# 시스템 관리

## Virtual Desktop Service

NetApp
April 12, 2022

# 목차

# 시스템 관리

## 도메인 관리자("레벨 3") 계정을 생성합니다

### 개요

VDS 관리자가 환경을 관리하기 위해 도메인 수준 자격 증명이 필요한 경우가 있습니다. VDS에서 이러한 계정을 "레벨 3" 또는 ".tech" 계정이라고 합니다.

이 지침은 이러한 계정을 적절한 권한으로 생성하는 방법을 보여 줍니다.

**Windows Server** 도메인 컨트롤러

내부적으로 호스팅되는 도메인 컨트롤러(또는 VPN/Express 경로를 통해 Azure에 연결된 로컬 DC)를 실행하는 경우 관리 기술 계정은 Active Directory Manager에서 직접 수행할 수 있습니다.

1. 도메인 관리자(.tech) 계정으로 도메인 컨트롤러(CWMGR1, DC01 또는 기존 VM)에 연결합니다.
2. 새 사용자를 생성합니다(필요한 경우).
3. 사용자를 "Level3 Technician" 보안 그룹에 추가합니다

   [관리. 시스템 관리. 도메인 관리자 계정 9ee17을 생성합니다] |

*Management.System_Administration.create_domain_admin_account-9ee17.png*

a. "Level3 Technician" 보안 그룹이 누락된 경우 그룹을 만들어 "CW-Infrastructure" 보안 그룹의 구성원으로 만드십시오.

   [Management.System Administration.create domain admin account 0fc27] |

*Management.System_Administration.create_domain_admin_account-0fc27.png*

사용자 이름 끝에 “.tech”를 추가하는 것은 최종 사용자 계정에서 관리자 계정을 설명하는 데 도움이 되는 권장 모범 사례입니다.

**Azure AD** 도메인 서비스

Azure AD 도메인 서비스에서 실행하거나 Azure AD에서 사용자를 관리하는 경우, 이러한 계정은 일반적인 Azure AD 사용자로 Azure Management Portal에서 관리(예: 암호 변경)할 수 있습니다.

새 계정을 만들 수 있으며 이러한 역할에 계정을 추가하면 필요한 권한이 부여됩니다.

1. AAD DC 관리자
2. 클라이언트 DHPAccess
3. 디렉토리의 전역 관리자.

사용자 이름 끝에 “.tech”를 추가하는 것은 최종 사용자 계정에서 관리자 계정을 설명하는 데 도움이 되는 권장 모범 사례입니다.

[]

# 제3자에 대한 임시 액세스 제공

## 개요

클라우드 솔루션으로 마이그레이션할 때 타사의 액세스를 제공하는 것은 일반적인 관행입니다.

VDS 관리자는 종종 이러한 제3자에게 "최소 필수" 보안 액세스 정책을 따르도록 하는 동일한 수준의 액세스 권한을 제공하지 않습니다.

제3자에 대한 관리자 액세스를 설정하려면 VDS에 로그인하여 Organizations(조직) 모듈로 이동한 후 조직을 클릭하고 Users & Groups(사용자 및 그룹) 를 클릭합니다.

그런 다음 제3자에 대한 새 사용자 계정을 만들고 관리자 액세스 섹션이 나타날 때까지 아래로 스크롤한 다음 이 확인란을 선택하여 관리자 권한을 활성화합니다.

[]

그런 다음 VDS Admin(VDS 관리자)이 Admin Access(관리자 액세스) 설정 화면이 표시됩니다. 사용자 이름, 로그인 또는 암호를 변경할 필요가 없습니다. 다단계 인증을 적용하고 부여할 액세스 수준을 선택하려면 전화 번호 및/또는 이메일을 추가하기만 하면 됩니다.

VAR 또는 ISV와 같은 데이터베이스 관리자의 경우 일반적으로 _Servers_는 필요한 유일한 액세스 모듈입니다.

[]

저장 후 최종 사용자는 표준 Virtual Desktop 사용자 자격 증명으로 VDS에 로그인하여 자체 관리 기능에 액세스할 수 있습니다.

