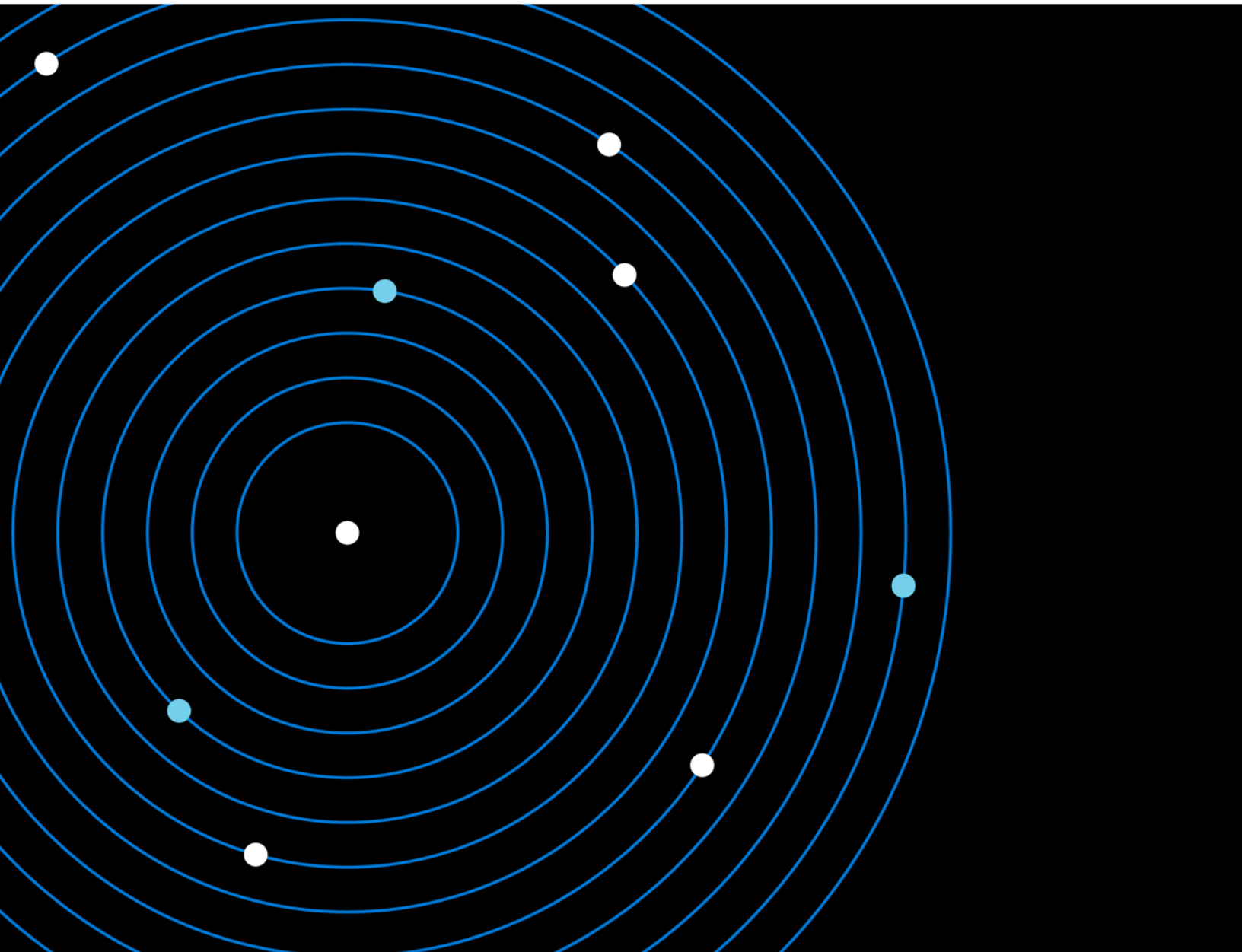
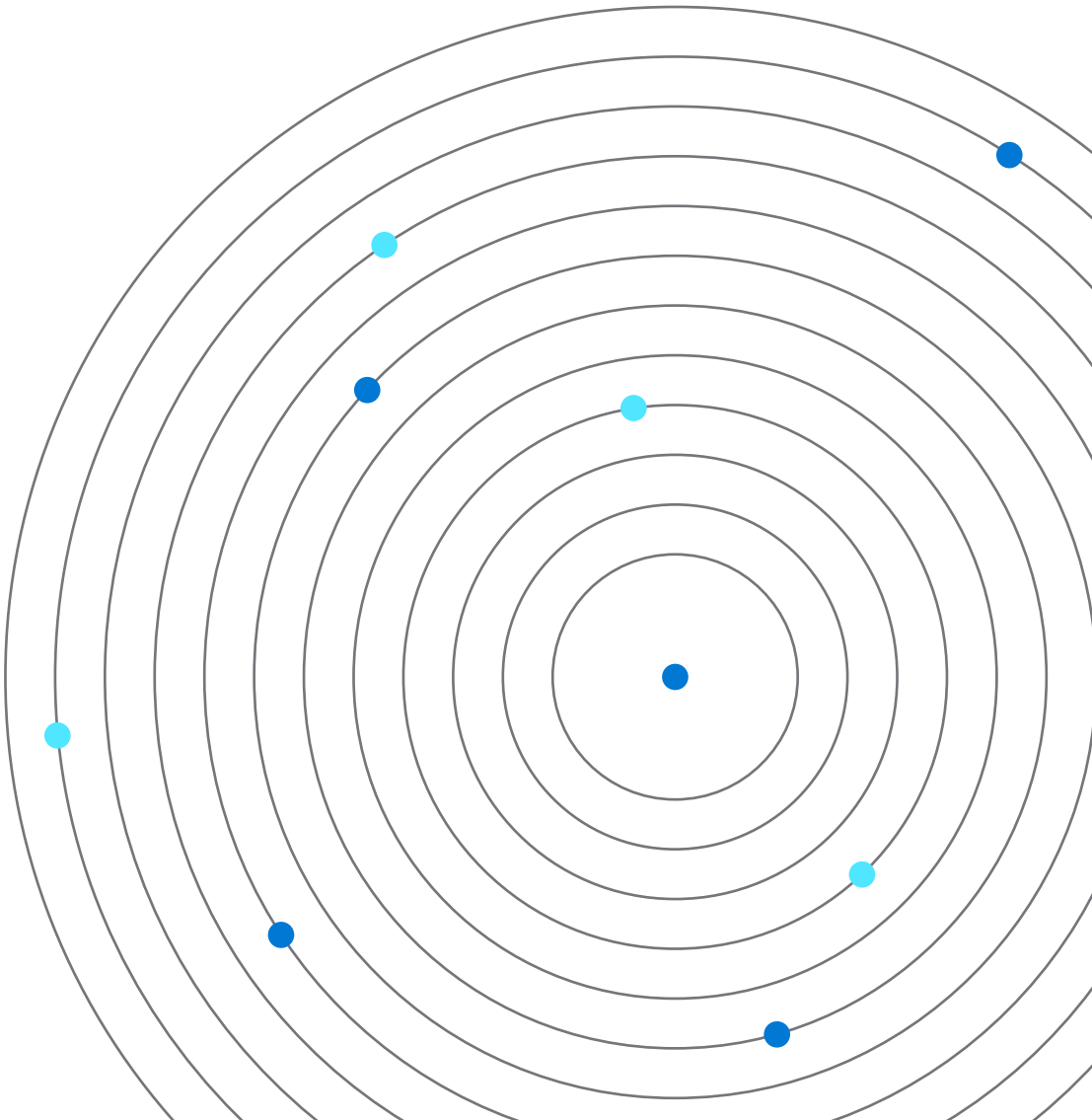
Azure eBook 시리즈

Microsoft Azure

Azure Virtual Desktop 핸드북: 보안 기초



Contents



소개

Azure Virtual Desktop을 통해 조직의 원격 근무 환경을 구축하는 여정을 진행하는 과정에서 사용자를 안전하게 보호하기 위해 따라야 할 보안 책임, 기능 및 모범 사례를 이해하는 것이 중요합니다.

이 핸드북은 Azure Virtual Desktop 환경에서 보안 기능을 환경 설정하는 프로세스를 안내합니다. 각 섹션은 특정 영역을 중점적으로 다루며 독립적으로 구현될 수 있지만, 귀사의 엔드 투 엔드 Azure Virtual Desktop 보안 전략에 도움이 되도록 전체 핸드북을 읽는 것이 좋습니다.

Azure Virtual Desktop 개요

Azure Virtual Desktop은 클라우드에서 실행되는 포괄적인 데스크톱 및 앱 가상화 서비스로, 어디서나 안전한 원격 데스크톱 환경을 제공하여 조직이 비즈니스 회복탄력성을 강화할 수 있도록 지원합니다. 관리 간소화, Windows 10 다중 세션, 기업용 Microsoft 365 앱의 최적화, RDS(원격 데스크톱 서비스) 환경 마이그레이션 지원 등을 제공합니다. 또한 Azure Virtual Desktop을 활용하면 Azure에서 Windows 데스크톱과 앱을 몇 분 안에 배포하고 확장할 수 있으며, 내장 보안 및 규정 준수 기능으로 앱과 데이터의 보안을 유지할 수 있습니다.

Azure Virtual Desktop은 PaaS(Platform as a Service)를 기반으로 하므로, 인프라와 관련된 많은 솔루션을 Microsoft에서 사용자 대신 관리합니다. 데스크톱 및 애플리케이션 워크로드와 관련된 다른 부분은 고객 또는 파트너가 관리합니다.

그림 *1*은 네 개의 서로 다른 버킷에 결합된 구성 요소를 보여 줍니다. **Azure Virtual Desktop 서비스** 및 **Azure 인프라** 버킷은 Microsoft에서 관리합니다. **데스크톱 및 원격 앱**과 **관리 및 정책** 버킷은 사용자가 관리하므로 세션 호스트 서버 및 애플리케이션 환경을 제어할 수 있는 유연성을 선사합니다.

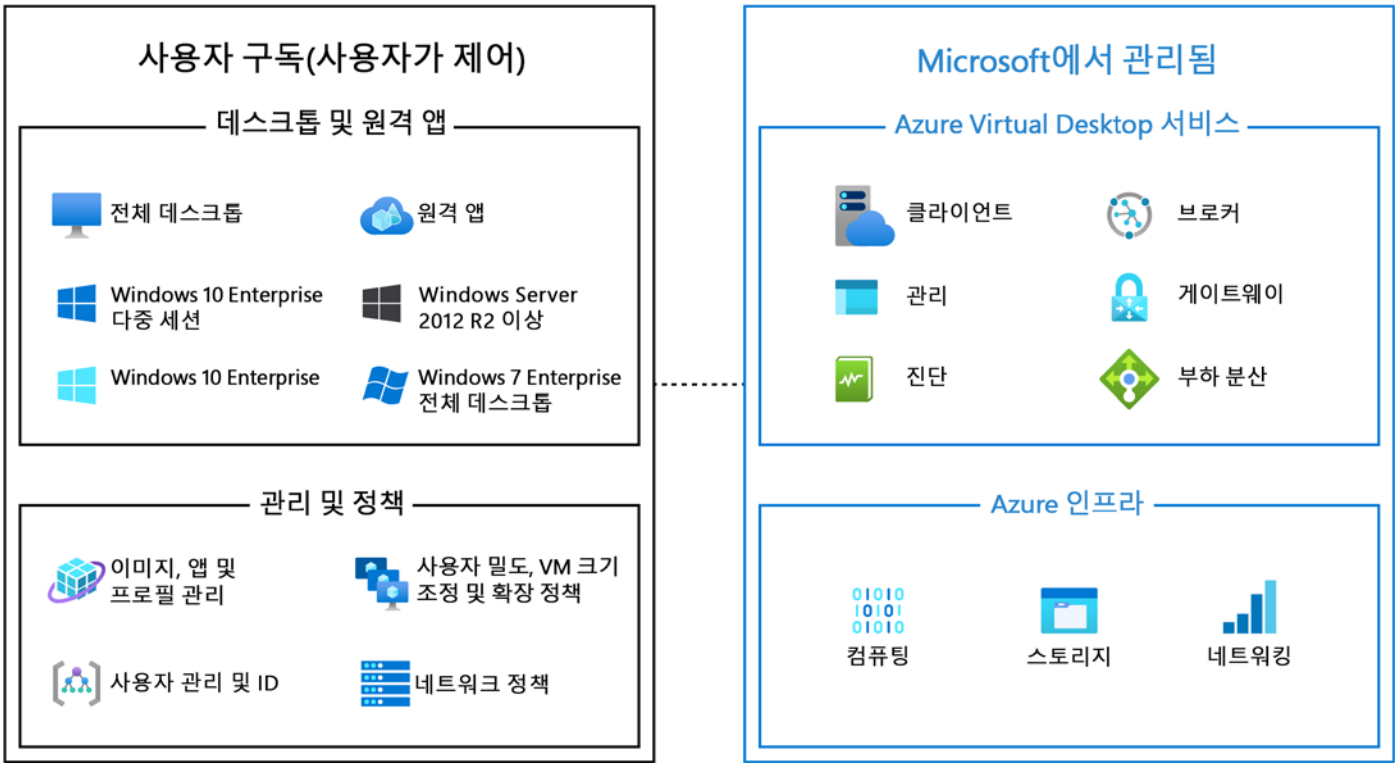


그림 1: Azure Virtual Desktop 구성 요소 및 책임

그림 *2*는 Azure Virtual Desktop의 엔터프라이즈 환경의 일반적인 아키텍처 설정을 보여 줍니다.

