDS** 설정 마법사 시작 지점

VDS 설정 마법사는 성공적인 AVD 배포에 필요한 필수 구성 요소 설정을 대부분 처리할 수 있습니다. 설정 마법사("")는 다음 부품을 작성하거나 사용합니다.

**Azure** 테넌트

- 필수: * Azure 테넌트 및 Azure Active Directory

Azure에서 Avd 활성화는 테넌트 전체 설정입니다. VDS는 테넌트당 하나의 AVD 인스턴스 실행을 지원합니다.

**Azure**에 가입했습니다

- 필수: * Azure 가입(사용하려는 가입 ID 참고)

배포된 모든 Azure 리소스는 하나의 전용 구독으로 설정해야 합니다. 따라서 AVD의 비용을 훨씬 쉽게 추적하고 구축 프로세스를 간소화할 수 있습니다. 참고: Azure 무료 평가판은 기능 AVD 구축을 위한 크레딧이 충분하지 않기 때문에 지원되지 않습니다.

**Azure** 코어 할당량

사용할 VM 제품군에 대한 할당량 - 특히 초기 플랫폼 배포에 대해 DS v3 제품군의 최소 10개 코어(2개 코어를 사용할 수 있지만 10개는 모든 초기 배포 가능성을 포괄함).

**Azure** 관리자 계정

- 필수: * Azure 글로벌 관리자 계정.

VDS 설정 마법사는 Azure 관리자가 VDS 서비스 보안 주체에 위임된 권한을 부여하고 VDS Azure Enterprise 응용 프로그램을 설치하도록 요청합니다. 관리자는 다음과 같은 Azure 역할을 할당해야 합니다.

- 테넌트의 글로벌 관리자

- 구독의 소유자 역할입니다

**VM** 이미지

- 필수: * 다중 세션 Windows 10을 지원하는 Azure 이미지.

Azure Marketplace는 가장 최신 버전의 기본 Windows 10 이미지를 제공하며 모든 Azure 구독은 이러한 이미지에 자동으로 액세스할 수 있습니다. 다른 이미지 또는 사용자 정의 이미지를 사용하려면 VDS 팀에서 다른 이미지 생성 또는 수정에 대한 조언을 제공하거나 Azure 이미지에 대한 일반적인 질문을 통해 저희에게 알려주시면 대화 일정을 잡을 수 있습니다.

**Active Directory**를 클릭합니다

Avd는 사용자 ID가 Azure AD의 일부이고 VM이 동일한 Azure AD 인스턴스와 동기화된 Active Directory 도메인에 가입되어야 합니다. VM을 Azure AD 인스턴스에 직접 연결할 수 없으므로 도메인 컨트롤러를 구성하여 Azure AD와 동기화해야 합니다.

지원되는 옵션은 다음과 같습니다**.**

- 구독 내에서 Active Directory 인스턴스의 자동 빌드. AD 인스턴스는 일반적으로 이 옵션을 사용하는 Azure 가상 데스크톱 배포의 경우 VDS 제어 VM(CWMGR1)에서 VDS에 의해 생성됩니다. 설치 프로세스의 일부로 Azure AD와 동기화하도록 AD Connect를 설정하고 구성해야 합니다.

  []

- Azure 가입(일반적으로 Azure VPN 또는 Express Route를 통해)에서 액세스할 수 있고 AD Connect 또는 타사 제품을 사용하여 Azure AD와 사용자 목록을 동기화한 기존 Active Directory 도메인에 통합할 수 있습니다.

  []

지원합니다

AVD에서 스토리지 전략은 AVD 세션 VM에 영구 사용자/회사 데이터가 상주하지 않도록 설계되었습니다. 사용자 프로필, 사용자 파일 및 폴더, 회사/애플리케이션 데이터에 대한 영구 데이터는 독립 데이터 계층에서 호스팅되는 하나 이상의 데이터 볼륨에 호스팅됩니다.

FSLogix는 세션 초기화 시 사용자 프로필 컨테이너(VHD 또는 VHDX 형식)를 세션 호스트에 마운트하여 데이터 스프롤 및 느린 로그인과 같은 다양한 사용자 프로필 문제를 해결하는 프로파일 컨테이너화 기술입니다.

이 아키텍처로 인해 데이터 저장 기능이 필요합니다. 이 기능은 사용자의 상당 부분이 동시에 로그인/로그오프하는 경우 매일 아침/오후에 필요한 데이터 전송을 처리할 수 있어야 합니다. 중간 규모의 환경에서도 상당한 데이터 전송 요구사항이 있을 수 있습니다. 데이터 스토리지 계층의 디스크 성능은 기본 최종 사용자 성능 변수 중 하나이므로 스토리지 용량뿐만 아니라 스토리지 성능의 크기를 적절하게 조정할 수 있도록 특별히 주의를 기울여야 합니다. 일반적으로 스토리지 계층의 크기는 사용자당 5-15 IOPS를 지원하도록 조정해야 합니다.

**VDS** 설정 마법사는 다음 구성을 지원합니다**.**

- Azure NetApp Files(ANF) 설정 및 구성(권장) _ANF 표준 서비스 수준은 최대 150명의 사용자를 지원하며 150-500명의 사용자 환경 ANF Premium을 권장합니다. 사용자 500명 이상인 경우 ANF Ultra를 권장합니다. _

  []

- 파일 서버 VM의 설정 및 구성

[]

네트워킹

- 필수: * Azure Express Route 또는 VPN을 통해 Azure 구독에 표시되는 서브넷을 포함하여 모든 기존 네트워크 서브넷의 인벤토리. 배포는 중복되는 서브넷을 피해야 합니다.

VDS 설정 마법사를 사용하면 기존 네트워크와의 계획된 통합의 일부로 필요한 범위 또는 피해야 할 범위가 있는 경우 네트워크 범위를 정의할 수 있습니다.

배포 중에 사용자에게 IP 범위를 결정합니다. Azure 모범 사례당, 전용 범위의 IP 주소만 지원됩니다.

지원되는 선택 항목은 다음과 같지만 기본적으로 **A/20** 범위입니다**.**

- 192.168.0.0 ~ 192.168.255.255
- 172.16.0.0 ~ 172.31.255.255
- 10.0.0.0 ~ 10.255.255.255

**CWMGR1**

비용 절감 워크로드 스케줄링 및 라이브 확장 기능과 같은 VDS의 고유한 기능 중 일부는 테넌트 및 구독 내에서 관리 기능을 필요로 합니다. 따라서 CWMGR1이라는 관리 VM은 VDS 설정 마법사 자동화의 일부로 배포됩니다. 이 VM은 VDS 자동화 작업 외에도 SQL Express 데이터베이스, 로컬 로그 파일 및 DCConfig라는 고급 구성 유틸리티에서 VDS 구성을 유지합니다.

**VDS** 설정 마법사에서 선택한 항목에 따라 이 **VM**을 사용하여 다음을 포함한 추가 기능을 호스팅할 수 있습니다**.**

- RDS 게이트웨이(RDS 배포에서만 사용)
- HTML 5 게이트웨이(RDS 배포에서만 사용됨)
- RDS 라이센스 서버(RDS 배포에서만 사용)
- 도메인 컨트롤러(선택된 경우)

배포 마법사의 의사 결정 트리 구조

초기 배포의 일부로 새로운 환경에 대한 설정을 사용자 지정하기 위한 일련의 질문에 대한 답변이 제공됩니다. 다음은 결정해야 할 주요 결정 사항에 대한 개요입니다.

**Azure** 지역

AVD 가상 머신을 호스팅할 Azure 지역 또는 지역을 결정합니다. Azure NetApp Files 및 특정 VM 제품군(예: GPU 지원 VM)에는 Azure 지역 지원 목록이 정의되어 있고 AVD는 대부분의 지역에서 사용할 수 있습니다.

- 이 링크를 사용하여 식별할 수 있습니다 "Azure 제품은 지역별로 제공됩니다"

**Active Directory** 유형입니다

사용할 Active Directory 유형 결정:

- 기존 온프레미스 Active Directory
- 을 참조하십시오 "Avd VDS 구성 요소 및 사용 권한" Azure 및 로컬 Active Directory 환경 모두에서 필요한 사용 권한 및 구성 요소에 대한 설명을 문서화하십시오

- 새로운 Azure 구독 기반 Active Directory 인스턴스
- Azure Active Directory 도메인 서비스

데이터 스토리지

사용자 프로필, 개별 파일 및 회사 공유에 대한 데이터를 배치할 위치를 결정합니다. 선택 가능한 항목은 다음과 같습니다.

- Azure NetApp Files
- Azure 파일
- 기존 파일 서버(관리형 디스크가 있는 Azure VM)

#### NetApp VDS 배포 요구 사항(기존 구성 요소에 대한 배포 요구 사항)

기존 **Active Directory** 도메인 컨트롤러를 사용한 **NetApp VDS** 배포

이 구성 유형은 기존 Active Directory 도메인을 확장하여 AVD 인스턴스를 지원합니다. 이 경우 VDS는 제한된 구성 요소 집합을 도메인에 배포하여 AVD 구성 요소에 대한 자동 프로비저닝 및 관리 작업을 지원합니다.

이 구성에는 다음이 필요합니다.

- Azure VNET의 VM에서 액세스할 수 있는 기존 Active Directory 도메인 컨트롤러이며, 일반적으로 Azure에서 생성된 Azure VPN 또는 Express Route 또는 도메인 컨트롤러를 통해 액세스할 수 있습니다.
- vDS 구성 요소 및 사용 권한 추가 AVD 호스트 풀 및 데이터 볼륨을 도메인에 연결할 때 VDS 관리에 필요합니다. AVD VDS 구성 요소 및 사용 권한 가이드에서는 필요한 구성 요소와 사용 권한을 정의하고 배포 프로세스를 수행하려면 도메인 권한이 있는 도메인 사용자가 필요한 요소를 만드는 스크립트를 실행해야 합니다.
- VDS 배포는 VDS에서 생성된 VM에 대해 기본적으로 VNET를 생성합니다. VNET는 기존 Azure 네트워크 VNets로 피어링하거나 CWMGR1 VM을 필요한 서브넷이 미리 정의된 기존 VNET로 이동할 수 있습니다.