새로 생성된 사용자가 로그인하면 할당된 모듈만 표시됩니다. 이들은 조직을 선택하고 Servers(서버) 섹션으로 아래로

스크롤하여 해당 서버 이름을 연결할 수 있습니다(예: <XYZ>D1, 여기서 XYZ는 회사 코드이고 D1은 서버가 데이터 서버임을 나타냅니다). 아래 예에서는 TSD1 서버에 연결하여 과제를 수행하도록 합니다.

[]

# 백업 일정을 구성합니다

## 개요

VDS는 Azure를 비롯한 일부 인프라 공급자의 기본 백업 서비스를 구성 및 관리할 수 있습니다.

## Azure를 지원합니다

Azure에서 VDS는 네이티브를 사용하여 백업을 자동으로 구성할 수 있습니다 "Azure Cloud 백업" 로컬 중복 저장소(LRS) 포함. 지리적 중복 스토리지(GRS)는 필요한 경우 Azure Management Portal에서 구성할 수 있습니다.

- 각 서버 유형에 대해 개별 백업 정책을 정의할 수 있습니다(기본 권장 사항 포함). 또한 VDS UI 내에서 개별 컴퓨터에 서버 유형을 기준으로 일정 독립(서버 유형)을 할당할 수 있습니다. 이 설정은 작업 영역 페이지에서 서버 이름을 클릭하여 서버 세부 정보 보기로 이동하면 적용할 수 있습니다(아래 비디오: 개별 백업 정책 설정 참조).
  - 데이터
    - 매일 7회, 매주 5회, 매월 2회 백업을 통한 백업 비즈니스 요구사항에 따라 보존 기간 증가
    - 이는 전용 데이터 서버와 애플리케이션 및 데이터베이스용 추가 VPS VM 모두에 적용됩니다.
  - 검토할 수 있습니다
    - CWMGR1 – 매일 백업, 매일 7회, 매주 5회, 매월 2회 유지
    - RDS 게이트웨이 – 매주 백업하고 4회 유지합니다.
    - HTML5 Gateway – 매주 백업하고 4주 단위로 유지합니다.
  - PowerUser(또는 VDI 사용자)
    - VM은 D1 또는 TSD1 서버에 데이터를 저장해야 하므로 백업하지 마십시오.
    - 일부 애플리케이션은 로컬에 데이터를 저장하므로 이 경우 특별한 사항을 고려해야 합니다.
    - VM 장애 발생 시 다른 VM의 클론을 통해 새 VM을 구축할 수 있습니다. 하나의 VDI VM(또는 하나의 고유한 VM 빌드)만 있는 경우 해당 VM을 완전히 재구축할 필요가 없도록 백업하는 것이 좋습니다.
    - 필요한 경우 모든 VDI 서버를 백업하는 대신 단일 VM을 수동으로 구성하여 Azure Management Portal에서 직접 백업함으로써 비용을 최소화할 수 있습니다.
  - TS
    - VM은 D1 또는 TSD1 서버에 데이터를 저장해야 하므로 백업하지 마십시오.
    - 일부 애플리케이션은 로컬에 데이터를 저장하므로 이 경우 특별한 사항을 고려해야 합니다.
    - VM 장애 발생 시 다른 VM의 클론을 통해 새 VM을 구축할 수 있습니다. TS VM이 하나만 있는 경우 해당 VM의 완전한 재구축이 필요하지 않도록 백업하는 것이 좋습니다.
    - 필요한 경우 모든 TS 서버를 백업하는 대신 단일 VM을 수동으로 구성하여 Azure Management Portal에서 직접 백업함으로써 비용을 최소화할 수 있습니다.
  - TSData(TS데이터)

        - 매일 7회, 매주 5회, 매월 2회 백업을 통한 백업 비즈니스 요구사항에 따라 보존 기간 증가
- 매일 또는 매주 백업을 실행하도록 정책을 설정할 수 있으며, Azure는 더 자주 스케줄을 지원하지 않습니다.
- 일일 스케줄의 경우 원하는 백업 시간을 입력합니다. 주별 스케줄의 경우 원하는 요일 및 백업 시간을 입력합니다. 참고: 시간을 정확히 12:00 am으로 설정하면 Azure Backup에서 문제가 발생할 수 있으므로 12:01 am이 권장됩니다.
- 매일, 매주, 매월 및 매년 백업을 얼마나 보존할지 정의합니다.