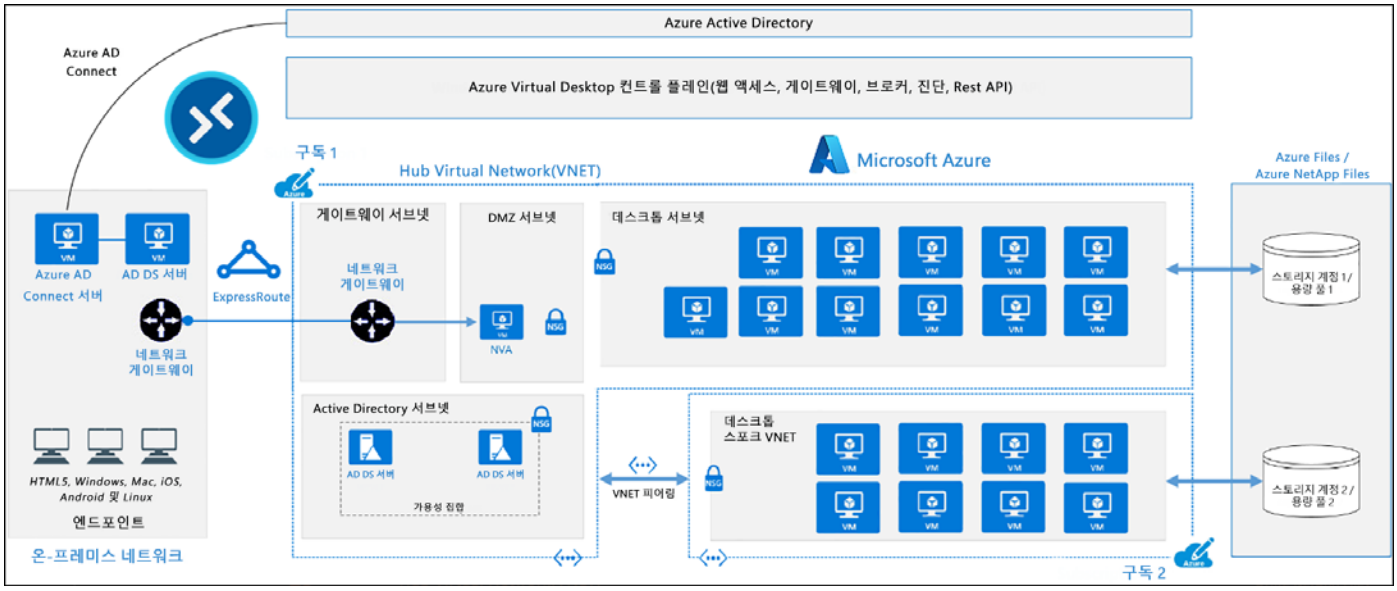


그림 2: 일반적인 Azure Virtual Desktop 아키텍처 설정

애플리케이션의 백 엔드 구성 요소는 고객의 온-프레미스 네트워크에 있습니다. ExpressRoute를 통해 온-프레미스 네트워크를 Azure 클라우드로 확장합니다. 선택적으로 데이터 센터 마이그레이션 시나리오에 따라 백 엔드 구성 요소를 Azure로 마이그레이션할 수도 있습니다. Azure AD Connect 구성 요소는 Active Directory Domain Services(AD DS)의 ID와 Azure AD를 동기화합니다. Azure Active Directory Domain Services(Azure AD DS)를 사용하는 경우에는 ID가 Azure AD에서 Azure AD DS로 자동으로 동기화됩니다. 고객은 AD DS 및 Azure AD, Azure 구독, 가상 네트워크, Azure Files 또는 Azure NetApp Files 및 Azure Virtual Desktop 호스트 풀 및 워크스페이스를 관리합니다.

Azure Virtual Desktop 서비스 아키텍처는 Windows Server 원격 데스크톱 서비스와 유사합니다. Azure Virtual Desktop에서 Microsoft는 인프라 및 중개 구성 요소를 관리하고 기업 고객은 자체 데스크톱 호스트 VM(가상 머신), 데이터 및 클라이언트를 관리합니다. 따라서 실제로 사용자는 그들에게 중요한 최종 사용자 환경에 더욱 주력할 수 있습니다. 온-프레미스 RDS, Azure로의 마이그레이션 및 Azure Virtual Desktop으로 마이그레이션 간의 차이점을 이해하려면 그림 *3*을 살펴보세요.

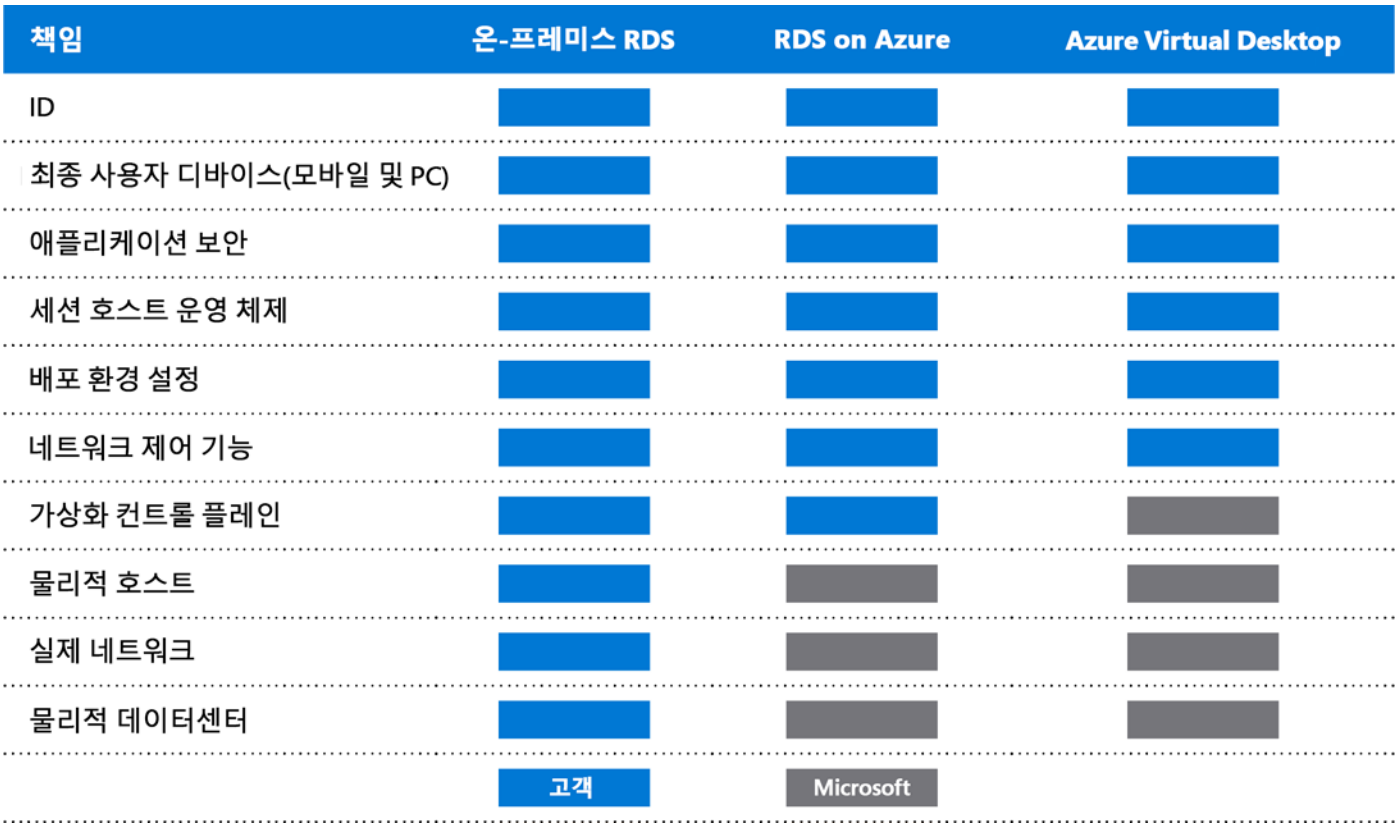


그림 3: 책임

기업용 Azure Virtual Desktop에 대한 자세한 내용은 이 페이지를 방문하세요.

Microsoft 및 고객 보안 책임

일반적으로 특정 보안 책임과 관련하여 온-프레미스 Virtual Desktop Infrastructure(VDI) 배포에서 보안의 모든 측면은 고객이 책임집니다. Azure Virtual Desktop에서는 이러한 책임을 고객과 Microsoft가 공동으로 책임집니다.

그림 *4*는 Microsoft와 고객으로 나뉜 Azure Virtual Desktop에 대한 보안 책임을 보여 줍니다.

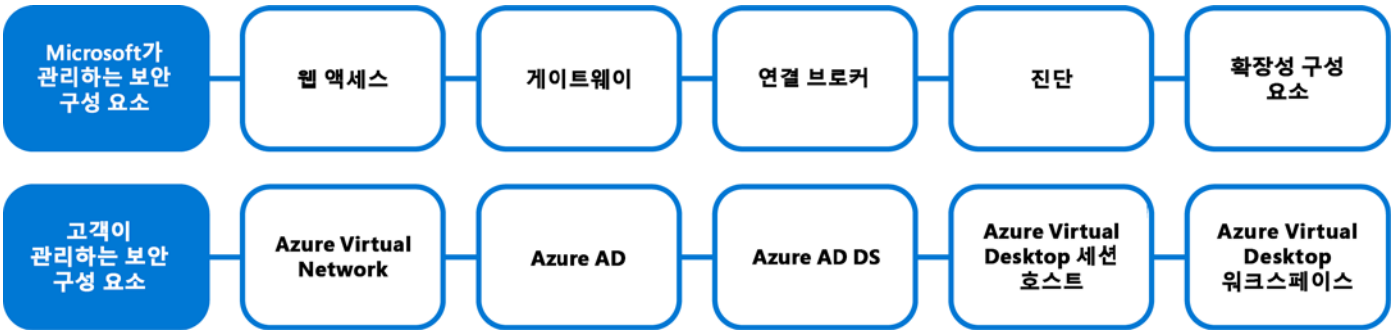


그림 4: 보안 구성 요소 책임

이러한 구성 요소에 대한 자세한 내용은 Azure Virtual Desktop 구성 요소 관리에 대한 설명을 참조하세요.

Azure Virtual Desktop을 이용할 때 유의할 점은 Microsoft가 이미 일부 서비스의 보안을 확보한 상태라는 것입니다. Microsoft는 Azure에서 실행되는 물리적 데이터센터, 물리적 네트워크 및 물리적 호스트를 보호합니다. 또한 Microsoft는 Azure에서 실행되는 Azure Virtual Desktop 서비스가 포함된 가상화 컨트롤 플레인을 보호에 대한 책임이 있습니다. 조직의 보안 요구 사항에 맞게 다른 영역을 환경 설정해야 합니다. 이 핸드북에서는 귀사가 담당하는 서비스 내의 보안 영역을 환경 설정하고 최적화하는 데 도움이 되는 지침과 모범 사례를 제공합니다.