자격 증명 및 도메인 준비 도구

관리자는 배포 프로세스의 특정 시점에 도메인 관리자 자격 증명을 제공해야 합니다. 임시 도메인 관리자 자격 증명은 나중에 생성, 사용 및 삭제할 수 있습니다(배포 프로세스가 완료되면). 또는 필수 구성 요소 구축에 도움이 필요한 고객은 도메인 준비 도구를 활용할 수 있습니다.

기존 파일 시스템을 사용한 **NetApp VDS** 배포

VDS는 사용자 프로필, 개인 폴더 및 기업 데이터를 AVD 세션 VM에서 액세스할 수 있는 Windows 공유를 생성합니다. VDS는 기본적으로 파일 서버 또는 Azure NetApp 파일 옵션을 배포하지만, 기존 파일 저장소 구성 요소가 있는 경우 VDS 배포가 완료되면 VDS가 해당 구성 요소에 공유를 지정할 수 있습니다.

및 기존 스토리지 구성요소를 사용하기 위한 요구사항:

- 이 구성 요소는 SMB v3을 지원해야 합니다
- 구성 요소는 AVD 세션 호스트와 동일한 Active Directory 도메인에 연결해야 합니다
- 구성 요소는 VDS 구성에서 사용할 UNC 경로를 노출할 수 있어야 합니다. 즉, 세 공유 모두에 대해 하나의 경로를 사용하거나 각 경로에 대해 별도의 경로를 지정할 수 있습니다. VDS는 이러한 공유에 대한 사용자 수준 권한을 설정하므로 VDS AVD Components and Permissions(VDS AVD 구성 요소 및 권한) 문서를 참조하여 적절한 권한이 VDS Automation Services에 부여되었는지 확인합니다.

### NetApp VDS 배포와 기존 Azure AD 도메인 서비스

이 구성을 수행하려면 기존 Azure Active Directory 도메인 서비스 인스턴스의 속성을 식별하는 프로세스가 필요합니다. 이 유형의 배포를 요청하려면 계정 관리자에게 문의하십시오. NetApp VDS Deployment with existing AVD deployment 이 구성 형식은 필요한 Azure VNET, Active Directory 및 AVD 구성 요소가 이미 있다고 가정합니다. VDS 배포는 “기존 AD를 사용한 NetApp VDS 배포” 구성과 동일한 방식으로 수행되지만 다음과 같은 요구 사항이 추가됩니다.

- AVD 테넌트의 RD 소유자 역할은 Azure의 VDS 엔터프라이즈 응용 프로그램에 부여해야 합니다
- vDS Web App의 VDS 가져오기 기능을 사용하여 Avd 호스트 풀 및 AVD 호스트 풀 VM을 vDS로 가져와야 합니다 이 프로세스는 AVD 호스트 풀 및 세션 VM 메타데이터를 수집하고 VDS에 저장하여 이러한 요소를 VDS에서 관리할 수 있도록 합니다
- Avd 사용자 데이터는 CRA 도구를 사용하여 VDS 사용자 섹션으로 가져와야 합니다. 이 프로세스는 각 사용자에 대한 메타데이터를 VDS 컨트롤 평면에 삽입하여 AVD 앱 그룹 구성원 및 세션 정보를 VDS에서 관리할 수 있도록 합니다

#### 부록 A: VDS 컨트롤 플레인 URL 및 IP 주소

Azure 구독의 VDS 구성 요소는 VDS 웹 응용 프로그램 및 VDS API 끝점과 같은 VDS 글로벌 컨트롤 플레인 구성 요소와 통신합니다. 액세스하려면 포트 443에서 양방향 액세스에 대해 다음 기본 URI 주소를 안전 목록에 추가해야 합니다.

"" "" "" "" ""

액세스 제어 장치가 IP 주소로만 안전 목록만 할 수 있는 경우 다음 IP 주소 목록을 안전하게 나열해야 합니다. VDS는 Azure Traffic Manager 서비스를 사용하므로 시간이 지남에 따라 이 목록이 변경될 수 있습니다.

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.167 40.147.2 40.147.2 40.86.86.86.86.86.86.86.86.0.1622.1752.1722.17.22.172.17.22.116.22.118.22.1722.172.116.22.118.22.118.22.118.22.172.118.17.22.118.22.118.22.118.17.22.118.22.172.118.22.118.22.118.22.118.22.

#### 부록 B: Microsoft AVD 요구 사항

이 Microsoft AVD 요구 사항 섹션은 Microsoft의 AVD 요구 사항을 요약한 것입니다. 전체 및 현재 AVD 요구 사항은 다음 여기에서 확인할 수 있습니다.

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

### Azure Virtual Desktop 세션 호스트 라이센스

Azure Virtual Desktop은 다음 운영 체제를 지원하므로 배포하려는 데스크톱 및 앱을 기반으로 사용자에게 적합한 라이센스를 보유하고 있어야 합니다.

| OS | 필수 라이센스 |
|---|---|
| Windows 10 Enterprise 다중 세션 또는 Windows 10 Enterprise | Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5 |
| Windows 7 Enterprise | Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5 |
| Windows Server 2012 R2, 2016, 2019년 | Software Assurance가 포함된 RDS CAL(클라이언트 액세스 라이선스 |

**AVD** 시스템의 **URL** 액세스

Azure Virtual Desktop용으로 생성한 Azure 가상 머신은 다음 URL에 대한 액세스 권한이 있어야 합니다.

| 주소 | 아웃바운드 **TCP** 포트 | 목적 | 서비스 태그 |
|---|---|---|---|
| .AVD.microsoft.com 으로 문의하십시오 | 443 | 서비스 트래픽 | WindowsVirtualDesktop을 참조하십시오 |
| mrsglobalsteus2prod.blob.core.windows.net | 443 | 에이전트 및 SxS 스택 업데이트 | AzureCloud를 참조하십시오 |
| .core.windows.net 으로 문의하십시오 | 443 | 상담원 트래픽 | AzureCloud를 참조하십시오 |
| .servicebus.windows.net 으로 문의하십시오 | 443 | 상담원 트래픽 | AzureCloud를 참조하십시오 |
| prod.warmpath.msftclouds.com | 443 | 상담원 트래픽 | AzureCloud를 참조하십시오 |
| catalogartifact.azureedge.net | 443 | Azure 마켓플레이스 를 참조하십시오 | AzureCloud를 참조하십시오 |
| kms.core.windows.net | 1688)을 참조하십시오 | Windows 정품 인증 | 인터넷 |
| AVDportalstorageblob.blob.core.windows.net | 443 | Azure 포털 지원 | AzureCloud를 참조하십시오 |

다음 표에는 Azure 가상 시스템에서 액세스할 수 있는 선택적 URL이 나열되어 있습니다.

| 주소 | 아웃바운드 **TCP** 포트 | 목적 | 서비스 태그 |
|---|---|---|---|
| .microsoftonline.com 으로 문의하십시오 | 443 | MS 온라인 서비스에 대한 인증 | 없음 |
| .events.data.microsoft.com 으로 문의하십시오 | 443 | 원격 측정 서비스 | 없음 |
| www.msftconnecttest.com | 443 | OS가 인터넷에 연결되어 있는지 감지합니다 | 없음 |
| .prod.do.dsp.mp.microsoft.com 으로 문의하십시오 | 443 | Windows 업데이트 | 없음 |
| login.windows.net | 443 | MS Online Services, Office 365에 로그인합니다 | 없음 |
| *.sfx.ms | 443 | OneDrive 클라이언트 소프트웨어 업데이트 | 없음 |
| .digicert.com 으로 문의하십시오 | 443 | 인증서 해지 확인 | 없음 |

최적의 성능 요소

최적의 성능을 위해 네트워크가 다음 요구 사항을 충족하는지 확인하십시오.

- 클라이언트 네트워크에서 호스트 풀이 구축된 Azure 영역까지의 RTT(Round-Trip) 지연 시간은 150ms 미만이어야 합니다.

- 데스크톱 및 앱을 호스팅하는 VM이 관리 서비스에 연결되면 네트워크 트래픽이 국가/지역 경계 외부로 흐를 수 있습니다.
- 네트워크 성능을 최적화하기 위해 세션 호스트의 VM이 관리 서비스와 동일한 Azure 영역에 배치되도록 권장합니다.

지원되는 가상 머신 **OS** 이미지

Azure Virtual Desktop은 다음 x64 운영 체제 이미지를 지원합니다.

- Windows 10 Enterprise 다중 세션, 버전 1809 이상
- Windows 10 Enterprise, 버전 1809 이상
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop은 x86(32비트), Windows 10 Enterprise N 또는 Windows 10 Enterprise KN 운영 체제 이미지를 지원하지 않습니다. 또한 Windows 7은 섹터 크기 제한으로 인해 관리되는 Azure 스토리지에서 호스팅되는 VHD 또는 VHDX 기반 프로파일 솔루션을 지원하지 않습니다.

