Amministrazione del sistema

Virtual Desktop Service

NetApp
May 24, 2023

Sommario

Amministrazione del sistema

Creare un account Domain Admin ("livello 3")

Panoramica

Occasionalmente, gli amministratori VDS avranno bisogno di credenziali a livello di dominio per gestire l'ambiente. In VDS questi account sono denominati "livello 3" o ".TECH".

Queste istruzioni mostrano come è possibile creare questi account con le autorizzazioni appropriate.

Controller di dominio Windows Server

Quando si esegue un controller di dominio ospitato internamente (o un controller di dominio locale collegato ad Azure tramite un percorso VPN/Express), è possibile gestire gli account .TECH direttamente in Active Directory Manager.

1. Connettersi al controller di dominio (CWMGR1, DC01 o alla macchina virtuale esistente) con un account admin di dominio (.TECH).
2. Creare un nuovo utente (se necessario).
3. Aggiungere l'utente al gruppo di sicurezza "tecnici livello 3"

   [Management.System Administration.creare un account admin di dominio 9ee17] |

Management.System_Administration.create_domain_admin_account-9ee17.png

a. Se il gruppo di sicurezza "tecnici livello 3" non è presente, crearlo e renderlo membro del gruppo di sicurezza "infrastruttura CW".

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

Management.System_Administration.create_domain_admin_account-0fc27.png

L'aggiunta di ".tech" alla fine del nome utente è una procedura consigliata per delineare gli account amministratore dagli account utente finali.

Servizi di dominio ad Azure

Se vengono eseguiti in Azure ad Domain Services o se si gestisce un utente in Azure ad, questi account possono essere gestiti (ad esempio, la modifica della password) nel portale di gestione Azure come un normale utente Azure ad.

È possibile creare nuovi account, aggiungendoli a questi ruoli per ottenere le autorizzazioni necessarie:

1. Amministratori di AAD DC
2. ClientDHPAccess
3. Amministratore globale nella directory.

L'aggiunta di ".tech" alla fine del nome utente è una procedura consigliata per delineare gli account amministratore dagli account utente finali.

[]

Accesso temporaneo a terze parti

Panoramica

Fornire l'accesso a terze parti è una pratica comune quando si esegue la migrazione a qualsiasi soluzione cloud.

Gli amministratori VDS spesso scelgono di non concedere a queste terze parti lo stesso livello di accesso di cui dispongono, per seguire una policy di accesso di sicurezza "meno richiesta".

Per impostare l'accesso admin per terze parti, accedere a VDS e accedere al modulo Organizations (organizzazioni), fare clic sull'organizzazione e fare clic su Users & Groups (utenti e gruppi).

Quindi, creare un nuovo account utente per la terza parte e scorrere verso il basso fino a visualizzare la sezione accesso amministratore e selezionare la casella per abilitare i diritti di amministratore.

[]

VDS Admin viene quindi visualizzata la schermata di configurazione di Admin Access. Non è necessario modificare il nome utente, l'accesso o la password: Basta aggiungere un numero di telefono e/o un'e-mail se si desidera applicare l'autenticazione multifattore e selezionare il livello di accesso da concedere.

Per gli amministratori di database come un VAR o un ISV, *Server* è generalmente l'unico modulo di accesso richiesto.

[]

Una volta salvato, l'utente finale ottiene l'accesso alle funzioni di gestione automatica accedendo a VDS con le proprie credenziali utente standard di Virtual Desktop.

Quando l'utente appena creato effettua l'accesso, vedrà solo i moduli assegnati. Possono selezionare l'organizzazione, scorrere verso il basso fino alla sezione Server e connettersi al nome del server indicato (ad esempio, <XYZ> D1, dove XYZ è il codice della società e D1 indica che il server è un server dati. Nell'esempio riportato di seguito, viene indicato di connettersi al server TSD1 per eseguire le assegnazioni.

[]

Configurare la pianificazione del backup

Panoramica

VDS è in grado di configurare e gestire i servizi di backup nativi in alcuni provider di infrastrutture, tra cui Azure.