배포 기본값 설정

[]

전체 배포에 대해 **Azure** 백업을 설정하려면 다음 단계를 수행하십시오**.**

1. 배포 세부 정보 페이지로 이동하고 백업 기본값 을 선택합니다
2. 드롭다운 메뉴에서 서버 유형을 선택합니다. 서버 유형은 다음과 같습니다.

```
Data: these are for LOB/database server types
Infrastructure: these are platform servers
Power User: these are for Users with a TS server dedicated solely to
them
TS: these are terminal servers that Users launch sessions on
TSData: these are servers doubling as terminal and data servers.
```

    - 그러면 전체 배포에 대한 중요 백업 설정이 정의됩니다. 이러한 설정은 나중에 필요에 따라 서버별 수준에서 재정의하고 설정할 수 있습니다.
3. 설정 휠을 클릭하면 나타나는 편집 팝업 창이 나타납니다.
4. 다음 백업 설정을 선택합니다.

```
On or off
Daily or weekly
What time of day backups take place
How long each backup type (daily, weekly, etc.) should be retained
```

5. 마지막으로, 일정 생성(또는 편집)을 클릭하여 이러한 설정을 배치합니다.

개별 백업 정책 설정

서버별 통합 백업 설정을 적용하려면 작업 영역 세부 정보 페이지로 이동합니다**.**

1. Servers(서버) 섹션으로 스크롤하여 서버 이름을 클릭합니다
2. 일정 추가를 클릭합니다
3. 원하는 대로 백업 설정을 적용하고 Create Schedule 을 클릭합니다

백업에서 복원 중입니다

지정된 **VM**의 백업을 복원하려면 먼저 해당 **Workspace** 세부 정보 페이지로 이동합니다**.**

1. Servers(서버) 섹션으로 스크롤하여 서버 이름을 클릭합니다
2. Backups(백업) 섹션으로 스크롤하고 휠을 클릭하여 옵션을 확장한 다음 둘 중 하나를 선택합니다
3. Server(서버) 또는 Restore to Disk(디스크로 복원)(백업에서 드라이브를 연결하여 백업에서 기존 VM 버전으로 데이터를 복사할 수 있습니다.)
4. 다른 복원 시나리오에서와 마찬가지로 이 시점에서 복원을 계속 진행합니다.

비용은 유지하려는 일정에 따라 달라지며, Azure 백업 비용에 따라 전적으로 결정됩니다. VM에 대한 백업 가격은 Azure 비용 계산기에서 확인할 수 있습니다. https://azure.microsoft.com/en-us/pricing/calculator/

# 가상 머신 클론 생성

## 개요

VDS(가상 데스크톱 서비스)는 기존 가상 머신(VM)을 복제할 수 있는 기능을 제공합니다. 이 기능은 정의된 사용자 수가 증가하거나 사용 가능한 리소스 풀에 서버를 추가할 때 서버 유닛 수 가용성을 자동으로 높이도록 설계되었습니다.

관리자는 다음 두 가지 방법으로 VDS에서 복제를 사용합니다.

1. 필요 시 기존 클라이언트 서버에서 새 서버를 자동으로 생성합니다
2. 파트너가 정의 및 제어하는 규칙에 따라 리소스를 자동으로 확장하기 위한 새로운 클라이언트 서버의 사전 예방적 자동 생성

## 공유 서버를 추가하기 위한 복제

클론은 기존 가상 머신의 복제본입니다. 클론 생성 기능은 게스트 운영 체제와 애플리케이션을 설치하는 데 시간이 오래 걸릴 수 있으므로 시간을 절약하고 관리자가 확장할 수 있도록 도와줍니다. 클론을 사용하면 단일 설치 및 구성 프로세스를 통해 가상 머신의 복제본을 여러 개 만들 수 있습니다. 이는 일반적으로 다음과 같습니다.