사용 가능한 자동화 및 구축 옵션은 다음 표와 같이 선택하는 OS와 버전에 따라 다릅니다.

| 운영 체제 | **Azure** 이미지 갤러리 | 수동 **VM** 배포 | **ARM** 템플릿 통합 | **Azure Marketplace**에서 호스트 풀을 프로비저닝합니다 |
|---|---|---|---|---|
| Windows 10 다중 세션, 버전 1903 | 예 | 예 | 예 | 예 |
| Windows 10 다중 세션, 버전 1809 | 예 | 예 | 아니요 | 아니요 |
| Windows 10 Enterprise, 버전 1903 | 예 | 예 | 예 | 예 |
| Windows 10 Enterprise, 버전 1809 | 예 | 예 | 아니요 | 아니요 |
| Windows 7 Enterprise | 예 | 예 | 아니요 | 아니요 |
| Windows Server 2019 | 예 | 예 | 아니요 | 아니요 |
| Windows Server 2016 | 예 | 예 | 예 | 예 |
| Windows Server 2012 R2 | 예 | 예 | 아니요 | 아니요 |

**Avd** 및 **VDS v6.0** 필수 구성 요소

**Avd** 및 **VDS** 요구 사항 및 참고 사항

이 문서에서는 VDS(NetApp Virtual Desktop Service)를 사용하여 Azure AVD(Virtual Desktop)를 구축하는 데 필요한 요소에 대해 설명합니다. "빠른 점검 목록"에서는 효율적인 배포를 위해 필요한 구성 요소 및 배포 전 단계에 대한 간단한 목록을 제공합니다. 이 가이드의 나머지 부분에서는 선택한 구성에 따라 각 요소에 대해 더 자세히 설명합니다.

### **Azure** 요구사항

- Azure AD 테넌트
- AVD 지원을 위한 Microsoft 365 라이선스
- Azure 구독
- Azure 가상 시스템에 사용 가능한 Azure 할당량
- 글로벌 관리자 및 구독 소유권 역할이 있는 Azure 관리자 계정
- AD Connect 설정에 대해 '엔터프라이즈 관리자' 역할이 있는 도메인 관리자 계정

### 배포 전 정보

- 총 사용자 수를 결정합니다
- Azure 지역 결정
- Active Directory 유형을 확인합니다
- 스토리지 유형을 확인합니다
- 세션 호스트 VM 이미지 또는 요구 사항을 식별합니다
- 기존 Azure 및 사내 네트워킹 구성을 평가합니다

#### **VDS** 배포 세부 요구 사항

### 최종 사용자 연결 요구 사항

다음 원격 데스크톱 클라이언트는 **Azure Virtual Desktop**을 지원합니다**.**

- Windows 데스크톱
- 웹
- macOS
- iOS
- IGEL 고려 클라이언트(Linux)
- Android(Preview)

> Azure Virtual Desktop은 RemoteApp 및 데스크탑 연결(RADC) 클라이언트 또는 원격 데스크톱 연결(MSCSC) 클라이언트를 지원하지 않습니다.

> Azure Virtual Desktop은 현재 Windows Store에서 원격 데스크톱 클라이언트를 지원하지 않습니다. 이 클라이언트에 대한 지원은 향후 릴리즈에서 추가될 예정입니다.

- 원격 데스크톱 클라이언트는 다음 URL에 액세스할 수 있어야 합니다. *

| 주소 | 아웃바운드 **TCP** 포트 | 목적 | 클라이언트 |
| --- | --- | --- | --- |
| .wvd.microsoft.com 으로 문의하십시오 | 443 | 서비스 트래픽 | 모두 |
| .servicebus.windows.net 으로 문의하십시오 | 443 | 데이터 문제 해결 | 모두 |
| go.microsoft.com | 443 | Microsoft FWLinks를 참조하십시오 | 모두 |
| aka.ms | 443 | Microsoft URL 바로가기 | 모두 |
| docs.microsoft.com | 443 | 문서화 | 모두 |
| privacy.microsoft.com | 443 | 개인 정보 보호 정책 | 모두 |
| query.prod.cms.rt.microsoft.com | 443 | 클라이언트 업데이트 | Windows 데스크톱 |

이러한 URL을 여는 것은 안정적인 클라이언트 환경을 위해 필수적입니다. 이러한 URL에 대한 액세스를 차단하는 것은 지원되지 않으며 서비스 기능에 영향을 줍니다. 이러한 URL은 클라이언트 사이트 및 리소스에만 해당되며 Azure Active Directory와 같은 다른 서비스의 URL은 포함하지 않습니다.

**VDS** 설정 마법사 시작 지점

VDS 설정 마법사는 성공적인 AVD 배포에 필요한 필수 구성 요소 설정을 대부분 처리할 수 있습니다. 설정 마법사("")는 다음 부품을 작성하거나 사용합니다.

**Azure** 테넌트

- 필수: * Azure 테넌트 및 Azure Active Directory

Azure에서 Avd 활성화는 테넌트 전체 설정입니다. VDS는 테넌트당 하나의 AVD 인스턴스 실행을 지원합니다.

**Azure**에 가입했습니다

- 필수: * Azure 가입(사용하려는 가입 ID 참고)

배포된 모든 Azure 리소스는 하나의 전용 구독으로 설정해야 합니다. 따라서 AVD의 비용을 훨씬 쉽게 추적하고 구축 프로세스를 간소화할 수 있습니다. 참고: Azure 무료 평가판은 기능 AVD 구축을 위한 크레딧이 충분하지 않기 때문에 지원되지 않습니다.

**Azure** 코어 할당량

사용할 VM 제품군에 대한 할당량 - 특히 초기 플랫폼 배포에 대해 DS v3 제품군의 최소 10개 코어(2개 코어를 사용할 수 있지만 10개는 모든 초기 배포 가능성을 포괄함).

**Azure** 관리자 계정

- 필수: * Azure 글로벌 관리자 계정.

VDS 설정 마법사는 Azure 관리자가 VDS 서비스 보안 주체에 위임된 권한을 부여하고 VDS Azure Enterprise 응용 프로그램을 설치하도록 요청합니다. 관리자는 다음과 같은 Azure 역할을 할당해야 합니다.

- 테넌트의 글로벌 관리자
- 구독의 소유자 역할입니다

**VM** 이미지

- 필수: * 다중 세션 Windows 10을 지원하는 Azure 이미지.

Azure Marketplace는 가장 최신 버전의 기본 Windows 10 이미지를 제공하며 모든 Azure 구독은 이러한 이미지에 자동으로 액세스할 수 있습니다. 다른 이미지 또는 사용자 정의 이미지를 사용하려면 VDS 팀에서 다른 이미지 생성 또는 수정에 대한 조언을 제공하거나 Azure 이미지에 대한 일반적인 질문을 통해 저희에게 알려주시면 대화 일정을 잡을 수 있습니다.

**Active Directory**를 클릭합니다

Avd는 사용자 ID가 Azure AD의 일부이고 VM이 동일한 Azure AD 인스턴스와 동기화된 Active Directory 도메인에 가입되어야 합니다. VM을 Azure AD 인스턴스에 직접 연결할 수 없으므로 도메인 컨트롤러를 구성하여 Azure AD와 동기화해야 합니다.

지원되는 옵션은 다음과 같습니다**.**

- 구독 내에서 Active Directory 인스턴스의 자동 빌드. AD 인스턴스는 일반적으로 이 옵션을 사용하는 Azure 가상 데스크톱 배포의 경우 VDS 제어 VM(CWMGR1)에서 VDS에 의해 생성됩니다. 설치 프로세스의 일부로 Azure AD와 동기화하도록 AD Connect를 설정하고 구성해야 합니다.

  []

- Azure 가입(일반적으로 Azure VPN 또는 Express Route를 통해)에서 액세스할 수 있고 AD Connect 또는 타사 제품을 사용하여 Azure AD와 사용자 목록을 동기화한 기존 Active Directory 도메인에 통합할 수 있습니다.

  []

지원합니다

AVD에서 스토리지 전략은 AVD 세션 VM에 영구 사용자/회사 데이터가 상주하지 않도록 설계되었습니다. 사용자 프로필, 사용자 파일 및 폴더, 회사/애플리케이션 데이터에 대한 영구 데이터는 독립 데이터 계층에서 호스팅되는 하나 이상의 데이터 볼륨에 호스팅됩니다.

FSLogix는 세션 초기화 시 사용자 프로필 컨테이너(VHD 또는 VHDX 형식)를 세션 호스트에 마운트하여 데이터 스프롤 및 느린 로그인과 같은 다양한 사용자 프로필 문제를 해결하는 프로파일 컨테이너화 기술입니다.

이 아키텍처로 인해 데이터 저장 기능이 필요합니다. 이 기능은 사용자의 상당 부분이 동시에 로그인/로그오프하는 경우 매일 아침/오후에 필요한 데이터 전송을 처리할 수 있어야 합니다. 중간 규모의 환경에서도 상당한 데이터 전송 요구사항이 있을 수 있습니다. 데이터 스토리지 계층의 디스크 성능은 기본 최종 사용자 성능 변수 중 하나이므로 스토리지 용량뿐만 아니라 스토리지 성능의 크기를 적절하게 조정할 수 있도록 특별히 주의를 기울여야 합니다. 일반적으로 스토리지 계층의 크기는 사용자당 5-15 IOPS를 지원하도록 조정해야 합니다.

**VDS** 설정 마법사는 다음 구성을 지원합니다**.**

- Azure NetApp Files(ANF) 설정 및 구성(권장) _ANF 표준 서비스 수준은 최대 150명의 사용자를 지원하며 150-500명의 사용자 환경 ANF Premium을 권장합니다. 사용자 500명 이상인 경우 ANF Ultra를 권장합니다. _

  []

- 파일 서버 VM의 설정 및 구성

  []

네트워킹

- 필수: * Azure Express Route 또는 VPN을 통해 Azure 구독에 표시되는 서브넷을 포함하여 모든 기존 네트워크 서브넷의 인벤토리. 배포는 중복되는 서브넷을 피해야 합니다.

VDS 설정 마법사를 사용하면 기존 네트워크와의 계획된 통합의 일부로 필요한 범위 또는 피해야 할 범위가 있는 경우 네트워크 범위를 정의할 수 있습니다.

배포 중에 사용자에게 IP 범위를 결정합니다. Azure 모범 사례당, 전용 범위의 IP 주소만 지원됩니다.