그림 5는 이 핸드북에서 다루는 여러 가지 보안 핵심 요소를 보여 줍니다.

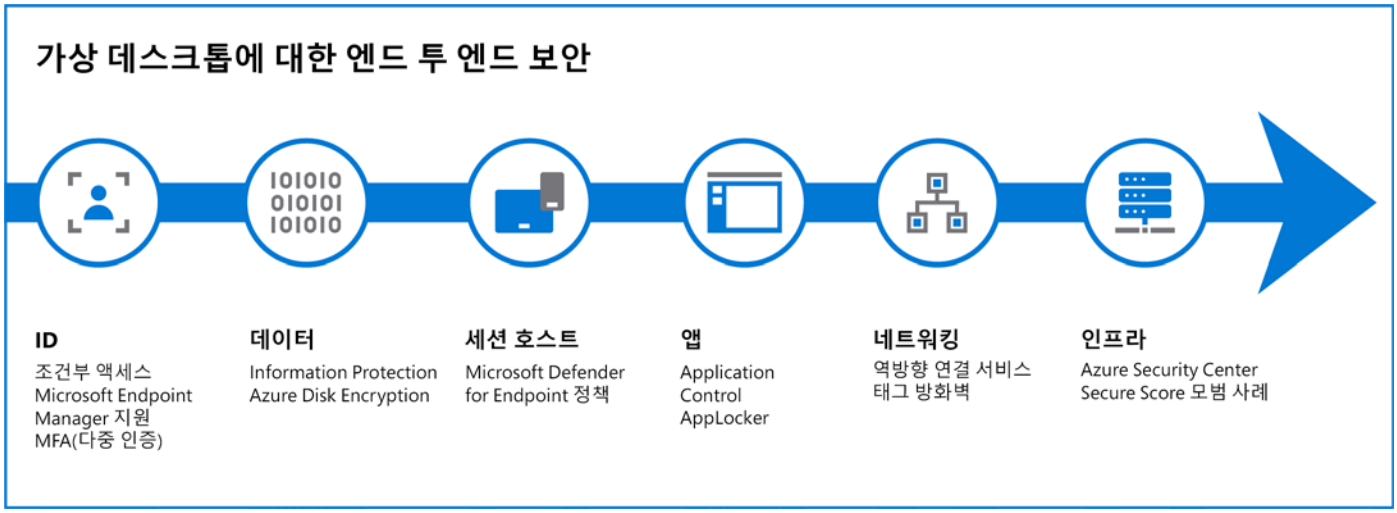


그림 5: Azure Virtual Desktop 보안 정보 및 이벤트 관리

사용자 ID 보호

이 챕터는 Azure Virtual Desktop 서비스 내의 다양한 영역에서 보안 기능을 환경 설정하는 프로세스를 안내합니다. 각 챕터는 특정 영역을 다루고 있으며 독립적으로 구현될 수 있지만, 모든 챕터를 읽고 다양한 보안 측면을 숙지하는 것이 좋습니다.

이 챕터에서는 사용자의 ID와 관련된 보안 환경 설정을 다룹니다. 사용자 개인 인증 정보, 조건부 액세스 적용 방법 및 감사 로그를 수집하는 방법에 대해 살펴보겠습니다.

사용자 개인 인증 정보

Azure Virtual Desktop용 Windows 클라이언트는 Azure Virtual Desktop을 로컬 컴퓨터와 통합할 수 있는 훌륭한 옵션입니다. 그러나 Azure Virtual Desktop 계정을 Windows 클라이언트로 환경 설정할 때 본인을 포함하여 사용자의 안전을 유지하기 위해 특정 조치를 취해야 합니다.

처음 로그인하면 클라이언트가 사용자 이름과 암호를 요청합니다. 그러면 다음에 로그인할 때 클라이언트는 Azure AD 엔터프라이즈 애플리케이션에서 토큰을 기억합니다. 세션 호스트의 개인 인증 정보를 묻는 메시지에서 **사용자 이름 및 암호 저장**을 선택한 경우 사용자가 클라이언트를 다시 시작할 때 개인 인증 정보를 다시 입력하지 않고도 로그인이 가능합니다. 해당 개인 인증 정보는 로컬 인증 정보 관리자에 저장됩니다. 개인 인증 정보를 저장해서 사용하면 편리하지만 엔터프라이즈 시나리오 또는 개인 디바이스에 배포하는 경우 보안이 저하될 수 있습니다. 사용자를 보호하려면 Azure Virtual Desktop에 대한 조건부 액세스 정책을 환경 설정하여 클라이언트가 Azure 다중 개인 인증 정보를 더 자주 요청하도록 할 수 있습니다.

조건부 액세스

조건부 액세스는 Azure AD에서 신호를 모아 의사 결정을 내리고 조직 정책을 적용하는 데 이용하는 도구입니다. 조건부 액세스는 새로운 ID 기반 컨트롤 플레인의 핵심입니다. 가장 간단한 조건부 액세스 정책은 if-then 문으로, 사용자가 특정 리소스에 액세스하려면 하나 이상의 작업을 완료해야 한다는 내용입니다. Azure Virtual Desktop에 대한 조건부 액세스 정책을 활용하면 필요할 때 적절한 액세스 제어를 적용하여 조직의 보안을 유지하고, 필요하지 않을 때는 사용자에 대한 제약을 해소할 수 있습니다. 보안과 유용성 사이에 올바르게 균형을 유지하도록 환경 설정하는 것이 중요합니다. 그림 *6*은 조건부 액세스의 작동 방식에 대한 기능 다이어그램을 보여 줍니다.

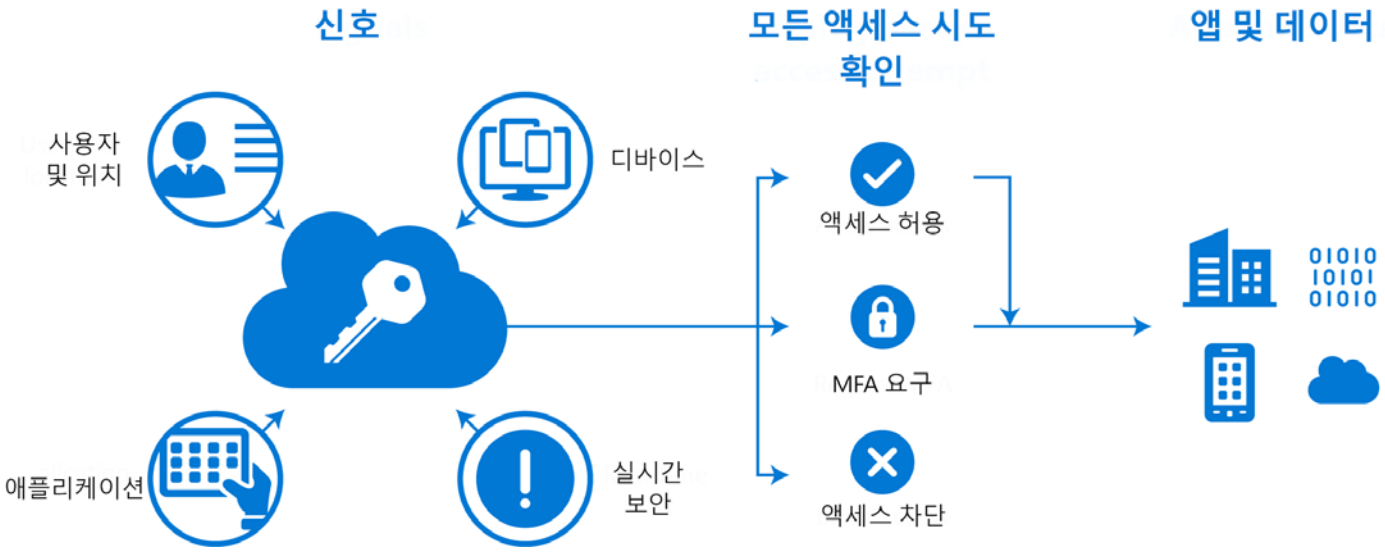


그림 6: 조건부 액세스 다이어그램

조건부 액세스를 시작하고 Azure Virtual Desktop에 대한 Multi-Factor Authentication(MFA)을 이용하려면 다음을 수행해야 합니다.

- Azure AD Premium P1 또는 P2가 포함된 라이선스를 사용자에게 할당합니다.
- 그룹 구성원으로 할당된 사용자로 Azure AD 그룹을 구성합니다.
- 모든 사용자에 대해 Azure 다중 인증을 사용하도록 설정합니다.

조건부 액세스를 환경 설정하려면 다음과 같이 합니다.

- Azure 포털에 글로벌 관리자, 보안 관리자 또는 조건부 액세스 관리자로 로그인하고 **Azure Active Directory** > **보안** > **조건부 액세스**를 찾아 **새 정책**을 선택합니다.
- 정책에 이름을 지정하고 **할당**에서 **사용자 및 그룹**을 선택하고, 이전에 만든 그룹을 할당합니다.
- **클라우드 앱 또는 작업** > **포함**에서 **앱 선택**을 선택한 다음 **Azure Virtual Desktop**을 선택합니다(앱 ID: 9cdead84-a844-4324-93f2-b2e6bb768d07).
- 이제 **조건** > **클라이언트 앱**으로 이동한 다음 정책을 적용할 위치를 선택합니다. 이는 **브라우저**(Azure Virtual Desktop 웹 클라이언트), **모바일 앱 및 데스크톱 클라이언트** 또는 둘 다일 수 있습니다.
- **액세스 제어** > **권한 부여**에서 **액세스 권한 부여**를 선택하고 **다중 인증 필요**를 선택한 다음 **선택**을 선택합니다.
- **액세스 제어** > **세션**에서 **로그인 빈도**를 선택하고 원하는 프롬프트 표시 시간 간격으로 값을 설정한 다음 **선택**을 클릭합니다.
- 마지막으로 설정을 확인하고 **정책 사용**을 **켜기**로 설정합니다. 정책은 그림 7과 같습니다.

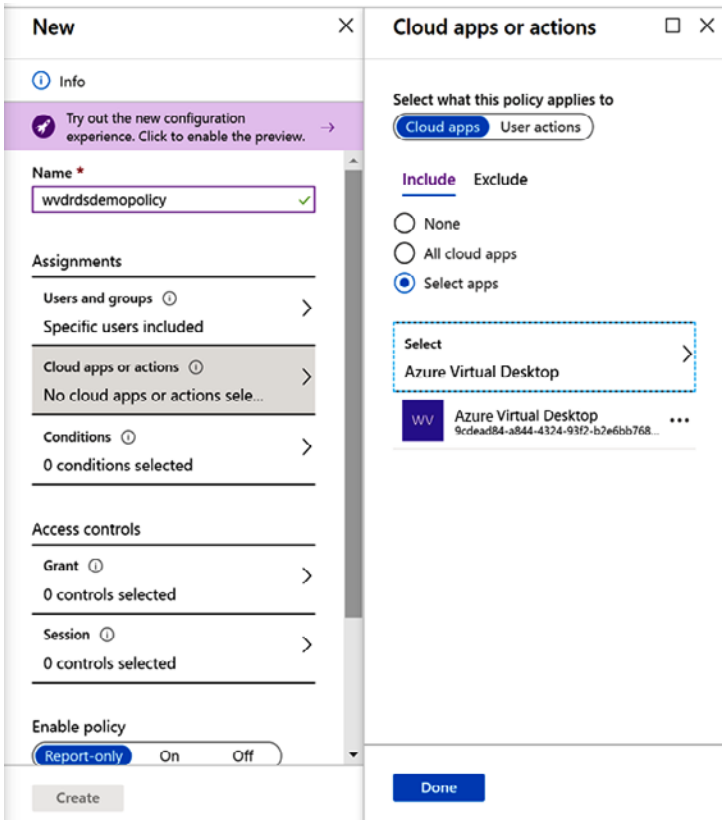


그림 7: Azure Virtual Desktop용 MFA 환경 설정

이제 특정 그룹에 대한 MFA를 적용하는 기본 조건부 액세스 정책 및 환경 설정된 로그인 빈도를 이용하는 특정 Azure Virtual Desktop 클라이언트를 환경 설정했습니다.