1. 원하는 모든 응용 프로그램 및 설정을 TS 또는 TSD 서버에 설치합니다
2. 소스 서버의 작업 공간 > 서버 섹션 > 기어 아이콘 으로 이동하고 클론 을 클릭합니다
3. 클론 프로세스를 실행하도록 허용(일반적으로 45-90분)
4. 마지막 단계에서는 복제된 서버를 활성화하여 새로운 연결을 수락하기 위해 RDS 풀에 넣습니다. 복제된 서버는 복제가 완료된 후 개별 구성이 필요할 수 있으므로 VDS는 관리자가 수동으로 서버를 회전시킬 때까지 기다립니다.

필요한 만큼 반복합니다.[]

공유 세션 호스트 환경에서 사용자의 용량을 늘리기 위해 세션 호스트를 복제하는 작업은 몇 단계만으로 간단하게 수행할 수 있습니다**.**

1. 복제할 세션 호스트를 선택하고 현재 시스템에 로그인되어 있는 사용자가 없는지 확인합니다.
2. VDS에서 대상 클라이언트의 Workspace로 이동합니다. Servers(서버) 섹션으로 스크롤하여 Gear(기어) 아이콘을 클릭하고 Clone(클론) 을 선택합니다. 이 프로세스는 상당한 시간이 소요되며 소스 시스템이 오프라인 상태가 됩니다. 30분 이상 소요됩니다.

[] []

3. 이 프로세스는 서버를 종료하고, 서버를 다른 이미지로 복제하고, 고객에게 다음 TS 번호로 이미지를 Sysprep 합니다. 서버 목록에서 서버가 _Type=Staged_and_Status=Activation Required_로 표시됩니다.

   []

4. 서버에 로그온하여 서버가 프로덕션 준비가 되었는지 확인합니다.

   []

5. 준비가 되면 활성화 를 클릭하여 서버를 세션 호스트 풀에 추가하여 사용자 연결 수락을 시작합니다.

   []

## VDS 클로닝 프로세스 정의

단계별 프로세스는 모든 클론 서버 작업의 VDS > 배포 > 작업 기록에 자세히 설명되어 있습니다. 이 프로세스는 20개 이상의 단계로 구성됩니다. 이 단계는 하이퍼바이저에 액세스하여 클론 프로세스를 시작하고 복제된 서버를 활성화하는 것으로 끝납니다. 클론 생성 프로세스에는 다음과 같은 주요 단계가 포함됩니다.

- DNS를 구성하고 서버 이름을 설정합니다
- StaticIP를 할당합니다
- 도메인에 추가
- Active Directory를 업데이트합니다
- VDS DB(CWMGR1의 SQL 인스턴스) 업데이트
- 클론에 대한 방화벽 규칙을 생성합니다

작업 내역뿐만 아니라 모든 복제 프로세스에 대한 세부 단계는 각 파트너의 가상 데스크톱 배포의 CWMGR1에 있는 CwVmAutomationService 로그에서 볼 수 있습니다. 이러한 로그 파일 검토는 문서화되어 있습니다 "여기".

## 새 서버 자동 생성

이 VDS 기능은 정의된 사용자 수가 증가함에 따라 서버 단위 수를 자동으로 늘리도록 설계되었습니다.

파트너가 VDS("")> 클라이언트 > 개요 – VM 리소스 > 자동 스케일링. 자동 배율 조정을 활성화/비활성화할 수 있을 뿐만 아니라 각 클라이언트에 대한 사용자 지정 규칙(예: 번호/사용자/서버, 사용자당 추가 RAM 및 CPU당 사용자 수)을 생성할 수 있도록 여러 컨트롤이 표시됩니다.

> ⓘ 위 가정에서는 전체 가상 데스크톱 배포에 대해 자동 복제가 활성화되었다고 가정합니다. 예를 들어 자동화된 모든 복제를 중지하려면 DCConfig를 사용하고 고급 창에서 서버 생성 → 자동 클론 생성 설정의 선택을 취소합니다.

자동화된 클론 프로세스는 언제 실행됩니까**?**

일별 유지 관리가 실행되도록 구성된 경우 자동화된 클론 프로세스가 실행됩니다. 기본값은 자정이지만 편집할 수 있습니다. 일일 유지 보수의 일부는 각 리소스 풀에 대해 Change Resources 스레드를 실행하는 것입니다. Change Resources 스레드는 풀의 구성 사용자 수에 따라 필요한 공유 서버 수를 결정합니다(사용자 지정 가능, 서버당 10, 21, 30 등 사용자 수).