지원되는 선택 항목은 다음과 같지만 기본적으로 **A/20** 범위입니다**.**

- 192.168.0.0 ~ 192.168.255.255
- 172.16.0.0 ~ 172.31.255.255
- 10.0.0.0 ~ 10.255.255.255

**CWMGR1**

비용 절감 워크로드 스케줄링 및 라이브 확장 기능과 같은 VDS의 고유한 기능 중 일부는 테넌트 및 구독 내에서 관리 기능을 필요로 합니다. 따라서 CWMGR1이라는 관리 VM은 VDS 설정 마법사 자동화의 일부로 배포됩니다. 이 VM은 VDS 자동화 작업 외에도 SQL Express 데이터베이스, 로컬 로그 파일 및 DCConfig라는 고급 구성 유틸리티에서 VDS 구성을 유지합니다.

**VDS** 설정 마법사에서 선택한 항목에 따라 이 **VM**을 사용하여 다음을 포함한 추가 기능을 호스팅할 수 있습니다**.**

- RDS 게이트웨이(RDS 배포에서만 사용)
- HTML 5 게이트웨이(RDS 배포에서만 사용됨)
- RDS 라이센스 서버(RDS 배포에서만 사용)
- 도메인 컨트롤러(선택된 경우)

배포 마법사의 의사 결정 트리 구조

초기 배포의 일부로 새로운 환경에 대한 설정을 사용자 지정하기 위한 일련의 질문에 대한 답변이 제공됩니다. 다음은 결정해야 할 주요 결정 사항에 대한 개요입니다.

**Azure** 지역

AVD 가상 머신을 호스팅할 Azure 지역 또는 지역을 결정합니다. Azure NetApp Files 및 특정 VM 제품군(예: GPU 지원 VM)에는 Azure 지역 지원 목록이 정의되어 있고 AVD는 대부분의 지역에서 사용할 수 있습니다.

- 이 링크를 사용하여 식별할 수 있습니다 "Azure 제품은 지역별로 제공됩니다"

**Active Directory** 유형입니다

사용할 Active Directory 유형 결정:

- 기존 온프레미스 Active Directory

- 을 참조하십시오 "Avd VDS 구성 요소 및 사용 권한" Azure 및 로컬 Active Directory 환경 모두에서 필요한 사용 권한 및 구성 요소에 대한 설명을 문서화하십시오
- 새로운 Azure 구독 기반 Active Directory 인스턴스
- Azure Active Directory 도메인 서비스

데이터 스토리지

사용자 프로필, 개별 파일 및 회사 공유에 대한 데이터를 배치할 위치를 결정합니다. 선택 가능한 항목은 다음과 같습니다.

- Azure NetApp Files
- Azure 파일
- 기존 파일 서버(관리형 디스크가 있는 Azure VM)

#### NetApp VDS 배포 요구 사항(기존 구성 요소에 대한 배포 요구 사항)

기존 **Active Directory** 도메인 컨트롤러를 사용한 **NetApp VDS** 배포

이 구성 유형은 기존 Active Directory 도메인을 확장하여 AVD 인스턴스를 지원합니다. 이 경우 VDS는 제한된 구성 요소 집합을 도메인에 배포하여 AVD 구성 요소에 대한 자동 프로비저닝 및 관리 작업을 지원합니다.

이 구성에는 다음이 필요합니다.

- Azure VNET의 VM에서 액세스할 수 있는 기존 Active Directory 도메인 컨트롤러이며, 일반적으로 Azure에서 생성된 Azure VPN 또는 Express Route 또는 도메인 컨트롤러를 통해 액세스할 수 있습니다.
- vDS 구성 요소 및 사용 권한 추가 AVD 호스트 풀 및 데이터 볼륨을 도메인에 연결할 때 VDS 관리에 필요합니다. AVD VDS 구성 요소 및 사용 권한 가이드에서는 필요한 구성 요소와 사용 권한을 정의하고 배포 프로세스를 수행하려면 도메인 권한이 있는 도메인 사용자가 필요한 요소를 만드는 스크립트를 실행해야 합니다.
- VDS 배포는 VDS에서 생성된 VM에 대해 기본적으로 VNET를 생성합니다. VNET는 기존 Azure 네트워크 VNets로 피어링하거나 CWMGR1 VM을 필요한 서브넷이 미리 정의된 기존 VNET로 이동할 수 있습니다.

자격 증명 및 도메인 준비 도구

관리자는 배포 프로세스의 특정 시점에 도메인 관리자 자격 증명을 제공해야 합니다. 임시 도메인 관리자 자격 증명은 나중에 생성, 사용 및 삭제할 수 있습니다(배포 프로세스가 완료되면). 또는 필수 구성 요소 구축에 도움이 필요한 고객은 도메인 준비 도구를 활용할 수 있습니다.

기존 파일 시스템을 사용한 **NetApp VDS** 배포

VDS는 사용자 프로필, 개인 폴더 및 기업 데이터를 AVD 세션 VM에서 액세스할 수 있는 Windows 공유를 생성합니다. VDS는 기본적으로 파일 서버 또는 Azure NetApp 파일 옵션을 배포하지만, 기존 파일 저장소 구성 요소가 있는 경우 VDS 배포가 완료되면 VDS가 해당 구성 요소에 공유를 지정할 수 있습니다.

및 기존 스토리지 구성요소를 사용하기 위한 요구사항:

- 이 구성 요소는 SMB v3을 지원해야 합니다
- 구성 요소는 AVD 세션 호스트와 동일한 Active Directory 도메인에 연결해야 합니다
- 구성 요소는 VDS 구성에서 사용할 UNC 경로를 노출할 수 있어야 합니다. 즉, 세 공유 모두에 대해 하나의 경로를 사용하거나 각 경로에 대해 별도의 경로를 지정할 수 있습니다. VDS는 이러한 공유에 대한 사용자 수준 권한을 설정하므로 VDS AVD Components and Permissions(VDS AVD 구성 요소 및 권한) 문서를 참조하여 적절한

권한이 VDS Automation Services에 부여되었는지 확인합니다.

### NetApp VDS 배포와 기존 Azure AD 도메인 서비스

이 구성을 수행하려면 기존 Azure Active Directory 도메인 서비스 인스턴스의 속성을 식별하는 프로세스가 필요합니다. 이 유형의 배포를 요청하려면 계정 관리자에게 문의하십시오. NetApp VDS Deployment with existing AVD deployment 이 구성 형식은 필요한 Azure VNET, Active Directory 및 AVD 구성 요소가 이미 있다고 가정합니다. VDS 배포는 “기존 AD를 사용한 NetApp VDS 배포” 구성과 동일한 방식으로 수행되지만 다음과 같은 요구 사항이 추가됩니다.

- AVD 테넌트의 RD 소유자 역할은 Azure의 VDS 엔터프라이즈 응용 프로그램에 부여해야 합니다
- vDS Web App의 VDS 가져오기 기능을 사용하여 Avd 호스트 풀 및 AVD 호스트 풀 VM을 vDS로 가져와야 합니다 이 프로세스는 AVD 호스트 풀 및 세션 VM 메타데이터를 수집하고 VDS에 저장하여 이러한 요소를 VDS에서 관리할 수 있도록 합니다
- Avd 사용자 데이터는 CRA 도구를 사용하여 VDS 사용자 섹션으로 가져와야 합니다. 이 프로세스는 각 사용자에 대한 메타데이터를 VDS 컨트롤 평면에 삽입하여 AVD 앱 그룹 구성원 및 세션 정보를 VDS에서 관리할 수 있도록 합니다

#### 부록 A: VDS 컨트롤 플레인 URL 및 IP 주소

Azure 구독의 VDS 구성 요소는 VDS 웹 응용 프로그램 및 VDS API 끝점과 같은 VDS 글로벌 컨트롤 플레인 구성 요소와 통신합니다. 액세스하려면 포트 443에서 양방향 액세스에 대해 다음 기본 URI 주소를 안전 목록에 추가해야 합니다.

"" "" "" "" ""

액세스 제어 장치가 IP 주소로만 안전 목록만 할 수 있는 경우 다음 IP 주소 목록을 안전하게 나열해야 합니다. VDS는 Azure Traffic Manager 서비스를 사용하므로 시간이 지남에 따라 이 목록이 변경될 수 있습니다.

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.167 40.147.2 40.147.2 40.86.86.86.86.86.86.86.86.0.1622.1752.1722.17.22.172.17.22.116.22.118.22.1722.172.116.22.118.22.118.22.118.22.172.118.17.22.118.22.118.22.118.17.22.118.22.172.118.22.118.22.118.22.118.22.

#### 부록 B: Microsoft AVD 요구 사항

이 Microsoft AVD 요구 사항 섹션은 Microsoft의 AVD 요구 사항을 요약한 것입니다. 전체 및 현재 AVD 요구 사항은 다음 여기에서 확인할 수 있습니다.