자세한 내용은 Azure Virtual Desktop에 대한 Azure 다중 인증 이용을 보다 자세히 설명하는 해당 문서를 읽어 보세요. 마지막으로, 조건부 액세스 정책에서 환경 설정한 로그인 빈도는 사용자가 리소스에 액세스하려고 할 때 다시 로그인하라는 메시지가 표시되기까지의 기간을 정의합니다. 사용자 로그인 빈도에 대한 자세한 내용은 해당 가이드를 참조하세요.

감사 로그 수집

사용자 ID 보안과 관련하여 감사 로그를 수집하고 검토하는 것도 중요합니다. 감사 로그 수집을 활용하면 Azure Virtual Desktop과 관련된 관리자 활동뿐만 아니라 사용자에 대한 인사이트를 수집하고 얻을 수 있습니다. 다음 목록은 Azure Virtual Desktop에 대한 감사 로그 수집을 시작하기 위한 여섯 가지 예제 영역을 나타냅니다.

- Azure 활동 로그
- Azure Active Directory 활동 로그
- Azure Active Directory
- 세션 호스트
- Azure Virtual Desktop 진단 로그
- Key Vault 로그

데이터 보호

사용자에게 Azure Virtual Desktop 환경에 대한 액세스 권한을 제공할 때 사용자 프로필의 일부로 개인 데이터를 저장하고 액세스하도록 허용할 수도 있습니다. 이 챕터에서는 해당 데이터를 보호하는 방법에 대해 설명합니다.

FSLogix 프로필 컨테이너

사용자 프로필은 시스템의 상태를 나타내는 환경 설정 모음입니다. 사용자의 프로필에 바인딩하는 시스템 구성 요소는 다양합니다. 이러한 구성 요소에는 애플리케이션, 레지스트리 항목 및 기타 사용자 맞춤형 항목이 포함됩니다. Windows 10에는 여러 유형의 사용자 프로필이 있지만 FSLogix 프로필 컨테이너를 활용하여 전체 사용자 프로필을 저장하는 것이 좋습니다. 프로파일 컨테이너는 전체 사용자 프로필을 원격 위치로 리디렉션하므로 기존 프로필 관리 솔루션이 아닙니다. 이러한 프로필 컨테이너를 저장하는 일반적인 방법에는 세 가지가 있습니다.

- 스토리지 공간 다이렉트를 기반으로 한 파일 공유를 활용하는 프로필 컨테이너
- Azure Files 및 Azure AD DS 또는 Azure Files 및 AD DS를 활용하는 프로필 컨테이너
- Azure NetApp Files 및 AD DS를 활용하는 프로필 컨테이너

대부분의 고객은 파일 공유를 활용하는 대신 Azure Files 또는 Azure NetApp Files에 FSLogix 프로필 컨테이너를 저장하는 것이 좋습니다. 차이점에 대한 자세한 내용은 스토리지 옵션 비교 문서를 참조하세요.

Azure Disk Encryption

Azure Files를 프로필 컨테이너 솔루션으로 활용하면 Azure AD DS의 온-프레미스 AD DS를 통해 SMB(서버 메시지 블록) ID 기반 인증이 지원됩니다. Azure Files는 온-프레미스 AD DS 또는 Azure AD DS로 인증하기 위해 Kerberos 프로토콜을 적용합니다.

Azure NetApp Files를 활용하면 Azure Virtual Desktop에서 이용하는 모든 파일이 연방 정보 처리 표준 간행물(FIPS PUBS) 140-2 표준을 통해 암호화됩니다. Azure NetApp Files 서비스는 모든 키를 관리하고 각 볼륨에 대해 고유한 XTS-AES-256 데이터 암호화 키를 생성합니다. Azure Virtual Desktop은 암호화 키를 이용하여 모든 볼륨 키를 암호화하고 보호합니다. 암호화 키는 암호화된 형식으로 사용하거나 보고할 수 없습니다. 볼륨이 삭제되면 키도 즉시 삭제됩니다.

보안 및 규정 준수와 관련해서는 Azure Files 및 스토리지 공간 다이렉트 모두 모든 Azure지원 인증서가 있습니다. Azure NetApp Files는 ISO가 완료되었습니다. FSLogix 프로필 컨테이너, 사용자 프로필 디스크 및 기타 사용자 프로필 기술에 대한 자세한 내용은 FSLogix 프로필 컨테이너 및 Azure Files의 표를 참조하세요.

직접 FSLogix 프로필 컨테이너 설정을 만들려면 다음 자습서 중 하나로 시작해 보세요.

- Azure Files 및 AD DS를 사용하여 프로필 컨테이너 만들기
- Azure NetApp Files 및 AD DS를 사용하여 프로필 컨테이너 만들기
- 파일 공유를 활용하여 프로필 컨테이너 만들기

세션 호스트 및 애플리케이션 보안

여러 작업을 수행하고 여러 도구를 이용하여 Azure Virtual Desktop 세션 호스트 및 애플리케이션을 보호할 수 있습니다. 이 챕터에서는 이러한 Azure Virtual Desktop 환경 구성 요소를 보호하기 위해 수행할 수 있는 작업을 설명합니다.

Microsoft Defender for Endpoint

맬웨어 및 인텔리전트형 위협으로부터 엔드포인트를 보호하려면 Microsoft Defender for Endpoint(이전의 Microsoft Defender Advanced Threat Protection)를 환경 설정하는 것이 좋습니다. Azure Virtual Desktop VM에 Microsoft Defender for Endpoint를 배포하는 여러 방법이 있습니다. 로컬 그룹 정책, 도메인 그룹 정책을 이용하거나 관리 도구로 온보딩할 수도 있습니다. 자세한 내용은 Azure Virtual Desktop에서 Windows 10 다중 세션 디바이스 온보딩 방법을 설명하는 해당 문서를 참조하세요. Windows 10 Enterprise 및 Windows 10 Enterprise 다중 세션의 단일 세션 시나리오가 모두 완전히 지원되며, Azure Virtual Desktop 컴퓨터를 Defender for Endpoint로 온보딩하는 방식에는 변경 사항이 없습니다. 이전에는 Windows 10 Enterprise 다중 세션에 대해 최대 50개의 동시 사용자 연결을 지원하는 Defender for Endpoint에 대한 소프트 제한이 있었지만 현재는 이 소프트 제한이 없어졌습니다. Windows 10 Enterprise 다중 세션을 활용하는 경우, 요구 사항에 따라 모든 사용자에게 Microsoft Defender for Endpoint(사용자당), Windows Enterprise E5, Microsoft 365 Security 또는 Microsoft 365 E5를 통해 라이선스를 부여하는 방법과 VM에 Azure Defender를 통해 라이선스를 부여하는 방법 중 선택할 수 있습니다. Azure Virtual Desktop의 Microsoft Defender for Endpoint 기능에 대한 자세한 내용은 해당 문서를 참조하세요.

Microsoft Endpoint Manager와 Microsoft Intune의 통합

Microsoft Intune을 사용하여 규정 준수에 대한 정책을 만들고 확인할 수 있습니다. 또한 이를 사용하여 Azure에서 실행되는 디바이스에 애플리케이션, 기능 및 설정을 배포할 수 있습니다. 지침을 보려면 Microsoft Endpoint Manager에서 Intune 연습을 참조하세요. Microsoft Intune은 인증 및 권한 부여를 위해 Azure AD와도 통합됩니다. 또한 데이터 보호를 위해 Azure Information Protection과 통합됩니다. Microsoft Intune은 Microsoft 365 제품군과 함께 사용할 수 있습니다. 애플리케이션 제어는 모든

애플리케이션을 신뢰할 수 있다고 간주하는 애플리케이션 신뢰 모델을 더 이상 따르지 않습니다. 새 모델에서는 신뢰도가 검증된 애플리케이션만 실행됩니다. Microsoft Defender Application Control 및 AppLocker는 애플리케이션 제어를 제공하기 위해 Windows 10에 포함되어 있으며 Azure Virtual Desktop 환경에서 보안 방법으로도 이용할 수 있습니다. 다음 단락에서 이 두 가지 방법에 대해 자세히 설명하겠습니다.

Windows Defender Application Control

매일 수천 개의 새로운 악성 파일이 생성되므로, 맬웨어를 방지하기 위한 서명 기반 탐지와 같은 기존의 바이러스 백신 솔루션을 활용하면 새로운 공격을 제대로 방어할 수 없습니다. Windows Defender Application Control은 사용자가 실행할 수 있는 애플리케이션과 시스템 코어(커널)에서 실행되는 코드를 제한하여 이러한 보안 위협 유형을 완화할 수 있습니다. Application Control은 Windows 10에 도입되었으며, Azure Virtual Desktop을 이용하면 Azure Virtual Desktop 호스트에서 실행할 수 있는 드라이버 및 애플리케이션을 제어할 수 있습니다. Application Control은 MSRC(Microsoft 보안 대응 센터)에서 정의한 서비스 기준에 따라 보안 기능으로 설계되었습니다. Application Control 빌드별로 사용 가능한 개별 Application Control 기능에 대한 자세한 내용은 기능 가용성 설명서를 참조하세요. Application Control을 시작하려면 이 페이지를 참조하세요.

AppLocker

AppLocker는 사용자가 승인되지 않은 소프트웨어를 실행하지 못하도록 하는 데 도움이 됩니다. AppLocker 제어 정책 제한 규칙은 파일 속성, 제품 이름, 파일 이름 또는 파일 버전을 기반으로 합니다. AppLocker에는 Windows가 제대로 작동하는 데 필요한 파일이 AppLocker 규칙 컬렉션에서 허용되도록 하기 위해 규칙 컬렉션별 기본 규칙이 포함되어 있습니다. 또한 기본 규칙을 사용하면 로컬 관리자 그룹의 구성원이 모든 Windows Installer 파일을 실행할 수 있습니다. AppLocker 규칙 컬렉션은 허용되는 파일 목록으로 작동합니다. 규칙 컬렉션에 나열된 파일만 실행할 수 있습니다. 이 환경 설정을 사용하면 AppLocker 규칙이 적용될 때 어떤 일이 발생하는지 쉽게 확인할 수 있습니다. AppLocker는 기본적으로 허용된 목록으로 작동하므로 규칙이 명시적으로 파일 실행을 허용하거나 거부하지 않으면 AppLocker의 기본 거부 동작이 파일을 차단합니다. 기본적으로 AppLocker는 매우 강력한 도구이지만, AppLocker가 아니라 Application Control을 활용하여 애플리케이션 제어를 구현하는 것이 가능한 경우 그렇게 하는 편이 좋습니다.

Application Control은 지속적으로 개선 중이며 Microsoft 관리 플랫폼에서 추가 지원을 받을 예정입니다. AppLocker에는 계속해서 보안 수정 사항이 적용되지만 새로운 기능 개선은 이루어지지 않을 예정입니다. 그러나 경우에 따라 AppLocker가 조직에 더 적합한 기술일 수 있습니다. 예를 들어 Windows OS(운영 체제) 환경이 혼합된 경우 공유 컴퓨터의 사용자 또는 그룹별로 다른 정책을 적용해야 합니다. 또는 DLL 또는 드라이버와 같은 애플리케이션 파일에 애플리케이션 제어를 적용하지 않는 것이 좋습니다. 모범 사례에 따르면 조직에 가능한 한 가장 제한적인 수준에서 Application Control을 적용해야 합니다. 그런 다음 AppLocker를 사용하여 제한을 더 세부적으로 조정할 수 있습니다. AppLocker를 시작하려면 이 페이지를 참조하세요.

Application Control 및 AppLocker 기능 가용성 행렬에서는 두 기술을 보다 자세히 비교합니다.