Azure

In Azure, VDS è in grado di configurare automaticamente i backup utilizzando i backup nativi "Backup cloud Azure" Con storage ridondante in locale (LRS). Se necessario, lo storage geodundant (GRS) può essere configurato nel portale di gestione Azure.

- È possibile definire singole policy di backup per ciascun tipo di server (con raccomandazioni predefinite). Inoltre, è possibile assegnare a singoli computer una pianificazione indipendente (dal tipo di server) dall'interfaccia utente VDS. Questa impostazione può essere applicata accedendo alla vista dettagli server facendo clic sul nome del server nella pagina Workspace (vedere il video seguente: Impostazione di criteri di backup individuali)
  - Dati
    - Backup con 7 backup giornalieri, 5 settimanali e 2 mensili. Aumentare i periodi di conservazione in base ai requisiti di business.
    - Ciò vale sia per un server dati dedicato che per le VM VPS add-on per applicazioni e database.
  - Infrastruttura
    - CWMGR1 – Backup giornaliero e conservazione 7 giorni su 7, 5 settimane, 2 mesi.
    - Gateway RDS: Backup settimanale e conservazione 4 alla settimana.
    - Gateway HTML5: Backup settimanale e conservazione 4 settimanale.
  - PowerUser (noto anche come utente VDI)
    - Non eseguire il backup della macchina virtuale poiché i dati devono essere memorizzati su un server D1 o TSD1.
    - Tenere presente che alcune applicazioni memorizzano i dati in locale e, in tal caso, è necessario prendere speciali considerazioni.
    - In caso di guasto di una macchina virtuale, è possibile creare una nuova macchina virtuale tramite la clonazione di un'altra. Nel caso in cui sia presente una sola VM VDI (o una build di VM univoca), si consiglia di eseguirne il backup in modo che non sia necessaria una ricostruzione completa della VM.
    - Se necessario, anziché eseguire il backup di tutti i server VDI, è possibile ridurre al minimo i costi configurando manualmente una singola macchina virtuale per il backup direttamente nel portale Azure Management.
  - TS
    - Non eseguire il backup della macchina virtuale poiché i dati devono essere memorizzati su un

server D1 o TSD1.

- Tenere presente che alcune applicazioni memorizzano i dati in locale e, in tal caso, è necessario prendere speciali considerazioni.
- In caso di guasto di una macchina virtuale, è possibile creare una nuova macchina virtuale tramite la clonazione di un'altra. Nel caso in cui sia presente una sola VM TS, si consiglia di eseguirne il backup in modo che non sia necessaria una ricostruzione completa della VM.
- Se necessario, anziché eseguire il backup di tutti i server TS, è possibile ridurre al minimo i costi configurando manualmente una singola macchina virtuale per il backup direttamente nel portale Azure Management.

◦ TSData

- Backup con 7 backup giornalieri, 5 settimanali e 2 mensili. Aumentare i periodi di conservazione in base ai requisiti di business.

- Le policy possono essere impostate per eseguire backup giornalieri o settimanali, Azure non supporta pianificazioni più frequenti.
- Per le pianificazioni giornaliere, inserire l'ora preferita per eseguire il backup. Per le pianificazioni settimanali, inserire il giorno e l'ora preferiti per eseguire il backup. Nota: Se si imposta l'ora esattamente alle 12:00, si possono verificare problemi in Azure Backup, quindi si consiglia di eseguire le 12:01.
- Definire il numero di backup giornalieri, settimanali, mensili e annuali da conservare.

Impostazione delle impostazioni predefinite di implementazione

[]

Per configurare il backup di Azure per l'intera implementazione, attenersi alla seguente procedura:

1. Accedere alla pagina Deployments Detail (Dettagli implementazioni) e selezionare Backup Defaults (Backup predefiniti)
2. Selezionare un tipo di server dal menu a discesa. I tipi di server sono:

```
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.
```

◦ In questo modo verranno definite le impostazioni di backup generali per l'intera implementazione. Questi possono essere ignorati e impostati in un secondo momento a un livello specifico del server, se lo si desidera.