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

### Azure Virtual Desktop 세션 호스트 라이센스

Azure Virtual Desktop은 다음 운영 체제를 지원하므로 배포하려는 데스크톱 및 앱을 기반으로 사용자에게 적합한 라이센스를 보유하고 있어야 합니다.

| OS | 필수 라이센스 |
| --- | --- |
| Windows 10 Enterprise 다중 세션 또는 Windows 10 Enterprise | Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5 |
| Windows 7 Enterprise | Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5 |

| OS | 필수 라이센스 |
| --- | --- |
| Windows Server 2012 R2, 2016, 2019년 | Software Assurance가 포함된 RDS CAL(클라이언트 액세스 라이선스 |

**AVD** 시스템의 **URL** 액세스

Azure Virtual Desktop용으로 생성한 Azure 가상 머신은 다음 URL에 대한 액세스 권한이 있어야 합니다.

| 주소 | 아웃바운드 **TCP** 포트 | 목적 | 서비스 태그 |
| --- | --- | --- | --- |
| .AVD.microsoft.com 으로 문의하십시오 | 443 | 서비스 트래픽 | WindowsVirtualDesktop을 참조하십시오 |
| mrsglobalsteus2prod.blob.core.windows.net | 443 | 에이전트 및 SxS 스택 업데이트 | AzureCloud를 참조하십시오 |
| .core.windows.net 으로 문의하십시오 | 443 | 상담원 트래픽 | AzureCloud를 참조하십시오 |
| .servicebus.windows.net 으로 문의하십시오 | 443 | 상담원 트래픽 | AzureCloud를 참조하십시오 |
| prod.warmpath.msftcloudes.com | 443 | 상담원 트래픽 | AzureCloud를 참조하십시오 |
| catalogartifact.azureedge.net | 443 | Azure 마켓플레이스 를 참조하십시오 | AzureCloud를 참조하십시오 |
| kms.core.windows.net | 1688)을 참조하십시오 | Windows 정품 인증 | 인터넷 |
| AVDportalstorageblob.blob.core.windows.net | 443 | Azure 포털 지원 | AzureCloud를 참조하십시오 |

다음 표에는 Azure 가상 시스템에서 액세스할 수 있는 선택적 URL이 나열되어 있습니다.

| 주소 | 아웃바운드 **TCP** 포트 | 목적 | 서비스 태그 |
| --- | --- | --- | --- |
| .microsoftonline.com 으로 문의하십시오 | 443 | MS 온라인 서비스에 대한 인증 | 없음 |
| .events.data.microsoft.com 으로 문의하십시오 | 443 | 원격 측정 서비스 | 없음 |
| www.msftconnecttest.com | 443 | OS가 인터넷에 연결되어 있는지 감지합니다 | 없음 |
| .prod.do.dsp.mp.microsoft.com 으로 문의하십시오 | 443 | Windows 업데이트 | 없음 |
| login.windows.net | 443 | MS Online Services, Office 365에 로그인합니다 | 없음 |
| *.sfx.ms | 443 | OneDrive 클라이언트 소프트웨어 업데이트 | 없음 |
| .digicert.com 으로 문의하십시오 | 443 | 인증서 해지 확인 | 없음 |

최적의 성능 요소

최적의 성능을 위해 네트워크가 다음 요구 사항을 충족하는지 확인하십시오.

- 클라이언트 네트워크에서 호스트 풀이 구축된 Azure 영역까지의 RTT(Round-Trip) 지연 시간은 150ms 미만이어야 합니다.
- 데스크톱 및 앱을 호스팅하는 VM이 관리 서비스에 연결되면 네트워크 트래픽이 국가/지역 경계 외부로 흐를 수 있습니다.
- 네트워크 성능을 최적화하기 위해 세션 호스트의 VM이 관리 서비스와 동일한 Azure 영역에 배치되도록 권장합니다.

지원되는 가상 머신 **OS** 이미지

Azure Virtual Desktop은 다음 x64 운영 체제 이미지를 지원합니다.

- Windows 10 Enterprise 다중 세션, 버전 1809 이상
- Windows 10 Enterprise, 버전 1809 이상
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop은 x86(32비트), Windows 10 Enterprise N 또는 Windows 10 Enterprise KN 운영 체제 이미지를 지원하지 않습니다. 또한 Windows 7은 섹터 크기 제한으로 인해 관리되는 Azure 스토리지에서 호스팅되는 VHD 또는 VHDX 기반 프로파일 솔루션을 지원하지 않습니다.

사용 가능한 자동화 및 구축 옵션은 다음 표와 같이 선택하는 OS와 버전에 따라 다릅니다.

| 운영 체제 | **Azure** 이미지 갤러리 | 수동 **VM** 배포 | **ARM** 템플릿 통합 | **Azure Marketplace**에서 호스트 풀을 프로비저닝합니다 |
|---|---|---|---|---|
| Windows 10 다중 세션, 버전 1903 | 예 | 예 | 예 | 예 |
| Windows 10 다중 세션, 버전 1809 | 예 | 예 | 아니요 | 아니요 |
| Windows 10 Enterprise, 버전 1903 | 예 | 예 | 예 | 예 |
| Windows 10 Enterprise, 버전 1809 | 예 | 예 | 아니요 | 아니요 |
| Windows 7 Enterprise | 예 | 예 | 아니요 | 아니요 |
| Windows Server 2019 | 예 | 예 | 아니요 | 아니요 |
| Windows Server 2016 | 예 | 예 | 예 | 예 |
| Windows Server 2012 R2 | 예 | 예 | 아니요 | 아니요 |

# 구글

## Google Cloud(GCP)용 RDS 구축 가이드

개요

이 가이드는 Google Cloud의 VDS(NetApp 가상 데스크톱 서비스)를 사용하여 원격 데스크톱 서비스(RDS) 배포를 생성하는 단계별 지침을 제공합니다.

이 POC(개념 증명) 가이드는 사용자가 자신의 테스트 GCP 프로젝트에 RDS를 빠르게 구축하고 구성하는 데 도움을 주기 위해 설계되었습니다.

특히 기존 AD 환경에 대한 프로덕션 배포는 매우 일반적이나 이 POC 가이드에서 이러한 프로세스는 고려되지 않습니다. 복잡한 POC 및 생산 배포는 NetApp VDS 영업/서비스 팀과 함께 시작되어야 하며 셀프 서비스 방식으로 수행되지 않습니다.

이 POC 문서는 전체 RDS 배포를 안내하며 VDS 플랫폼에서 사용할 수 있는 배포 후 구성의 주요 영역을 간략하게 설명합니다. 완료되면 세션 호스트, 응용 프로그램 및 사용자가 모두 포함된 완전한 배포 및 기능 RDS 환경을 갖게 됩니다. 선택적으로 자동 애플리케이션 전송, 보안 그룹, 파일 공유 권한, 클라우드 백업, 지능형 비용 최적화를 구성할 수 있습니다. VDS는 GPO를 통해 일련의 모범 사례 설정을 배포합니다. 이러한 컨트롤을 선택적으로 비활성화하는 방법에 대한 지침도 POC에 관리되지 않는 로컬 장치 환경과 유사한 보안 컨트롤이 필요하지 않은 경우에 포함됩니다.

구축 아키텍처

[너비 = 75%]

**RDS** 기초

VDS는 완전한 기능의 RDS 환경을 구축하며 필요한 모든 지원 서비스를 처음부터 새로 제공합니다. 이 기능에는 다음이 포함될 수 있습니다.

- RDS 게이트웨이 서버
- 웹 클라이언트 액세스 서버
- 도메인 컨트롤러 서버
- RDS 라이센스 서비스
- ThinPrint 라이센스 서비스
- FileZilla FTPS 서버 서비스입니다

가이드 범위

이 가이드에서는 GCP 및 VDS 관리자의 관점에서 NetApp VDS 기술을 사용하는 RDS 배포를 안내합니다. 사전 구성이 필요 없는 GCP 프로젝트를 제공하며 이 가이드를 통해 RDS의 엔드 투 엔드를 설정할 수 있습니다

서비스 계정을 생성합니다

1. GCP에서 _IAM 및 Admin > 서비스 계정 _ 으로 이동하거나 검색합니다

   []

2. 서비스 계정 생성 _ 을(를) 클릭합니다

   []

3. 고유한 서비스 계정 이름을 입력하고 _create_를 클릭합니다. 서비스 계정의 이메일 주소를 기록해 두십시오. 이 주소는 이후 단계에서 사용됩니다.

   []

4. 서비스 계정의 _Owner_role을 선택하고 _continue_를 클릭합니다

   []

5. 다음 페이지에서 변경할 필요가 없습니다(이 서비스 계정에 대한 사용자 액세스 권한 부여(선택 사항)). _Done_을 클릭합니다

   []

6. Service accounts_page에서 작업 메뉴를 클릭하고 _Create key_를 선택합니다

   []

7. P12_를 선택하고 _create_를 클릭합니다

   []

8. P12 파일을 다운로드하여 컴퓨터에 저장합니다. Private 키 password_changed를 리브 했습니다.

   []

   []

**Google** 컴퓨팅 **API**를 활성화합니다

1. GCP에서 _API & Services > Library_로 이동하거나 검색합니다

   []

2. GCP API 라이브러리에서 _Compute Engine API_로 이동하거나 검색합니다. _ENABLE_을 클릭합니다

   []

새 **VDS** 배포를 생성합니다

1. VDS에서 _Deployments_로 이동하여 _ + New Deployment_를 클릭합니다

   []

2. 배포 이름을 입력합니다

   []

3. Google Cloud Platform _ 을(를) 선택합니다

[]

알아봅니다

1. 프로젝트 ID_ 및 OAuth 이메일 주소를 입력합니다. 이 가이드의 앞부분에서 .p12 파일을 업로드하고 이 배포에 적합한 영역을 선택합니다. Test_를 클릭하여 항목이 올바르고 적절한 권한이 설정되었는지 확인합니다.

   OAuth 이메일은 이 가이드 앞부분에서 생성된 서비스 계정의 주소입니다.

   []

2. 확인이 완료되면 _Continue_를 클릭합니다

   []

계정

로컬 **VM** 계정

1. 로컬 관리자 계정의 암호를 입력합니다. 나중에 사용할 수 있도록 이 암호를 문서화합니다.
2. SQL SA 계정에 대한 암호를 제공합니다. 나중에 사용할 수 있도록 이 암호를 문서화합니다.

암호의 복잡성에는 대문자, 소문자, 숫자, 특수 문자 등 4가지 문자 유형 중 3개가 포함된 최소 8자의 문자가 필요합니다

**SMTP** 계정

VDS는 사용자 정의 SMTP 설정을 통해 이메일 알림을 전송할 수 있으며, 또는 _Automatic_을 선택하여 내장된 SMTP 서비스를 사용할 수 있습니다.