FSLogix Application Masking

Application Masking의 기본 사용 사례는 많은 골든 이미지(마스터 이미지)를 관리하는 복잡성을 크게 줄이는 것입니다. Application Masking은 주로 보안 수단으로 의도된 것은 아니지만 애플리케이션에 대한 보안을 제공하는 데 사용할 수도 있습니다. Application Masking은 기준에 따라 애플리케이션, 폰트 및 기타 항목에 대한 액세스를 관리합니다. Application Rules Editor는 애플리케이션과 같이 관리할 항목을 설명하는 데 사용됩니다. Application Masking은 물리적 환경과 가상 환경에서 모두 사용할 수 있습니다. Application Masking은 Virtual Desktop과 같은 비영구 가상 환경을 관리하기 위해 가장 자주 적용됩니다. Application Masking을 시작하려면 FSLogix Application Masking 구현 자습서를 참조하세요.

화면 캡처 보호

화면 캡처 보호(미리 보기) 기능은 클라이언트 엔드포인트에서 중요한 정보가 캡처되지 않도록 합니다. 이 기능을 사용하도록 설정하면 스크린샷 및 화면 공유에서 원격 콘텐츠가 자동으로 차단되거나 숨겨집니다. 또한 화면의 콘텐츠를 지속적으로 캡처할 수 있는 악성 소프트웨어에서 원격 콘텐츠가 숨겨집니다. 이 기능을 활용하는 경우 원격 콘텐츠가 엔드포인트에 복사되지 않도록 클립보드 리디렉션(추후 이 핸드북 설명 참조)을 이용하지 않는 것이 좋습니다. 이 정책은 레지스트리 키를 환경 설정하여 호스트 수준에서 적용됩니다. 이 정책을 활성화하려면 PowerShell을 열고 EnableScreenCaptureProtection 레지스트리 키를 설정합니다.

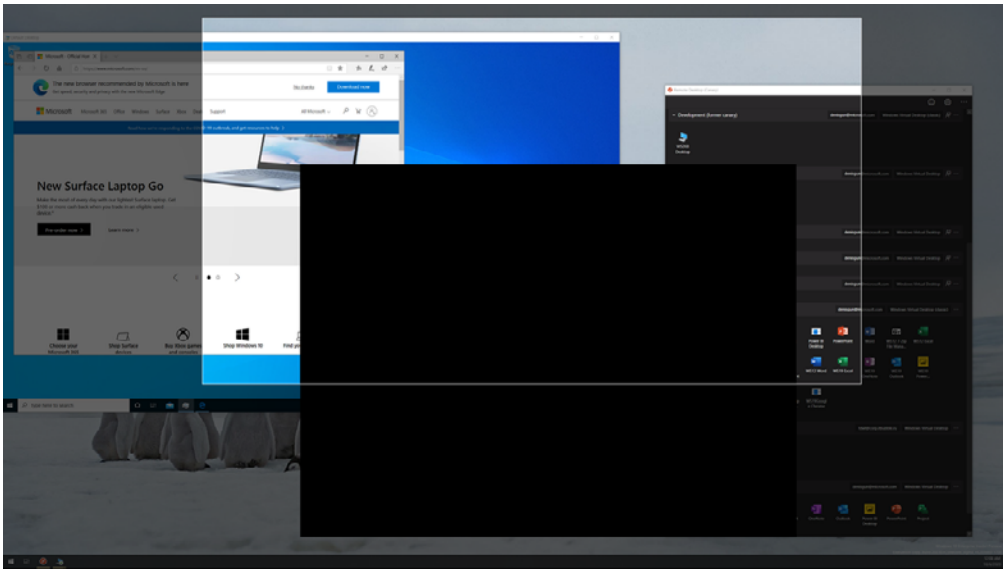


그림 8: 화면 캡처 보호 기능의 예

이 새 기능을 테스트하려면 호스트 풀을 유효성 검사 환경에서 프로비저닝해야 하며 Windows Desktop 클라이언트, 버전 1.2.1526 이상을 다운로드하여 설치해야 합니다. 물론 이 기능은 사용자가 휴대폰을 이용하여 화면 사진을 찍는 것을 막지는 못합니다. 그러나 추가 보안 계층을 추가할 수 있는 옵션을 제공합니다.

화면 캡처 보호 사용에 대한 자세한 지침은 이 페이지를 참조하세요.

사용자 환경의 소프트웨어 패치

모든 환경에서 취약점을 식별하면 가능한 한 빨리 패치해야 합니다. 이는 Azure Virtual Desktop 환경에도 적용됩니다. 여기에는 실행 중인 운영 체제, 운영 체제 내부에 배포되는 애플리케이션 및 새 컴퓨터를 만드는 이미지가 포함됩니다. 공급업체 패치 알림 통신을 따르고 적시에 패치를 적용합니다. 새로 배포된 컴퓨터를 가능한 한 안전하게 보호할 수 있도록 기본 이미지를 매월 패치하는 것이 좋습니다.

자세한 내용은 마스터 VHD 이미지 준비 및 사용자 맞춤화에 대한 가이드를 따르세요.

마스터 이미지에는 일반적으로 미리 정의된 보안 외에도 필요한 소프트웨어 및 환경 설정이 포함됩니다. 자체 이미징 파이프라인을 설정하려면 시간과 인프라가 필요합니다. Azure VM Image Builder를 사용하면 이미지를 설명하는 간단한 환경 설정을 제공하고 서비스에 제출하여 이미지를 구축하고 배포할 수 있습니다. Azure Image Builder는 Azure 리소스 공급자가 액세스할 수 있는 완전 관리형

Azure 서비스입니다. Azure Image Builder 프로세스에는 원본, 사용자 맞춤형 및 배포의 세 가지 주요 부분이 있으며, 이러한 부분은 템플릿에 표시됩니다.

그림 *9*는 Image Builder 프로세스를 보여 줍니다. Azure Image Builder 프로세스의 결과는 Shared Image Gallery 내에 VHD(가상 하드 디스크) 관리형 이미지로 저장된 템플릿 이미지로, 이는 Azure Virtual Desktop 세션 호스트를 다시 구축하는 데 이용할 수 있습니다.

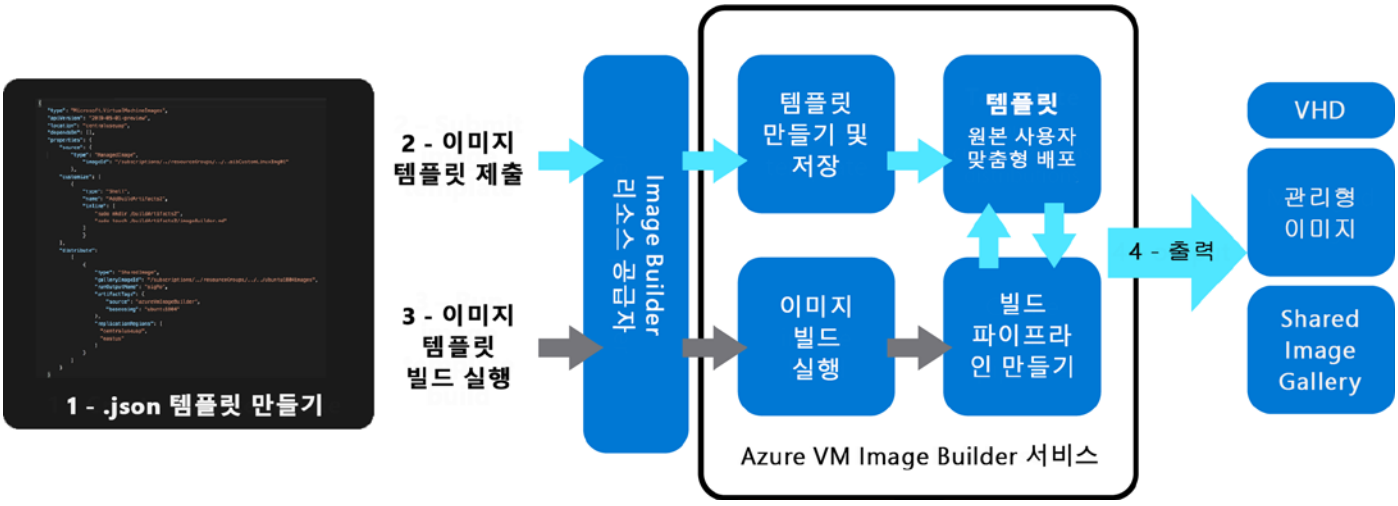


그림 9: Azure Image Builder 프로세스

자세한 내용은 Azure Image Builder 개요를 참조하세요.

최대 비활성/연결 해제 시간 정책 및 화면 잠금

비활성 상태인 사용자를 로그아웃하면 리소스가 보존되고 권한 없는 사용자가 액세스할 수 없습니다. 시간 제한을 사용하여 리소스 사용과 사용자 생산성의 균형을 맞추는 것이 좋습니다. 상태 비저장 애플리케이션과 상호 작용하는 사용자의 경우, 시스템을 끄고 리소스를 보존하는 것과 같은 더욱 적극적인 정책을 고려해야 합니다. 시뮬레이션 또는 CAD 렌더링과 같이 사용자가 유휴 상태일 경우 계속 실행되는 장기간 실행 중인 애플리케이션의 연결을 해제하면 사용자의 작업을 방해할 수 있으며 컴퓨터를 다시 시작해야 할 수도 있습니다. 또한 유휴 시간 동안 컴퓨터의 화면이 잠기도록 Azure Virtual Desktop을 환경 설정하고 잠금을 해제하려면 인증을 요구하여, 원치 않는 시스템 액세스를 방지할 수 있습니다. 로컬 그룹 정책 편집기 또는 중앙에서 그룹 정책 개체를 활용하여 템플릿 이미지 내에서 최대 비활성/연결 해제 시간을 환경 설정할 수 있습니다. 그림 *10*은 다양한 설정의 위치를 보여 줍니다.

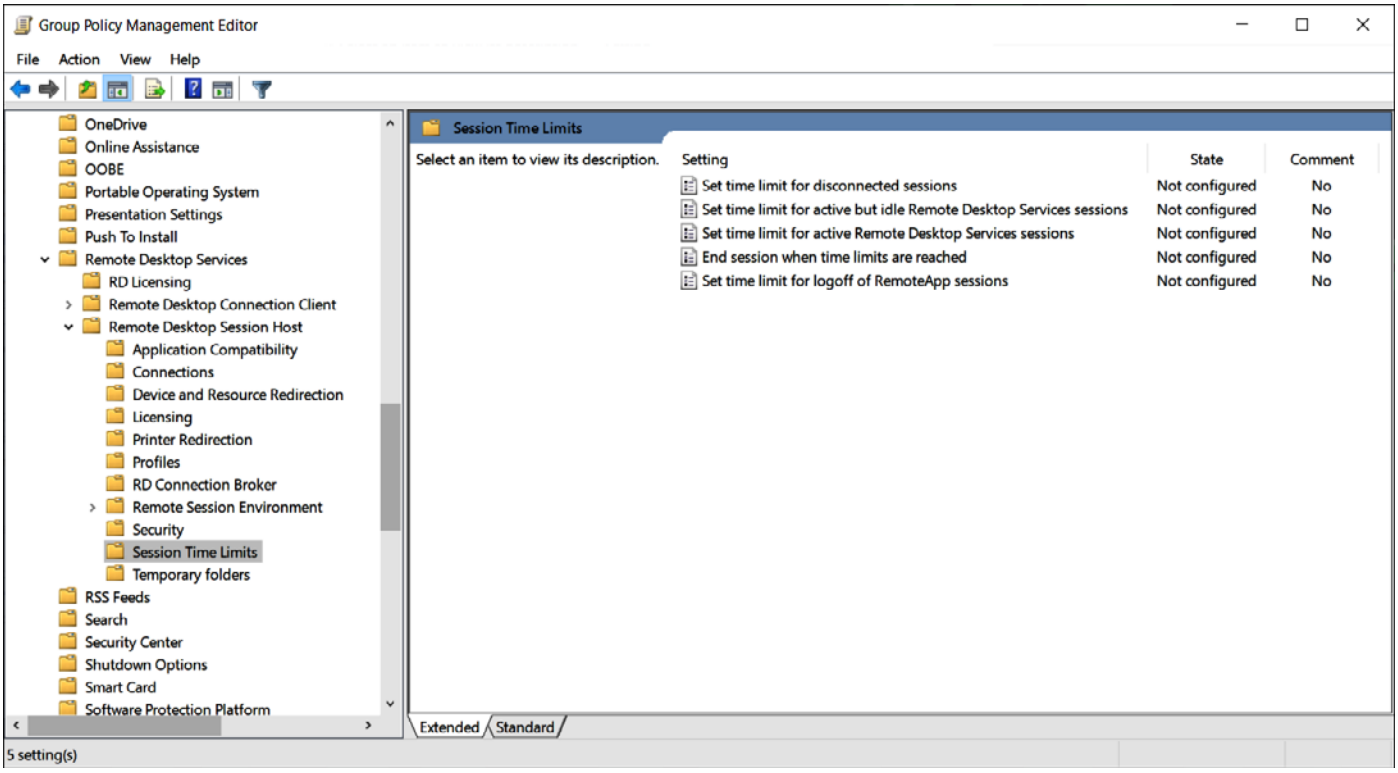


그림 10: 세션 제한에 대한 그룹 정책 위치

디바이스 리디렉션 환경 설정하기

사용자는 Azure Virtual Desktop 세션에 다양한 (주변) 디바이스를 가져올 수 있습니다. 이 기능은 전체 사용자 환경을 크게 향상시키는 훌륭한 기능입니다. 단, 사용자가 리디렉션할 수 있는 것을 현명하게 선택해야 합니다. 예를 들어 사용자가 Azure Virtual Desktop 세션의 클립보드 데이터를 로컬 클라이언트로 복사하지 않도록 하거나, Azure Virtual Desktop 내의 USB 드라이브에 액세스하지 못하도록 막을 수 있습니다. 보안 요구 사항을 평가하고 이러한 기능을 이용 중지해야 하는지 여부를 확인하는 것이 좋습니다.