### "필요 시" 새 서버 자동 생성

이 VDS 기능을 사용하면 사용 가능한 리소스 풀에 추가 서버를 자동으로 "필요 시" 복제할 수 있습니다.

VDS 관리자는 VDS에 로그인하고 조직 또는 작업 영역 모듈 아래에서 특정 클라이언트를 찾고 개요 탭을 엽니다. 서버 타일에 모든 서버(TSD1, TS1, D1 등)가 나열됩니다. 개별 서버를 복제하려면 서버 이름의 맨 오른쪽에 있는 톱니바퀴를 클릭하고 클론 옵션을 선택하면 됩니다.

일반적으로 프로세스는 약 1시간 정도 걸립니다. 그러나 기간은 VM의 크기와 기본 하이퍼바이저의 사용 가능한 리소스에 따라 달라집니다. 복제되는 서버는 재부팅해야 하므로 파트너는 일반적으로 몇 시간 이후 또는 예약된 유지 관리 기간 동안 수행됩니다.

TSData 서버를 복제할 때, 단계 중 하나는 c:\Home, c:\Data 및 c:\Pro 폴더를 삭제하여 중복 파일이 없도록 하는 것입니다. 이 경우 클론 프로세스가 실패했습니다. 이 파일을 삭제하는 동안 문제가 발생했습니다. 이 오류는 모호합니다. 일반적으로 이는 열린 파일 또는 프로세스가 있기 때문에 클론 이벤트가 실패했음을 의미합니다. 다음 시도에서는 모든 AV를 비활성화하십시오(이 오류에 대한 설명이 있을 수 있음).

# 디스크 공간 자동 증가 기능

### 개요

NetApp은 사용자가 언제든지 문서에 액세스하고 저장할 수 있는 공간을 관리자에게 쉽게 제공할 수 있는 방법을 인식합니다. 또한 VM에는 백업을 성공적으로 완료할 수 있는 충분한 여유 공간이 있으므로 관리자와 재해 복구 및 무중단 업무 운영 계획이 가능하게 되고 그 역량을 강화할 수 있습니다. 이를 염두에 두고 드라이브가 공간 부족에 의해 실행될 때 사용 중인 관리 디스크를 다음 계층으로 자동 확장하는 기능을 구축했습니다.

이 설정은 Azure의 모든 새 VDS 배포에서 기본적으로 적용되며 모든 배포에서 기본적으로 사용자와 테넌트의 백업을 보호하도록 합니다.

관리자는 배포 탭으로 이동한 다음 배포를 선택한 다음 해당 서버에서 CWMGR1 서버에 연결하여 이 기능을 사용할 수 있는지 확인할 수 있습니다. 그런 다음 바탕 화면에서 DCConfig 바로 가기를 열고 고급을 클릭한 다음 아래로 스크롤합니다.

[]

관리자는 DCConfig의 동일한 고급 섹션에 있는 관리 대상 디스크의 다음 계층으로 이동하기 전에 사용 가능한 드라이브의 GB 여유 공간 또는 백분율 중 원하는 여유 공간의 크기를 변경할 수 있습니다.

[]

몇 가지 실제 적용 사례:

- 드라이브에서 50GB 이상을 사용하려면 MinFreeSpaceGB를 50으로 설정합니다
- 드라이브의 15% 이상이 사용 가능한 상태인지 확인하려면 MinFreeSpacePercent를 10에서 15로 설정합니다.

이 작업은 서버의 표준 시간대의 자정에 수행됩니다.

# Azure Key Vault에서 VDS 자격 증명에 액세스

## 개요

CWASetup 5.4는 이전 Azure 배포 방법에서 출발합니다. 구축을 시작하는 데 필요한 정보의 양을 줄이기 위해 구성 및 검증 프로세스가 간소화됩니다. 제거된 프롬프트 중 대부분은 로컬 VM 관리자, SMTP 계정, 기술 계정, SQL SA 등과 같은 자격 증명 또는 계정을 위한 것입니다. 이러한 계정은 자동으로 생성되어 Azure Key Vault에 저장됩니다.
기본적으로 이러한 자동 생성 계정에 액세스하려면 아래에 설명된 추가 단계가 필요합니다.