1. VDS에서 이메일 알림을 보낼 때 _from_address로 사용할 이메일 주소를 입력합니다. _no-reply@<your-domain>.com_은(는) 일반적인 형식입니다.
2. 성공 보고서를 보내야 하는 이메일 주소를 입력합니다.
3. 오류 보고서를 보내야 하는 이메일 주소를 입력합니다.

[]

레벨 **3** 정비사

레벨 3 정비사 계정(또는 *.tech accounts*)는 VDS 환경의 VM에서 관리 작업을 수행할 때 사용할 VDS 관리자의 도메인 수준 계정입니다. 이 단계 및/또는 그 이후에 추가 계정을 생성할 수 있습니다.

1. 레벨 3 관리자 계정의 사용자 이름과 암호를 입력합니다. 최종 사용자와 기술 계정을 구분하기 위해 입력하는 사용자 이름에 ".tech"가 추가됩니다. 나중에 사용할 수 있도록 이 자격 증명을 기록합니다.

   모범 사례는 환경에 대한 도메인 수준 자격 증명을 가져야 하는 모든 VDS 관리자에 대해 명명된 계정을 정의하는 것입니다. 이러한 유형의 계정이 없는 VDS 관리자는 VDS에 내장된 _Connect to server_functionality를 통해 VM 수준 관리자 액세스 권한을 가질 수 있습니다.

[]

도메인

활성 디렉토리

원하는 AD 도메인 이름을 입력합니다.

공용 도메인입니다

외부 액세스는 SSL 인증서를 통해 보호됩니다. 사용자 고유의 도메인 및 자체 관리되는 SSL 인증서를 사용하여 사용자 지정할 수 있습니다. 또는 _Automatic_을 선택하면 VDS에서 인증서의 자동 90일 새로 고침을 비롯한 SSL 인증서를 관리할 수 있습니다. 자동을 사용하는 경우 각 배포에서는 _cloudworkspace.app_의 고유한 하위 도메인을 사용합니다.

[]

가상 머신

RDS 배포의 경우 도메인 컨트롤러, RDS 브로커 및 RDS 게이트웨이와 같은 필수 구성 요소가 플랫폼 서버에 설치되어 있어야 합니다. 운영 환경에서 이러한 서비스는 전용 및 중복 가상 시스템에서 실행되어야 합니다. 개념 증명 배포를 위해 단일 VM을 사용하여 이러한 서비스를 모두 호스팅할 수 있습니다.

플랫폼 **VM** 구성

단일 가상 머신

이는 POC 배포를 위한 권장 선택 사항입니다. 단일 가상 시스템 배포에서 다음 역할은 모두 단일 VM에서 호스팅됩니다.

- CW Manager(CW 관리자)
- HTML5 게이트웨이
- RDS 게이트웨이
- 원격 앱
- FTPS 서버(옵션)
- 도메인 컨트롤러

이 구성에서 RDS 사용 사례에 권장되는 최대 사용자 수는 100명입니다. 로드 밸런싱된 RDS/HTML5 게이트웨이는 이 구성에서 옵션이 아니며 향후 확장을 위한 중복성과 옵션을 제한합니다.

이 환경이 멀티 테넌시를 위해 설계된 경우에는 단일 가상 시스템 구성이 지원되지 않습니다.

여러 대의 서버

VDS 플랫폼을 여러 가상 시스템으로 분할할 때 다음 역할은 전용 VM에서 호스팅됩니다.

- 원격 데스크탑 게이트웨이

  VDS 설정은 하나 또는 두 개의 RDS 게이트웨이를 배포하고 구성하는 데 사용할 수 있습니다. 이러한 게이트웨이는 열린 인터넷에서 구축 내의 세션 호스트 VM으로 RDS 사용자 세션을 중계합니다. RDS 게이트웨이는 중요한

기능을 처리하여 개방형 인터넷으로부터 직접 공격으로부터 RDS를 보호하고 환경 내/외부로 모든 RDS 트래픽을 암호화합니다. 두 개의 원격 데스크탑 게이트웨이를 선택하면 VDS Setup에서 두 개의 VM을 배포하고 들어오는 RDS 사용자 세션의 로드 밸런싱을 위해 구성합니다.

- HTML5 게이트웨이

  VDS Setup(VDS 설정)을 사용하여 하나 또는 두 개의 HTML5 게이트웨이를 배포 및 구성할 수 있습니다. 이러한 게이트웨이는 VDS 및 웹 기반 VDS 클라이언트(H5 Portal)의 _Connect to Server_feature에서 사용하는 HTML5 서비스를 호스팅합니다. HTML5 포털 2개를 선택한 경우 VDS Setup은 2개의 VM을 배포하고 들어오는 HTML5 사용자 세션의 로드 균형을 유지하도록 구성합니다.

  다중 서버 옵션을 사용하는 경우(사용자가 설치된 VDS 클라이언트를 통해서만 연결할 수 있는 경우에도) VDS에서 _Connect to Server_functionality를 활성화하려면 하나 이상의 HTML5 게이트웨이를 사용하는 것이 좋습니다.

- 게이트웨이 확장성 참고 사항

  RDS 사용 사례의 경우, 각 RDS 또는 HTML5 게이트웨이에서 약 500명의 사용자를 지원하는 추가 게이트웨이 VM을 사용하여 환경의 최대 크기를 확장할 수 있습니다. 최소 NetApp 프로페셔널 서비스 지원을 통해 추가 게이트웨이를 추가할 수 있습니다

이 환경이 멀티 테넌시를 위해 설계된 경우에는 _multiple servers_selection이 필요합니다.

서비스 역할

- Cwmgr1

  이 VM은 NetApp VDS 관리 VM입니다. SQL Express 데이터베이스, 도우미 유틸리티 및 기타 관리 서비스를 실행합니다. 단일 서버_배포에서 이 VM은 다른 서비스를 호스팅할 수도 있지만 _multiple server_configuration에서 이러한 서비스는 다른 VM으로 이동됩니다.

- CWPortal1(2)

  첫 번째 HTML5 게이트웨이 이름은 _CWPortal1_이며 두 번째 게이트웨이 이름은 _CWPortal2_입니다. 배포 시 하나 또는 두 개를 만들 수 있습니다. 배포 후 추가 서버를 추가하여 용량을 늘릴 수 있습니다(서버당 최대 500개의 연결).

- CWRDSGateway1(2)

  첫 번째 RDS 게이트웨이의 이름은 _CWRDSGateway1_이고, 두 번째는 _CWRDSGateway2_입니다. 배포 시 하나 또는 두 개를 만들 수 있습니다. 배포 후 추가 서버를 추가하여 용량을 늘릴 수 있습니다(서버당 최대 500개의 연결).

- 원격 앱

  앱 서비스는 RemotApp 응용 프로그램 호스팅을 위한 전용 컬렉션이지만 최종 사용자 세션 요청을 라우팅하고 RDWeb 응용 프로그램 구독 목록을 호스팅하는 데 RDS 게이트웨이와 해당 RDWeb 역할을 사용합니다. 이 서비스 역할에는 VM 전용 VM이 배포되지 않습니다.

- 도메인 컨트롤러

  배포에서 하나 또는 두 개의 도메인 컨트롤러를 자동으로 구축하고 VDS와 함께 작동하도록 구성할 수 있습니다.

[]

운영 체제

플랫폼 서버에 배포할 서버 운영 체제를 선택합니다.

시간대

원하는 시간대를 선택합니다. 플랫폼 서버는 이 시간으로 구성되며 로그 파일에는 이 시간대가 반영됩니다. 최종 사용자 세션은 이 설정에 관계없이 고유한 시간대를 반영합니다.

추가 서비스

**FTP**

VDS는 환경 내/외부로 데이터를 이동하기 위해 FTPS 서버를 실행하도록 FileZilla를 선택적으로 설치 및 구성할 수 있습니다. 이 기술은 구형이며 Google Drive와 같은 보다 현대적인 데이터 전송 방법을 사용하는 것이 좋습니다.

[]

네트워크

VM을 용도에 따라 다른 서브넷으로 분리하는 것이 가장 좋습니다.

네트워크 범위를 정의하고 A/20 범위를 추가합니다.

VDS Setup(VDS 설정)은 성공을 입증할 범위를 감지하고 제안합니다. 모범 사례에 따라 서브넷 IP 주소는 전용 IP 주소 범위에 속해야 합니다.

이러한 범위는 다음과 같습니다.

- 192.168.0.0 ~ 192.168.255.255
- 172.16.0.0 ~ 172.31.255.255
- 10.0.0.0 ~ 10.255.255.255

필요한 경우 검토 및 조정한 다음 유효성 검사 를 클릭하여 다음 각 서브넷에 대한 서브넷을 확인합니다.

- 테넌트: 세션 호스트 서버와 데이터베이스 서버가 상주할 범위입니다
- 서비스: Cloud Volumes Service와 같은 PaaS 서비스가 상주하는 범위입니다
- 플랫폼: 이 범위는 플랫폼 서버가 상주할 범위입니다
- 디렉토리: AD 서버가 상주할 범위입니다

[]

라이센싱

**SPLA** 번호

SPLA 번호를 입력하여 VDS가 보다 쉽게 SPLA RDS CAL 보고를 위해 RDS 라이선스 서비스를 구성할 수 있도록 합니다. 임시 번호(예: 12345)는 POC 배포를 위해 입력할 수 있지만 시험 기간(120일) 후 RDS 세션의 연결이

중지됩니다.

**SPLA** 제품

VDS 보고서에서 SPLA를 통해 라이선스를 취득한 모든 Office 제품에 대한 MAK 라이선스 코드를 입력하여 SPLA 보고를 단순화합니다.

**ThinPrint**

포함된 ThinPrint 라이센스 서버 및 라이센스를 설치하여 최종 사용자 프린터 리디렉션을 단순화하도록 선택합니다.

[]

검토 및 제공

모든 단계가 완료된 후 선택 항목을 검토한 후 환경을 검증 및 프로비저닝합니다.[]

다음 단계

이제 배포 자동화 프로세스에서 구축 마법사 전체에서 선택한 옵션이 포함된 새로운 RDS 환경을 구현합니다.