그림 *11*은 호스트 풀의 RDP 속성의 일부로 변경할 수 있는 몇 가지 옵션을 보여 줍니다. Azure Virtual Desktop 페이지의 화면 왼쪽의 메뉴에서 호스트 풀을 선택한 다음 화면 왼쪽의 메뉴에서 RDP 속성을 선택합니다. 또는 고급 탭을 열고 세미콜론으로 구분된 형식으로 RDP 속성을 추가할 수 있습니다. 작업이 완료되면 저장을 선택하여 변경 내용을 저장합니다.

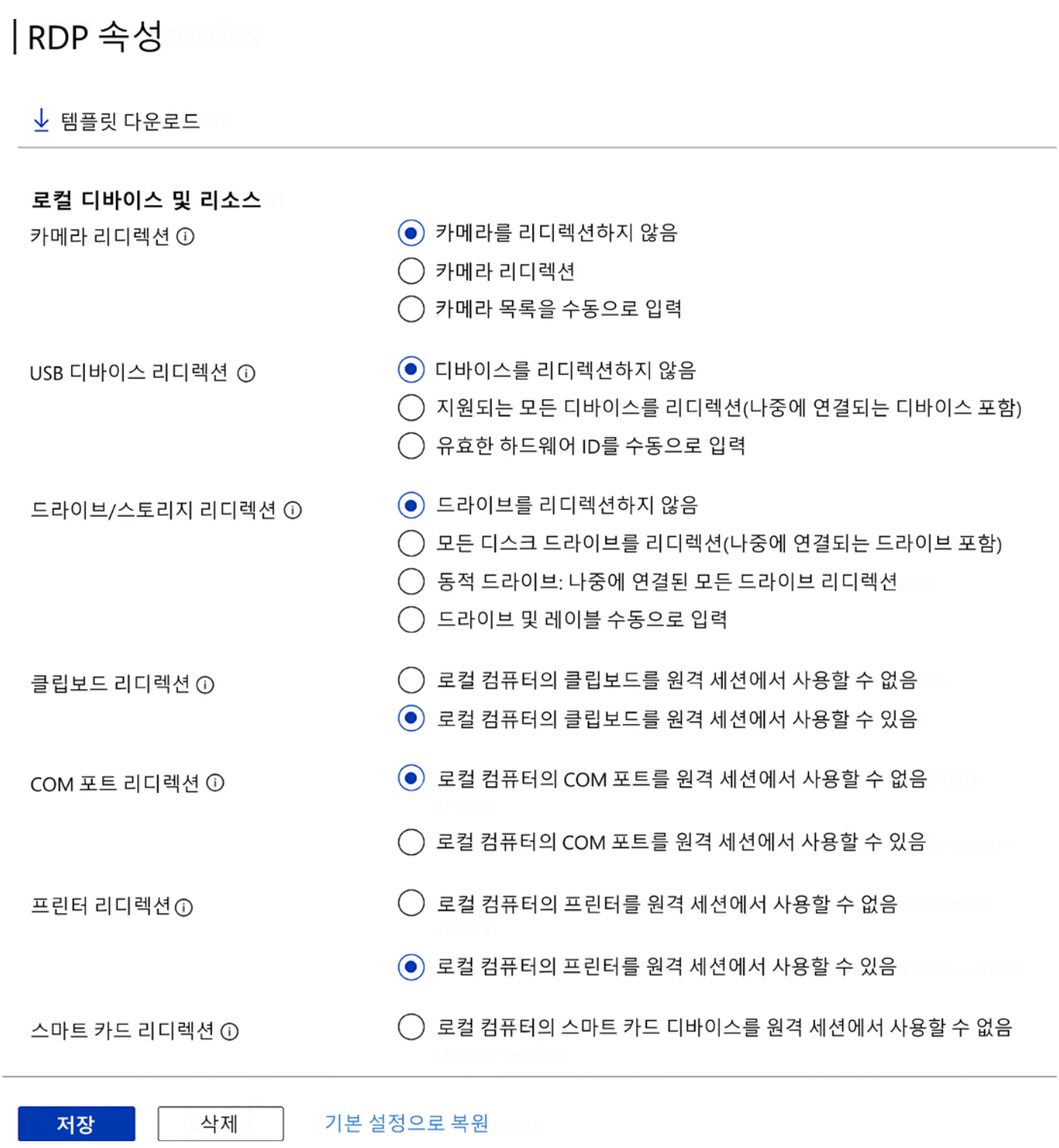


그림 11: 호스트 풀의 RDP 속성에 대한 옵션

자세한 내용은 [호스트 풀의 RDP(원격 데스크톱 프로토콜) 속성 사용자 맞춤]에 대한 자세한 정보를 제공하는 이 가이드를 참조하세요.

Windows 탐색기 액세스 제한

대부분의 Azure Virtual Desktop 배포에서는 더 나은 비용 최적화를 제공하는 풀링된 시나리오가 구현됩니다. 이는 기본적으로 사용자가 여러 사용자와 동시에 세션 호스트에 로그인하여 Azure VM 리소스를 공유한다는 것을 의미합니다. 따라서 사용자가 서로의 세션 데이터에 액세스하거나 공유 VM에서 원치 않는 작업을 수행할 수 없도록 잠금 정책을 수행하는 것이 좋습니다. 로컬 및 원격 드라이브 매핑을 숨김으로써 Windows 탐색기 액세스를 제한하면 사용자가 시스템 환경 설정 및 사용자에 대한 원치 않는 정보를 검색할 수 없습니다. 이러한 환경 설정은 템플릿 이미지 내에서 수행할 수 있지만 그룹 정책 개체를 활용하여 적용할 수도 있습니다.

그림 *12*는 Windows 탐색기 액세스를 환경 설정하는 데 활용할 수 있는 그룹 정책 개체 위치를 보여 줍니다.

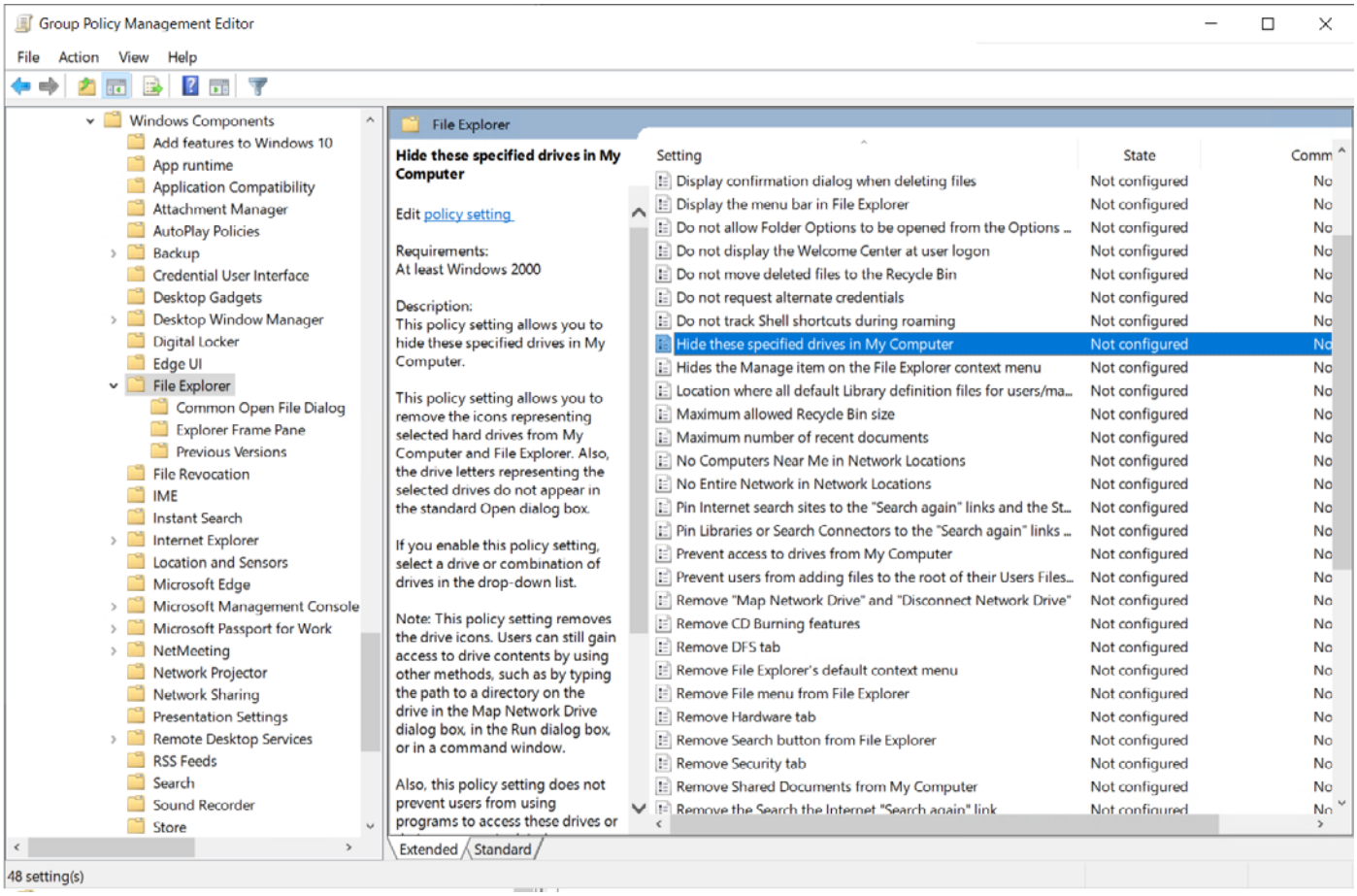


그림 12: Windows 탐색기 액세스를 환경 설정하기 위한 그룹 정책 개체 위치

드라이브를 숨겨 Windows 탐색기 액세스를 제한하는 방법에 자세한 내용은 그룹 정책 개체(Group Policy Object)를 활용하여 지정된 드라이브를 숨기기 자습서를 확인하세요. 드라이브를 숨긴다고 해서 액세스가 차단되지는 않습니다. 선택적으로 특정 드라이브에 대한 액세스를 차단할 수도 있습니다. 기본적으로 설정을 조사하여 세션 호스트를 잠글 수 있습니다(예: 명령 프롬프트, 제어판 또는 Windows 설정에 대한 액세스 차단). 이러한 모든 설정에 대한 자세한 설명은 이 핸드북에서 다루지 않습니다.