- '키 볼트' 리소스를 찾아서 클릭합니다.

  [너비 = 75%]

- '설정'에서 'Shetrets'를 클릭합니다. 볼 권한이 없다는 메시지가 표시됩니다.

  [너비 = 75%]

- '액세스 정책'을 추가하여 Azure AD 계정(글로벌 관리자 또는 시스템 관리자 등)에 다음과 같은 중요한 키에 대한 액세스 권한을 부여합니다.

  [너비 = 75%]

- 이 예에서는 전역 관리자가 사용됩니다. 보안 주체를 선택한 후 '선택'을 클릭하고 '추가'를 클릭합니다.

  [너비 = 75%]

- '저장'을 클릭합니다.

  [너비 = 75%]

- 액세스 정책이 추가되었습니다.

  [너비 = 75%]

- '백렛'을 다시 방문하여 현재 이 계정이 배포 계정에 액세스할 수 있는지 확인합니다.

  [너비 = 75%]

- 예를 들어, CWMGR1에 로그인하고 그룹 정책을 업데이트하기 위해 도메인 관리자 자격 증명이 필요한 경우 각 항목을 클릭하여 cjDomainAdministratorName 및 cjDomainAdministratorPassword 아래의 문자열을 확인합니다.

  [너비 = 75%]

  [너비 = 75%]

- 값 표시 또는 복사:

  [너비 = 75%]

# Monitoring and Antivirus를 적용합니다

## 개요

VDS(가상 데스크톱 서비스) 관리자는 플랫폼 인프라(최소 CWMGR1로 구성) 및 기타 모든 인프라 및 VM(가상 머신)을 모두 모니터링할 책임이 있습니다. 대부분의 경우 관리자는 데이터 센터/IaaS 공급자와 함께 인프라스트럭처(하이퍼바이저/SAN) 모니터링을 직접 정렬합니다. 관리자는 일반적으로 선호하는 원격 관리 및 모니터링(RMM) 솔루션을 배포하여 터미널 서버 및 데이터 서버를 모니터링할 책임이 있습니다.

안티바이러스(Anti-Virus)는 관리자의 책임입니다(플랫폼 인프라 및 터미널/데이터 서버 VM 모두 해당). 이 프로세스를 간소화하기 위해 Azure 서버용 VDS에는 기본적으로 Windows Defender가 적용됩니다.

타사 솔루션을 설치할 때 VDS 자동화를 방해할 수 있는 방화벽 또는 기타 구성 요소를 포함하지 마십시오.

보다 구체적으로, 매우 구체적인 안티바이러스 정책이 기본적으로 적용되는 경우 이러한 안티바이러스 에이전트가 Virtual Desktop Service에서 관리하는 서버에 설치될 때 부작용이 발생할 수 있습니다.

전체 지침은 VDS 플랫폼 자동화는 일반적으로 안티바이러스 또는 안티맬웨어 제품의 영향을 받지 않지만 모든 플랫폼 서버(CWMGR1, RDGateways, HTML5Gateways, FTP 등)에서 다음 프로세스에 대한 예외/예외를 추가하는 것이 가장 좋은 방법입니다.

```
*\paexec.exe
*\paexec_1_25.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CW Automation
Service\cw.automation.service.exe
C:\Program
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Printer.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Services.exe
```

또한 클라이언트 서버에서 다음 프로세스를 안전하게 나열하는 것이 좋습니다.

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe
C:\Program Files\CloudWorkspace\Pen\Pen.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

# 매핑된 드라이브 추가 및 이동

## 개요

기본적으로 최종 사용자 세션에 표시되는 공유 폴더는 세 개입니다. 이러한 폴더는 정의된 스토리지 계층에서 찾을 수 있습니다. 파일 서버(TSD1 또는 D1) 또는 Azure Files, Azure NetApp Files, NetApp CVO, NetApp CVS와 같은 스토리지 서비스에 있을 수 있습니다.