배포가 완료되면 여러 개의 이메일을 받게 됩니다. 작업이 완료되면 첫 번째 작업 영역을 위한 환경이 준비됩니다. 작업 공간에는 최종 사용자를 지원하는 데 필요한 세션 호스트와 데이터 서버가 포함됩니다. 1-2시간 후에 배포 자동화가 완료되면 이 가이드를 다시 참조하여 다음 단계를 수행하십시오.

새 프로비저닝 컬렉션을 생성합니다

컬렉션 프로비저닝은 vDS의 기능이며 VM 이미지의 생성, 사용자 정의 및 sysprep을 허용합니다. 작업 공간 배포로 들어가면 배포할 이미지가 필요하며 다음 단계를 통해 VM 이미지를 만들 수 있습니다.

배포용 기본 이미지를 만들려면 다음 단계를 수행하십시오**.**

1. Deployments > Provisioning Collections _ 로 이동하여 _Add_를 클릭합니다

   []

2. 이름과 설명을 입력합니다. CHOOSE_TYPE: Shared _.

   

   공유 또는 VDI를 선택할 수 있습니다. 공유는 세션 서버와 데이터베이스 같은 응용 프로그램에 대한 비즈니스 서버(선택 사항)를 지원합니다. VDI는 개별 사용자 전용의 VM용 단일 VM 이미지입니다.

3. Add_를 클릭하여 빌드할 서버 이미지의 유형을 정의합니다.

   []

4. TSData를 *SERVER ROLE*, 적절한 VM 이미지(이 경우 Server 2016) 및 원하는 스토리지 유형으로 선택합니다. 서버 추가 _ 를 클릭합니다

   []

5. 선택적으로 이 이미지에 설치할 응용 프로그램을 선택합니다.

   a. 사용 가능한 응용 프로그램 목록은 앱 라이브러리에서 채워집니다. 이 목록은 오른쪽 위 구석에 있는 _Settings > App Catalog_페이지 아래의 관리자 이름 메뉴를 클릭하여 액세스할 수 있습니다.

[]

6. Add Collection _ 을 클릭하고 VM이 구축될 때까지 기다립니다. VDS는 액세스 및 사용자 지정이 가능한 VM을 구성합니다.
7. VM 빌드가 완료되면 서버에 연결하고 원하는 대로 변경합니다.

   a. 상태가 _Collection Validation_으로 표시되면 컬렉션 이름을 클릭합니다.

      []

   b. 그런 다음 _ 서버 템플릿 이름 _ 을(를) 클릭합니다

      []

   c. 마지막으로, *Connect to Server* 단추를 클릭하여 연결하고 로컬 관리자 자격 증명으로 VM에 자동으로 로그인합니다.

      []

   []

8. 모든 사용자 정의가 완료되면 _Validate Collection_을 클릭하여 VDS가 sysprep을 수행하고 이미지를 완료할 수 있도록 합니다. 완료되면 VM이 삭제되고 VDS 배포 마법사 내에서 이미지를 배포 양식에 사용할 수 있습니다.

   []5

## 새 작업 영역을 만듭니다

작업 영역은 사용자 그룹을 지원하는 세션 호스트 및 데이터 서버의 모음입니다. 배포에는 단일 작업 공간(단일 테넌트) 또는 여러 작업 공간(멀티 테넌트)이 포함될 수 있습니다.

작업 영역은 특정 그룹에 대한 RDS 서버 컬렉션을 정의합니다. 이 예에서는 가상 데스크톱 기능을 시연하기 위해 단일 컬렉션을 구축합니다. 그러나 동일한 Active Directory 도메인 공간 내에서 서로 다른 그룹 및 위치를 지원하기 위해 모델을 여러 작업 공간/RDS 컬렉션으로 확장할 수 있습니다. 선택적으로 관리자는 작업 영역/컬렉션 간의 액세스를 제한하여 응용 프로그램과 데이터에 대한 제한된 액세스가 필요한 사용 사례를 지원할 수 있습니다.

### 클라이언트 및 설정

1. NetApp VDS에서 _Workspaces_로 이동하고 _ + New Workspace _ 를 클릭합니다

   []

2. Add_를 클릭하여 새 클라이언트를 생성합니다. 클라이언트 세부 정보는 일반적으로 회사 정보 또는 특정 위치/부서에 대한 정보를 나타냅니다.

   []

   a. 회사 세부 정보를 입력하고 이 작업 영역을 배포할 배포를 선택합니다.
   b. * 데이터 드라이브: * 회사 공유 매핑된 드라이브에 사용할 드라이브 문자를 정의합니다.
   c. * 사용자 홈 드라이브: * 개별 매핑된 드라이브에 사용할 드라이브 문자를 정의합니다.
   d. * 추가 설정 *

배포 및/또는 배포 후 선택 시 다음 설정을 정의할 수 있습니다.

i. _원격 앱 활성화: _ 원격 앱은 전체 원격 데스크톱 세션을 제공하는 대신 스트리밍 응용 프로그램으로 응용 프로그램을 제공합니다(또는 추가).

ii. _Enable App Locker: _ VDS에는 응용 프로그램 배포 및 권한 기능이 포함되어 있으며 기본적으로 시스템은 최종 사용자에게 응용 프로그램을 표시하거나 숨깁니다. App Locker를 활성화하면 GPO 허용 목록을 통해 응용 프로그램 액세스가 적용됩니다.

iii. _작업 공간 사용자 데이터 저장소 사용: _ 최종 사용자가 가상 데스크톱에서 데이터 저장소 액세스 권한이 있어야 하는지 여부를 결정합니다. RDS 배포의 경우 사용자 프로필에 대한 데이터 액세스를 활성화하려면 이 설정을 항상 선택해야 합니다.

iv. _프린터 액세스 비활성화: _VDS는 로컬 프린터에 대한 액세스를 차단할 수 있습니다.

v. _작업 관리자에 대한 액세스 허용: _VDS는 Windows의 작업 관리자에 대한 최종 사용자 액세스를 활성화/비활성화할 수 있습니다.

vi. _복잡한 사용자 암호 필요: _ 복잡한 암호를 필요로 하면 네이티브 Windows Server 복잡한 암호 규칙이 활성화됩니다. 또한 잠긴 사용자 계정의 시간 지연 자동 잠금 해제를 비활성화합니다. 따라서 이 옵션을 설정하면 최종 사용자가 암호를 여러 번 시도하여 계정을 잠글 때 관리자 개입이 필요합니다.

vii. _모든 사용자에 대해 MFA 활성화:_VDS에는 최종 사용자 및/또는 VDS 관리자 계정 액세스를 보호하는 데 사용할 수 있는 무료 이메일/SMS MFA 서비스가 포함되어 있습니다. 이를 활성화하려면 이 작업 영역의 모든 최종 사용자가 MFA를 사용하여 인증하여 데스크톱 및/또는 앱에 액세스해야 합니다.

응용 프로그램을 선택합니다

이 가이드 앞부분에서 생성한 Windows OS 버전 및 프로비저닝 컬렉션을 선택합니다.

이 시점에서 추가 응용 프로그램을 추가할 수 있지만 이 POC의 경우 배포 후 응용 프로그램 자격 요건에 대해 다루겠습니다.

[]

사용자 추가

기존 AD 보안 그룹 또는 개별 사용자를 선택하여 사용자를 추가할 수 있습니다. 이 POC 가이드에서는 배포 후 사용자를 추가할 것입니다.

[]

검토 및 제공

마지막 페이지에서 선택한 옵션을 검토하고 _provision_을 클릭하여 RDS 리소스 자동 빌드를 시작합니다.

[]

배포 프로세스 중에 로그가 생성되며 배포 세부 정보 페이지 아래쪽에 있는 _Task History_에서 액세스할 수 있습니다. VDS > 배포에서 배포 이름 _ 으로 이동하여 액세스할 수 있습니다

다음 단계

WorkPlace 자동화 프로세스가 이제 구축 마법사 전체에서 선택한 옵션이 포함된 새로운 RDS 리소스를 배포합니다.

이 작업이 완료되면 일반적인 RDS 구축 환경을 사용자 지정하기 위해 따라야 할 몇 가지 워크플로우가 있습니다.

- "사용자 추가"
- "최종 사용자 액세스"
- "응용 프로그램 소유 권한"
- "비용 최적화"

## Google Compute Platform(GCP) 및 VDS 사전 요구 사항

### GCP 및 VDS 요구 사항 및 참고 사항

이 문서에서는 VDS(NetApp 가상 데스크톱 서비스)를 사용하여 RDS(원격 데스크톱 서비스)를 배포하는 데 필요한 요소에 대해 설명합니다. "빠른 점검 목록"에서는 효율적인 배포를 위해 필요한 구성 요소 및 배포 전 단계에 대한 간단한 목록을 제공합니다. 이 가이드의 나머지 부분에서는 선택한 구성에 따라 각 요소에 대해 더 자세히 설명합니다.