Microsoft 365 앱 보안 관리

세션 호스트를 보호하는 것 외에도 내부에서 실행되는 애플리케이션을 보호하는 것도 중요합니다. Microsoft 365 앱(이전 Microsoft Office Pro Plus)은 세션 호스트에 배포된 가장 일반적인 애플리케이션 중 일부입니다. Office 배포 보안을 개선하려면 엔터프라이즈용 Microsoft 365 앱의 보안 정책 관리자를 사용하는 것이 좋습니다. 이 도구는 배포에 적용하여 보안 기능을 추가할 수 있는 정책을 식별합니다. 또한 보안 정책 관리자는 보안 및 생산성에 미치는 영향을 기준으로 정책을 권장합니다. 보안 그룹에 정책 환경 설정이 할당된 경우 보안 정책 관리자는 해당 그룹의 사용자가 Microsoft 365 애플리케이션을 활용하는 방식을 분석합니다. 이 분석과 Microsoft 모범 사례를 기반으로 하여, 특정 보안 정책과 이러한 정책이 생산성 및 보안에 미치는 영향에 대한 인사이트를 제시하는 권장 사항이 생성됩니다. 자세한 내용은 엔터프라이즈용 Microsoft 365 앱에 대한 보안 정책 관리자 개요를 참조하세요.

네트워크 액세스 보안

Azure Virtual Desktop은 RDP(원격 데스크톱 프로토콜)를 이용하여 네트워크 연결을 통해 원격 표시 및 입력 기능을 제공합니다. Azure Virtual Desktop의 연결 데이터 흐름은 가장 가까운 Azure 데이터센터에 대한 DNS 조회로 시작합니다. 게이트웨이는 인텔리전트형 역방향 프록시 역할을 합니다. 게이트웨이는 클라이언트에 도달하는 픽셀만으로 모든 세션 연결을 관리합니다. 사용자 연결 상태를 구성하는 데는 다섯 가지 단계가 있습니다.

1. 토큰이 Azure AD에서 인증되면 원격 데스크톱 서비스 클라이언트로 반환됩니다.
2. 게이트웨이가 연결 브로커를 통해 토큰을 검사합니다.
3. 브로커는 사용자에게 할당된 리소스에 대해 Azure SQL Database를 쿼리합니다.
4. 게이트웨이와 브로커는 연결된 클라이언트의 세션 호스트를 선택합니다.
5. 세션 호스트는 Azure Virtual Desktop 게이트웨이를 활용하여 클라이언트에 대한 역방향 연결을 만듭니다.

그림 *13*은 Azure에서 실행되는 Azure Virtual Desktop의 5단계 연결 프로세스를 보여 줍니다.

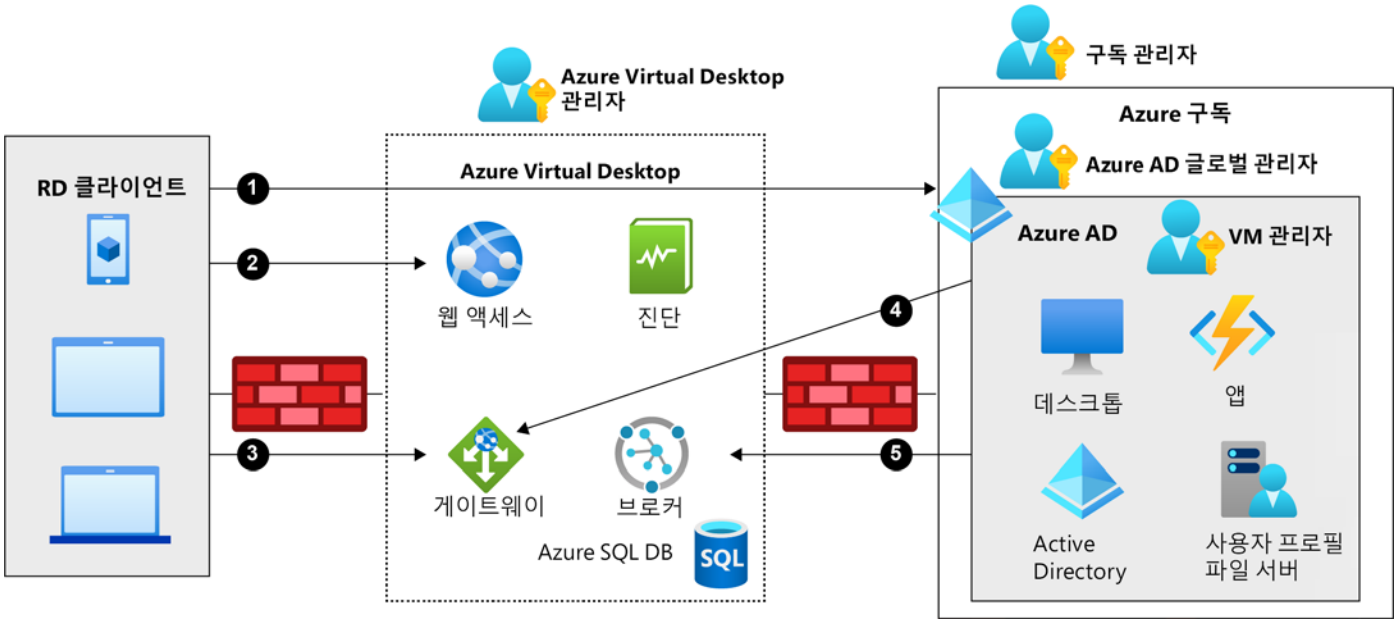


그림 13: Azure Virtual Desktop의 5단계 연결 프로세스

TLS 1.2는 클라이언트 및 세션 호스트에서 시작되어 Azure Virtual Desktop 인프라 구성 요소로 향하는 모든 연결에 이용됩니다. Azure Virtual Desktop은 Azure Front Door와 동일한 TLS 1.2 암호를 이용합니다. 클라이언트 컴퓨터와 세션 호스트가 이러한 암호를 모두 사용할 수 있는지 확인하는 것이 중요합니다. 역방향 연결 전송(다음 단락에서 자세히 설명됨)의 경우 클라이언트와 세션 호스트는 모두 Azure Virtual Desktop 게이트웨이에 연결합니다. TCP 연결을 설정한 후 클라이언트 또는 세션 호스트는 Azure Virtual Desktop 게이트웨이 인증서의 유효성을 검사합니다. 기본 전송을 설정한 후 RDP는 세션 호스트의 인증서를 이용하여 클라이언트와 세션 호스트 간에 중첩된 TLS 연결을 설정합니다.

역방향 연결

RDS(원격 데스크톱 서비스) 및 RD 게이트웨이(원격 데스크톱 게이트웨이)에 익숙하다면, 사용자가 RD 세션 호스트(원격 데스크톱 세션 호스트)에 연결할 수 있도록 허용하기 위해서는 RD 게이트웨이에서 RD 세션 호스트를 향해 TCP 포트 3389를 열어야 한다는 점을 알고 있을 것입니다.

RDS와 달리 Azure Virtual Desktop은 기본적으로 추가 보안 계층을 제공하므로 들어오는 RDP 연결을 수신하는 데 TCP 수신기가 필요하지 않습니다. Azure Virtual Desktop은 역방향 연결 전송을 이용하여 원격 세션을 설정하고 RDP 트래픽을 전송합니다. 세션 호스트에 자동으로 설치된 Azure Virtual Desktop Agent는 HTTPS 연결을 통해 Azure Virtual Desktop 인프라에 대한 아웃바운드 연결을 이용하도록 환경 설정됩니다. 따라서 세션 호스트 앞의 방화벽 내부에 인바운드 포트가 필요하지 않습니다. 역방향 연결을 활성화하는 데 필요한 추가 작업은 없지만 TCP 포트 3389가 불필요하게 열리지 않도록 하는 것이 좋습니다.

일반적으로는 사용자 환경에서 세션 호스트에 대한 직접 RDP 액세스를 차단해야 합니다. 관리 또는 문제 해결을 위해 직접 RDP 액세스가 필요한 경우 내부 네트워크에서 연결하거나 Just-In-Time 액세스를 활성화하여 세션 호스트의 잠재적 공격 노출을 줄일 수 있습니다.

네트워크 보안 그룹 서비스 태그

취할 수 있는 또 다른 보안 조치는 NSG(네트워크 보안 그룹) 서비스 태그를 활용하여 Azure Virtual Desktop 트래픽을 제한하는 것입니다.

서비스 태그는 Azure VM에 대한 보안을 단순화합니다. Azure 가상 네트워크는 Azure Virtual Desktop 배포에 이용되므로 서비스 태그를 이용하면 Azure 서비스에 대한 네트워크 액세스만 쉽게 제한할 수 있습니다. NSG 규칙에서 서비스 태그를 사용하여 전 세계적으로나 Azure 리전별로 특정 Azure 서비스에 대한 트래픽을 허용하거나 거부할 수 있습니다. NSG는 Azure 리소스 내부 또는 외부로 향하는 네트워크 트래픽 흐름을 허용하거나 거부하는 보안 규칙 모음입니다. 각 규칙은 이름, 우선 순위, 원본 또는 대상, 프로토콜, 방향, 포트 범위 및 작업과 같은 속성을 지정할 수 있습니다. NSG는 계층 3 및 계층 4 네트워크 보안 서비스입니다.

Azure Virtual Desktop용으로 만든 Azure VM은 제대로 작동하려면 여러 FQDN(정규화된 도메인 이름)에 액세스할 수 있어야 합니다. 다음 표에는 이러한 FQDN 및 포트가 표시됩니다.

주소	아웃바운드 TCP 포트	목적	서비스 태그
*.wvd.microsoft.com	443	서비스 트래픽	WindowsVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	에이전트 트래픽	AzureCloud
production.diagnostics.monitoring.core.windows.net	443	에이전트 트래픽	AzureCloud
*xt.blob.core.windows.net	443	에이전트 트래픽	AzureCloud
*eh.servicebus.windows.net	443	에이전트 트래픽	AzureCloud
*xt.table.core.windows.net	443	에이전트 트래픽	AzureCloud
*xt.queue.core.windows.net	443	에이전트 트래픽	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows 정품 인증	인터넷
mrsglobalsteus2prod.blob.core.windows.net	443	에이전트 및 SXS 스택 업데이트	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Azure 포털 지원	AzureCloud
169.254.169.254	80	Azure Instance Metadata 서비스 엔드포인트	해당 없음
168.63.129.16	80	세션 호스트 상태 모니터링	해당 없음

애플리케이션 수준 보호를 위한 Azure Firewall

Azure Firewall은 이전에 설명한 대로 환경 설정을 단순화하기 위해 Azure Virtual Desktop FQDN 태그를 제공합니다. 다음 단계를 활용하여 Azure Firewall을 통해 아웃바운드 Azure Virtual Desktop 플랫폼 트래픽을 허용합니다.

- Azure Firewall을 배포하고 Azure Virtual Desktop 호스트 풀 서브넷 UDR(사용자 정의 경로)을 환경 설정하여 Azure Firewall을 통해 모든 트래픽을 라우팅합니다.
- 애플리케이션 규칙 컬렉션을 만들고 AzureVirtualDesktop FQDN 태그를 이용하는 규칙을 추가합니다.
- Azure Virtual Desktop 호스트 풀에 필요한 스토리지 및 Service Bus 계정 집합은 배포별로 다르므로 AzureVirtualDesktop FQDN 태그에 아직 캡처되어 있지 않습니다. *xt.blob.core.windows.net, *eh.servicebus.windows.net 및 *xt.table.core.windows.net에 대한 호스트 풀 서브넷의 HTTPS 액세스를 허용하여 이 문제를 해결합니다. 이러한 와일드카드 FQDN은 필요한 액세스를 제공하지만 덜 제한적입니다. 다른 옵션은 로그 분석 쿼리를 사용하여 필요한 정확한 FQDN을 나열한 다음 방화벽 애플리케이션 규칙에 명시적으로 허용하는 것입니다.
- 네트워크 규칙 컬렉션을 만들고, TCP 및 UDP 포트 53의 경우 AD DS 프라이빗 IP 주소에서 *로 가는 트래픽을 허용하고, Azure Virtual Desktop VM에서 Windows Activation Service TCP 포트 1688로 트래픽을 허용합니다.