이 문서에서는 명확한 이해를 돕기 위해 회사 코드 "NECA"를 사용하는 고객을 예로 소개합니다. 이 예제에서는 NECATSD1이라는 단일 TDS1 서버가 구축되었다고 가정합니다. 폴더를 다른 VM("NECAD1"이라는 이름)으로 이동하는 프로세스를 진행할 것입니다. 이 전략은 다음 예와 같이 동일한 시스템의 파티션 간 또는 다른 시스템으로 이동하는 데 사용할 수 있습니다.

폴더 시작 위치:

- 데이터: NECATSD1\C:\data\NECA\(TSD1은 첫 번째 터미널 서버이며 데이터 서버로도 작동함을 의미)
- FTP: NECATSD1\C:\FTP\NECA\
- 홈: NECATSD1\C:\HOME\NECA\

폴더 종료 위치:

- 데이터: NECAD1\G:\data\NECA\(D1은 첫 번째 데이터 서버임을 의미)
- FTP: 동일한 프로세스가 적용되며 세 배 이상 설명할 필요가 없습니다
- 가정: 동일한 프로세스가 적용되며 세 배 이상 설명할 필요가 없습니다

## NECAD1에서 G:에 대한 디스크를 추가합니다

1. E: 드라이브에 공유 폴더를 배치하려면 하이퍼바이저(예 Azure Management Portal)을 사용하여 초기화한 다음 포맷합니다

   []

2. 기존 폴더(NECATSD1, C:\) 경로를 새 위치(NECAD1, G:\)로 복사합니다.
3. 원래 위치에서 새 위치로 폴더를 복사합니다.

   []

## 원본 폴더 공유에서 정보 수집(NECATSD1, C:\DATA\NECA\)

1. 원래 위치의 폴더와 정확히 동일한 경로를 사용하여 새 폴더를 공유합니다.
2. 새 NECAD1, G:\data\ 폴더를 열면 회사 코드 "NECA"라는 이름의 폴더가 이 예에 표시됩니다.

   []

3. 원본 폴더 공유의 보안 권한을 확인합니다.

   []

4. 다음은 일반적인 설정이지만 보존해야 하는 기존 사용자 정의가 있는 경우 원래 설정을 복사하는 것이 중요합니다. 다른 모든 사용자/그룹 권한은 새 폴더 공유에서 제거해야 합니다
   - 시스템: 모든 권한이 허용됩니다
   - LocalClientDHPAccess(로컬 컴퓨터): 모든 권한이 허용됩니다
   - ClientDHPAccess (도메인): 모든 권한이 허용됩니다
   - NECA - 도메인에 있는 모든 사용자: "모든 권한"을 제외한 모든 권한이 허용됩니다

## 공유 경로 및 보안 권한을 새 공유 폴더에 복제합니다

1. 새 위치(NECAD1, G:\data\NECA\)로 돌아가서 동일한 네트워크 경로(시스템 제외)로 NECA 폴더를 공유합니다(예: "NECA-DATA$").

   []

2. 사용자 보안을 위해 모든 사용자를 추가하려면 해당 권한을 일치시킬 수 있도록 설정합니다.

   []

3. 이미 있을 수 있는 다른 사용자/그룹 권한을 제거합니다.

   []

## 그룹 정책 편집(폴더가 새 컴퓨터로 이동된 경우에만)

1. 그런 다음 그룹 정책 관리 편집기에서 드라이브 맵을 편집합니다. Azure AD 도메인 서비스의 경우 매핑은 다음 위치에 있습니다.

   ```
   “Cloud Workspace Users > User Configuration > Preferences > Windows Settings> Drive Maps”
   ```

   []

2. 그룹 정책이 업데이트되면 다음에 각 사용자가 연결할 때 새 위치를 가리키는 매핑된 드라이브가 표시됩니다.
3. 이때 NECATSD1, C:\에서 원래 폴더를 삭제할 수 있습니다.

## 문제 해결

최종 사용자가 빨간색 X가 있는 매핑된 드라이브를 볼 경우 드라이브를 마우스 오른쪽 버튼으로 클릭하고 DISCONNECT를 선택합니다. 로그아웃한 후 드라이브에 다시 로그인하면 올바르게 표시됩니다.[]

## Copyright Information



## Trademark Information