[너비 = 75%]

빠른 점검 목록

#### GCP 요구사항

- GCP 테넌트
- GCP 프로젝트
- 소유자 역할이 할당된 서비스 계정

#### 배포 전 정보

- 총 사용자 수를 결정합니다
- GCP 지역 및 지역을 결정합니다
- Active Directory 유형을 확인합니다
- 스토리지 유형을 확인합니다
- 세션 호스트 VM 이미지 또는 요구 사항을 식별합니다
- 기존 GCP 및 온프레미스 네트워킹 구성을 평가합니다

### VDS 배포 세부 요구 사항

#### 최종 사용자 연결 요구 사항

다음 원격 데스크톱 클라이언트는 **GCP**에서 **RDS**를 지원합니다**.**

- "Windows용 NetApp VDS 클라이언트"
  - Windows 아웃바운드 URL 안전 상장용 NetApp VDS 클라이언트 요구 사항
    - api.cloudworkspace.com
    - vdsclient.app
    - api.vdsclient.app
    - bin.vdsclient.app

    - 향상된 기능:
        - VDS 필요할 때 깨우기를 사용합니다
        - ThinPrint 클라이언트 및 lice ning
        - 셀프 서비스 암호 재설정
        - 자동 서버 및 게이트웨이 주소 협상
        - 완벽한 데스크탑 및 스트리밍 애플리케이션 지원
        - 사용 가능한 사용자 지정 브랜딩
        - 자동 배포 및 구성을 위한 설치 관리자 스위치
        - 문제 해결 도구가 내장되어 있습니다
- "NetApp VDS 웹 클라이언트"
- "Microsoft RD 클라이언트"
    - Windows
    - macOS
    - ISO
    - Android
- 타사 소프트웨어 및/또는 씬 클라이언트
    - 요구 사항: RD 게이트웨이 구성을 지원합니다

지원합니다

VDS에서 배포된 RDS의 경우 저장소 전략은 AVD 세션 VM에 영구 사용자/회사 데이터가 없도록 설계되었습니다. 사용자 프로필, 사용자 파일 및 폴더, 회사/애플리케이션 데이터에 대한 영구 데이터는 독립 데이터 계층에서 호스팅되는 하나 이상의 데이터 볼륨에 호스팅됩니다.

FSLogix는 세션 초기화 시 사용자 프로필 컨테이너(VHD 또는 VHDX 형식)를 세션 호스트에 마운트하여 데이터 스프롤 및 느린 로그인과 같은 다양한 사용자 프로필 문제를 해결하는 프로파일 컨테이너화 기술입니다.

이 아키텍처로 인해 데이터 저장 기능이 필요합니다. 이 기능은 사용자의 상당 부분이 동시에 로그인/로그오프하는 경우 매일 아침/오후에 필요한 데이터 전송을 처리할 수 있어야 합니다. 중간 규모의 환경에서도 상당한 데이터 전송 요구사항이 있을 수 있습니다. 데이터 스토리지 계층의 디스크 성능은 기본 최종 사용자 성능 변수 중 하나이므로 스토리지 용량뿐만 아니라 스토리지 성능의 크기를 적절하게 조정할 수 있도록 특별히 주의를 기울여야 합니다. 일반적으로 스토리지 계층의 크기는 사용자당 5-15 IOPS를 지원하도록 조정해야 합니다.

네트워킹

- 필수: * VPN을 통해 GCP 프로젝트에 표시되는 서브넷을 포함하여 기존의 모든 네트워크 서브넷의 인벤토리. 배포는 중복되는 서브넷을 피해야 합니다.

VDS 설정 마법사를 사용하면 기존 네트워크와의 계획된 통합의 일부로 필요한 범위 또는 피해야 할 범위가 있는 경우 네트워크 범위를 정의할 수 있습니다.

배포 중에 사용자에게 IP 범위를 결정합니다. 모범 사례에 따라 전용 범위의 IP 주소만 지원됩니다.

지원되는 선택 항목은 다음과 같지만 기본적으로 **A/20** 범위입니다**.**

- 192.168.0.0 ~ 192.168.255.255
- 172.16.0.0 ~ 172.31.255.255
- 10.0.0.0 ~ 10.255.255.255

**CWMGR1**

비용 절감 워크로드 스케줄링 및 라이브 확장 기능과 같은 VDS의 고유한 기능 중 일부는 조직 및 프로젝트 내에서 관리 기능을 필요로 합니다. 따라서 CWMGR1이라는 관리 VM은 VDS 설정 마법사 자동화의 일부로 배포됩니다. 이 VM은 VDS 자동화 작업 외에도 SQL Express 데이터베이스, 로컬 로그 파일 및 DCConfig라는 고급 구성 유틸리티에서 VDS 구성을 유지합니다.

**VDS** 설정 마법사에서 선택한 항목에 따라 이 **VM**을 사용하여 다음을 포함한 추가 기능을 호스팅할 수 있습니다**.**

- RDS 게이트웨이
- HTML 5 게이트웨이
- RDS 라이센스 서버입니다
- 도메인 컨트롤러

배포 마법사의 의사 결정 트리 구조

초기 배포의 일부로 새로운 환경에 대한 설정을 사용자 지정하기 위한 일련의 질문에 대한 답변이 제공됩니다. 다음은 결정해야 할 주요 결정 사항에 대한 개요입니다.

**GCP** 지역

VDS 가상 컴퓨터를 호스팅할 GCP 지역 또는 지역을 결정합니다. 이 지역은 최종 사용자와 이용 가능한 서비스에 근접하여 선택해야 합니다.

데이터 스토리지

사용자 프로필, 개별 파일 및 회사 공유에 대한 데이터를 배치할 위치를 결정합니다. 선택 가능한 항목은 다음과 같습니다.

- GCP용 Cloud Volumes Service
- 기존 파일 서버

**NetApp VDS** 배포 요구 사항**(**기존 구성 요소에 대한 배포 요구 사항**)**

기존 **Active Directory** 도메인 컨트롤러를 사용한 **NetApp VDS** 배포

이 구성 유형은 기존 Active Directory 도메인을 확장하여 RDS 인스턴스를 지원합니다. 이 경우 VDS는 RDS 구성 요소에 대한 자동 프로비저닝 및 관리 작업을 지원하기 위해 제한된 구성 요소 집합을 도메인에 배포합니다.

이 구성에는 다음이 필요합니다**.**

- 일반적으로 GCP에서 생성된 VPN 또는 도메인 컨트롤러를 통해 GCP VPC 네트워크의 VM에서 액세스할 수 있는 기존 Active Directory 도메인 컨트롤러입니다.
- 도메인에 가입되어 있는 RDS 호스트 및 데이터 볼륨의 VDS 관리에 필요한 VDS 구성 요소 및 사용 권한 추가. 배포 프로세스를 수행하려면 도메인 권한이 있는 도메인 사용자가 필요한 요소를 만드는 스크립트를 실행해야 합니다.
- VDS 배포는 기본적으로 VDS에서 생성된 VM에 대해 VPC 네트워크를 생성합니다. VPC 네트워크는 기존 VPC

네트워크를 통해 피어링하거나 CWMGR1 VM을 필요한 서브넷이 미리 정의된 기존 VPC 네트워크로 이동할 수 있습니다.

자격 증명 및 도메인 준비 도구

관리자는 배포 프로세스의 특정 시점에 도메인 관리자 자격 증명을 제공해야 합니다. 임시 도메인 관리자 자격 증명은 나중에 생성, 사용 및 삭제할 수 있습니다(배포 프로세스가 완료되면). 또는 필수 구성 요소 구축에 도움이 필요한 고객은 도메인 준비 도구를 활용할 수 있습니다.

기존 파일 시스템을 사용한 **NetApp VDS** 배포

VDS는 사용자 프로필, 개인 폴더 및 기업 데이터를 RDS 세션 호스트에서 액세스할 수 있도록 하는 Windows 공유를 생성합니다. VDS는 기본적으로 파일 서버를 배포하지만 기존 파일 저장소 구성 요소가 있는 경우 VDS 배포가 완료되면 VDS가 해당 구성 요소에 공유를 지정할 수 있습니다.

및 기존 스토리지 구성요소를 사용하기 위한 요구사항**:**

- 이 구성 요소는 SMB v3을 지원해야 합니다
- 구성 요소는 RDS 세션 호스트와 동일한 Active Directory 도메인에 연결해야 합니다.
- 구성 요소는 VDS 구성에서 사용할 UNC 경로를 노출할 수 있어야 합니다. 즉, 세 공유 모두에 대해 하나의 경로를 사용하거나 각 경로에 대해 별도의 경로를 지정할 수 있습니다. VDS는 이러한 공유에 대한 사용자 수준 권한을 설정하고 VDS Automation Services에 적절한 권한이 부여되었는지 확인합니다.

부록 **A: VDS** 컨트롤 플레인 **URL** 및 **IP** 주소

GCP 프로젝트의 VDS 구성 요소는 VDS 웹 응용 프로그램 및 VDS API 끝점을 포함하여 Azure에서 호스팅되는 VDS 글로벌 컨트롤 플레인 구성 요소와 통신합니다. 액세스하려면 포트 443에서 양방향 액세스에 대해 다음 기본 URI 주소를 안전 목록에 추가해야 합니다.

"" "" "" ""

액세스 제어 장치가 IP 주소로만 안전 목록만 할 수 있는 경우 다음 IP 주소 목록을 안전하게 나열해야 합니다. VDS는 이중화된 공용 IP 주소가 있는 로드 밸런서를 사용하므로 시간이 지남에 따라 이 목록이 변경될 수 있습니다.

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.136.91 40.122.119.157 40.78.132.166 40.78.129.17 40.122.167 40.147.2 40.147.2 40.86.86.86.86.86.86.86.86.0.1622.1752.1722.17.22.172.17.22.116.22.118.22.1722.172.116.22.118.22.118.22.118.22.172.118.17.22.118.22.118.22.118.17.22.118.22.172.118.22.118.22.118.22.118.22.

최적의 성능 요소

최적의 성능을 위해 네트워크가 다음 요구 사항을 충족하는지 확인하십시오.

- 클라이언트 네트워크에서 세션 호스트가 구축된 GCP 영역까지의 RTT(Round-Trip) 지연 시간은 150ms 미만이어야 합니다.
- 데스크톱 및 앱을 호스팅하는 VM이 관리 서비스에 연결되면 네트워크 트래픽이 국가/지역 경계 외부로 흐를 수 있습니다.
- 네트워크 성능을 최적화하기 위해 세션 호스트의 VM이 관리 서비스와 동일한 영역에 배치되도록 권장합니다.

VDS에서 배포된 RDS 세션 흐트는 다음 x64 운영 체제 이미지를 지원합니다.

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2