3. Fare clic sulla rotella delle impostazioni, quindi sulla finestra a comparsa Edit (Modifica) che viene visualizzata.
4. Selezionare le seguenti impostazioni di backup:

```
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. Infine, fare clic su Create (o Edit) Schedule (Crea (o Modifica) pianificazione) per attivare queste impostazioni.

Impostazione di singoli criteri di backup

Per applicare le impostazioni di backup integrato specifiche del server, accedere alla pagina dei dettagli dell'area di lavoro.

1. Scorrere verso il basso fino alla sezione Server e fare clic sul nome di un server
2. Fare clic su Aggiungi pianificazione
3. Applicare le impostazioni di backup desiderate e fare clic su Create Schedule (Crea pianificazione)

Ripristino dal backup

Per ripristinare i backup di una determinata macchina virtuale, accedere alla pagina dei dettagli dell'area di lavoro.

1. Scorrere verso il basso fino alla sezione Server e fare clic sul nome di un server
2. Scorrere verso il basso fino alla sezione Backup e fare clic sulla manopola per espandere le opzioni, quindi selezionare una delle due opzioni
3. Restore to Server (Ripristina su server) o Restore to Disk (Ripristina su disco) (collegare un disco dal backup in modo da poter copiare i dati dal backup alla versione esistente della macchina virtuale).
4. Procedere con il ripristino da questo punto in poi come in qualsiasi altro scenario di ripristino.

> ⓘ I costi dipendono dalla pianificazione che si desidera mantenere e sono interamente determinati dai costi di backup di Azure. I prezzi di backup per le macchine virtuali sono disponibili in Azure Cost Calculator: https://azure.microsoft.com/en-us/pricing/calculator/

Clonazione di macchine virtuali

Panoramica

Virtual Desktop Service (VDS) consente di clonare una macchina virtuale (VM) esistente. Questa funzionalità è progettata per aumentare automaticamente la disponibilità del numero di unità server in base all'aumento del numero di utenti definiti O per aggiungere server ai pool di risorse disponibili.

Gli amministratori utilizzano la clonazione in VDS in due modi:

1. Creazione automatica on-demand di nuovo server da un server client esistente
2. Creazione automatica proattiva di nuovi server client per la scalabilità automatica delle risorse in base alle regole definite e controllate dai partner

Cloning per aggiungere altri server condivisi

Un clone è una copia di una macchina virtuale esistente. La funzionalità di cloning consente di risparmiare tempo e di scalare gli amministratori, poiché l'installazione di un sistema operativo guest e di applicazioni può richiedere molto tempo. Con i cloni, è possibile eseguire molte copie di una macchina virtuale da un singolo processo di installazione e configurazione. Questo aspetto in genere è simile a:

1. Installare tutte le applicazioni e le impostazioni desiderate su un server TS o TSD
2. Accedere a: Aree di lavoro > Sezione Server > icona ingranaggio per il server di origine > fare clic su Clone (Clona)
3. Consentire l'esecuzione del processo di clonazione (in genere 45-90 minuti)
4. La fase finale attiva il server clonato, inserendolo nel pool RDS per accettare nuove connessioni. I server clonati potrebbero richiedere una singola configurazione dopo essere stati clonati, in modo che VDS aspetti che l'amministratore metta manualmente in rotazione il server.

Ripetere tutte le volte necessarie.[]

Per aumentare la capacità degli utenti in un ambiente host di sessione condivisa, la clonazione di un host di sessione è un processo semplice che richiede solo pochi passaggi.

1. Selezionare un host di sessione da clonare e verificare che nessun utente sia attualmente connesso alla macchina.
2. In VDS, accedere all'area di lavoro del client di destinazione. Scorrere fino alla sezione Server, fare clic sull'icona ingranaggio e selezionare Clone (Clona). Questo processo richiede molto tempo e porta il computer di origine offline. Sono previsti oltre 30 minuti per il completamento.

   [] []

3. Il processo arresta il server, clonerà il server in un'altra immagine e preparerà l'immagine al successivo numero di servizio per il cliente. Il server viene visualizzato come *Type=Staged* e *Status=Activation Required* nell'elenco Servers (Server).

   []

4. Accedere al server e verificare che il server sia pronto per la produzione.