이 환경 설정에 대한 자세한 내용은 Azure Virtual Desktop에 대한 호스트 풀 아웃바운드 액세스 가이드에서 확인할 수 있습니다.

인터넷에 대한 호스트 풀 아웃바운드 액세스

사용 사례에 따라 사용자에 대한 보안 아웃바운드 인터넷 액세스를 사용하도록 설정해야 할 수 있습니다. 허용되는 대상 목록(예: Microsoft 365 액세스)이 효과적으로 정의된 경우 Azure Firewall 애플리케이션 및 네트워크 규칙을 활용하여 필요한 액세스를 환경 설정할 수 있습니다. 애플리케이션이 효과적으로 정의되어 있지 않은 경우 이러한 대상을 허용 목록에 포함하는 것이 다소 까다로울 수 있습니다. 또한 기존 온-프레미스 보안 웹 게이트웨이를 활용하여 아웃바운드 사용자 인터넷 트래픽을 필터링하려는 경우 명시적 프록시 환경 설정으로 Azure Virtual Desktop 호스트 풀에서 실행되는 웹 브라우저 또는 기타 애플리케이션을 환경 설정할 수도 있습니다.

Azure 보안 모범 사례

이 섹션에서는 Azure Security Center를 활용하여 보안을 제공하고, 보안 점수를 개선하고, Azure Virtual Desktop의 Azure 보안 기준을 활용하는 방법에 대한 일반적인 지침을 제공합니다.

Azure Security Center

Azure Security Center는 Azure Defender를 통합하여 보안 점수 및 위협 보호 기능을 통해 무료 보안 태세 관리 기능을 제공합니다.

일반적으로 Azure Virtual Desktop을 포함하여 환경의 전반적인 보안을 강화하기 위해 보안 점수를 모니터링하는 것이 좋습니다. 시작하려면 Azure Security Center 설정을 위한 빠른 시작 가이드를 따르세요.

보안 점수는 전반적인 보안을 개선하기 위한 권장 사항 및 모범 사례 조언을 제공합니다. 이러한 권장 사항은 우선순위가 지정되어 있어 가장 중요한 권장 사항을 선택하는 데 도움이 되며, 빠른 수정 옵션을 통해 잠재적인 취약점을 신속하게 해결할 수 있습니다. 또한 이러한 권장 사항은 시간이 지남에 따라 업데이트되어 환경의 보안을 유지하는 최선의 방법에 대한 최신 정보를 제공합니다. 자세한 내용은 Azure Security Center의 보안 점수 향상을 참조하세요.

보안 태세 모니터링을 시작하면 Azure Defender를 사용하여 VM, SQL, 스토리지 계정, 컨테이너 및 키 자격 증명 모음과 같은 하이브리드 클라우드 워크로드를 보호하는 것이 좋습니다. Azure Defender를 사용하면 위협 경고의 우선순위를 확인하고, 취약점을 관리하고, PCI와 같은 일반 프레임워크의 규정 준수를 평가할 수 있습니다.

보안 경고는 Azure Defender 포털에서 관리할 수 있으며, SIEM(보안 정보 및 이벤트 관리) 도구로 내보내 분석 및 수정을 수행할 수도 있습니다. Microsoft의 클라우드 SIEM 도구는 Azure Sentinel이라고 합니다. Azure Security Center를 Azure Sentinel과 통합하면 보안 운영 센터에 매우 유용합니다.

Azure Sentinel은 조직 전체에서 인텔리전트형 보안 분석 기능을 제공하여 모든 사용자, 데이터, 애플리케이션 및 인프라에서 데이터를 수집하는 클라우드 네이티브 SIEM 도구입니다. Azure Sentinel은 AI와 머신 러닝을 이용하여 더욱 스마트하고 빠르게 위협을 탐지하며, 클라우드 네이티브 특성으로 인해 기존 SIEM 도구에서 요구하는 비용, 인프라 및 유지 관리가 필요 없습니다. 특히 Azure Virtual Desktop의 경우 Azure Sentinel은 세션 호스트, Microsoft Defender for Endpoint 경고 및 Azure Virtual Desktop 진단에서 Windows 이벤트 로그를 수집할 수 있습니다. 후자는 Azure Virtual Desktop 서비스의 기능으로, 누군가가 Azure Virtual Desktop 역할을 할당받고 서비스를 이용할 때마다 정보를 기록합니다.

자세한 내용은 Azure Virtual Desktop의 진단 기능에 Log Analytics를 이용하는 방법에 대해 설명하는 문서에서도 제공됩니다.

Azure Virtual Desktop의 Azure 보안 기준

Azure Virtual Desktop의 Azure 보안 기준은 Azure Security Benchmark 버전 2.0의 지침을 Azure Virtual Desktop에 적용하는 역할을 합니다. Azure에서 클라우드 솔루션을 보호하는 방법에 대한 권장 사항을 제공합니다. Azure Virtual Desktop의 Azure 보안 기준의 내용은 Azure Security Benchmark에서 정의한 보안 컨트롤과 Azure Virtual Desktop에 적용되는 관련 지침으로 쉽게 그룹화됩니다.

다음 표에는 기준에 포함된 항목에 대한 직접 링크가 나와 있습니다.

Azure Virtual Desktop의 Azure 보안 기준
NS - 네트워크 보안
IM - ID 관리
PA - 권한 있는 액세스
DP - 데이터 보호
AM - 자산 관리
LT - 로깅 및 위협 탐지
IR - 인시던트 대응
PV - 태세 및 취약성 관리
ES - 엔드포인트 보안
BR - 백업 및 복구
GS - 거버넌스 및 전략

결론

요약

이 핸드북에서는 먼저 Azure Virtual Desktop 환경 보안의 중요성을 소개했으며 일반적인 배포의 상위 레벨 아키텍처에 대해 알아보았습니다. 그런 다음 조건부 액세스를 활용하여 환경에 액세스하는 ID를 보호하는 방법과 감사 로그를 수집하는 방법을 다루었습니다. 이를 진행하면서 FSLogix 프로필 및 디스크 암호화로 사용자 데이터를 보호하는 방법을 설명했습니다. 그런 다음 세션 호스트 및 애플리케이션 보안, Azure Defender for Endpoint, AppLocker, 패치, 잠금 및 Microsoft 365 보안 관리에 대해 설명했습니다. 마지막으로 역방향 연결, Azure Firewall 및 Azure 보안 기준과 같은 주제를 다루는 Azure Virtual Desktop에 대한 네트워크 액세스 보안에 대한 지침을 제공했습니다.

Azure Virtual Desktop 보안 기초에 대한 이 핸드북을 통해 고객의 Azure Virtual Desktop 배포를 안전하게 유지하는 방법을 더 잘 이해할 수 있기를 바랍니다. 시작하는 데 도움이 되는 추가 정보 및 지원은 리소스 섹션을 확인하세요.

리소스

Azure Virtual Desktop을 통해 보안을 강화하는 여정에 도움이 되는 리소스는 다음과 같습니다.

- Azure Virtual Desktop 모범 사례에 대한 자세한 내용을 확인하세요.
- Azure Virtual Desktop 지침에 대한 Azure 보안 기준을 따르세요.
- 이 학습 모듈을 활용하여 Azure Virtual Desktop 보안 지식을 테스트하세요.
- Azure 무료 계정으로 지금 시작하세요.
- Azure 영업 전문가에게 문의하여 맞춤형 가이드를 받고, 가격 책정, 기술 요구 사항 및 보안 원격 작업을 지원하기 위한 솔루션에 대해 알아보세요.
- Azure 마이그레이션 및 현대화 프로그램에 가입하여 온-프레미스 VDI를 마이그레이션하는 데 대한 참고 자료 및 전문가의 도움을 받으세요.

용어집

다음 표에는 이 핸드북 전체에 사용된 용어 설명이 포함되어 있습니다.

용어	설명
Active Directory Domain Services	디렉터리는 네트워크 개체에 대한 정보를 저장하는 계층 구조입니다. Active Directory Domain Services(AD DS)와 같은 디렉터리 서비스는 디렉터리 데이터를 저장하고 네트워크 사용자와 관리자가 이 데이터를 사용할 수 있도록 합니다.
Azure Active Directory(Azure AD)	Azure AD는 직원들이 로그인하고 리소스에 액세스할 수 있도록 도와주는 Microsoft의 클라우드 기반 ID 및 액세스 관리 서비스입니다.
Microsoft Defender Application Control	Application Control은 MSRC(Microsoft 보안 대응 센터)에서 정의한 서비스 기준에 따라 보안 기능으로 설계되었으며, 디바이스에서 특정 드라이버 또는 애플리케이션을 실행할 수 있는지 여부를 정의하는 정책을 통해 Windows 10 디바이스를 제어할 수 있도록 합니다.
MSRC(Microsoft 보안 대응 센터)	MSRC(Microsoft 보안 대응 센터)는 Microsoft의 단일 보안 조정 및 통신 지점 역할을 하며 세계에서 가장 경험이 풍부한 전문가들이 이끌고 있습니다. MSRC는 Microsoft 소프트웨어의 취약점을 포함한 보안 인시던트를 식별, 모니터링, 해결 및 대응합니다.
FSLogix	FSLogix는 Azure Virtual Desktop과 같은 원격 컴퓨팅 환경에서 프로필을 로밍하도록 설계되었습니다. 전체 사용자 프로필을 단일 컨테이너에 저장합니다.
Azure Virtual Desktop	Microsoft Azure에서 실행되는 데스크톱 및 앱 가상화 서비스입니다.
NSG(네트워크 보안 그룹)	NSG에는 다양한 Azure 리소스의 인바운드 네트워크 트래픽 또는 아웃바운드 네트워크 트래픽을 허용하거나 거부하는 보안 규칙이 존재합니다.
AppLocker	AppLocker는 사용자가 실행할 수 있는 앱 및 파일을 제어하는 데 도움이 됩니다. 여기에는 실행 파일, 스크립트, Windows Installer 파일, DLL(동적 연결 라이브러리), 패키지 앱 및 패키지 앱 설치 프로그램이 포함됩니다.
Windows 10 Enterprise 다중 세션	Windows 10 Enterprise 다중 세션(이전의 Windows 10 Enterprise for Virtual Desktops(EVD))은 여러 동시 대화형 세션을 허용하는 새로운 원격 데스크톱 세션 호스트입니다.
Azure NetApp Files	Azure NetApp Files 서비스는 엔터프라이즈급 고성능 요금제형 파일 스토리지 서비스입니다. Azure NetApp Files는 모든 워크로드 유형을 지원하며 기본적으로 고가용성입니다.

저자 소개

프릭 버거슨(Freek Berson)은 원격 기술을 기반으로 애플리케이션 및 데스크톱 제공을 전문으로 하는 클라우드 솔루션 설계자입니다. 그는 RDS 분야에서 오랜 실적을 보유하고 있으며 2011년부터 Microsoft MVP(Most Valuable Professional)로 선정되었습니다.

Freek은 IT 관련 커뮤니티에 적극적으로 참여하고 있고, Microsoft Ignite, Microsoft Ignite | The Tour, Microsoft TechSummit, Microsoft TechDays, Azure Saturday, BriForum, E2EVC, ExpertsLive 등과 같은 이벤트(온라인)를 비롯하여 전 세계의 다양한 회의에서 강연합니다. 또한 이미 여러 권의 책을 출간한 저자이기도 합니다.

그는 네덜란드에 기반을 둔 클라우드 통합 회사인 WorteII에서 근무하며 최종 사용자 컴퓨팅(주로 Azure를 포함하여 Microsoft 플랫폼)에 중점을 둡니다

또한 그는 RDS Gurus社에서 임원으로 일하고 있습니다. Freek은 themicrosoftplatform.net에 개인 블로그를 보유하고 있으며 Azure Virtual Desktop, RDS, Azure 및 기타 Microsoft 관련 기사와 블로그 게시물을 작성합니다.

Twitter(@fberson)를 팔로우하거나 GitHub 계정을 통해 그의 기고문을 확인할 수 있습니다.