   []

5. Quando si è pronti, fare clic su Activate (attiva) per aggiungere il server al pool di host di sessione e iniziare ad accettare le connessioni utente.

   []

Definizione del processo di cloning VDS

Il processo passo per passo è descritto in dettaglio in VDS > Deployment > Task History (VDS > implementazione > Cronologia attività) in qualsiasi operazione di Clone Server. Il processo prevede oltre 20 passaggi, che iniziano con l'accesso all'hypervisor per avviare il processo di clonazione e terminano con l'attivazione del server clonato. Il processo di cloning include passaggi chiave come:

- Configurare il DNS e impostare il nome del server
- Assegnare StaticIP

- Aggiungi al dominio
- Aggiornare Active Directory
- Aggiorna database VDS (istanza SQL su CWMGR1)
- Creare regole firewall per il clone

Oltre a Cronologia attività, i passaggi dettagliati per qualsiasi processo di cloning possono essere visualizzati nel log CwVmAutomationService su CWMGR1 in Virtual Desktop Deployment di ciascun partner. La revisione di questi file di log è documentata "qui".

Creazione automatica di nuovi server

Questa funzionalità VDS è progettata per aumentare automaticamente la disponibilità del numero di unità server in base all'aumento del numero di utenti definito.

Il partner definisce e gestisce tramite VDS ("") > Client > Panoramica – risorse VM > scalabilità automatica. Sono esposti diversi controlli per consentire ai partner di attivare/disattivare la scalabilità automatica e creare regole personalizzate per ciascun client, ad esempio: Numero/utenti/server, RAM aggiuntiva per utente e numero di utenti per CPU.

In precedenza, si presuppone che la clonazione automatica sia abilitata per l'intera implementazione di Virtual Desktop. Ad esempio, per interrompere tutti i cloning automatici, utilizzare DCConfig, nella finestra Advanced (Avanzate), deselezionare Server Creation (creazione server)→Automated Cloning enabled (clonazione automatica abilitata).

Quando viene eseguito il processo di clonazione automatica?

Il processo automatizzato di clonazione viene eseguito quando la manutenzione giornaliera è configurata per l'esecuzione. L'impostazione predefinita è mezzanotte, ma è possibile modificarla. Parte della manutenzione giornaliera consiste nell'eseguire il thread Change Resources per ogni pool di risorse. Il thread Change Resources determina il numero di server condivisi richiesti in base al numero di utenti della configurazione del pool (personalizzabile; può essere 10, 21, 30, ecc. utenti per server).

Creazione automatica "on-demand" di nuovi server

Questa funzionalità VDS consente la clonazione automatica "on-demand" di server aggiuntivi nei pool di risorse disponibili.

L'amministratore VDS accede a VDS e, sotto i moduli Organizations (organizzazioni) o Workspaces (aree di lavoro), individua il client specifico e apre la scheda Overview (Panoramica). La sezione Server elenca tutti i server (TSD1, TS1, D1, ecc.). Per clonare un singolo server, fare clic sul simbolo all'estrema destra del nome del server e selezionare l'opzione Clone (Clona).

In genere, il processo dovrebbe richiedere circa un'ora. Tuttavia, la durata dipende dalle dimensioni della macchina virtuale e dalle risorse disponibili dell'hypervisor sottostante. Tenere presente che il server clonato dovrà essere riavviato, in modo che i partner eseguano in genere dopo l'orario di lavoro o durante una finestra di manutenzione pianificata.

Durante la clonazione di un server TSData, uno dei passaggi consiste nell'eliminare le cartelle c: Home, c: Dati e c: Pro in modo che non siano file duplicati. In questo caso, il processo di clonazione non è riuscito. Si sono verificati problemi durante l'eliminazione di questi file. Questo errore è vago. In genere, questo significa che l'evento clone non è riuscito a causa di un file o processo aperto. Tentativo successivo, disattivare qualsiasi AV (perché questo potrebbe spiegare questo errore).

Funzione di aumento automatico dello spazio su disco

Panoramica

NetApp riconosce la necessità di offrire agli amministratori un modo semplice per garantire che gli utenti abbiano sempre spazio per accedere e salvare i documenti. In questo modo, le macchine virtuali dispongono anche di spazio libero sufficiente per completare correttamente i backup, consentendo agli amministratori e ai piani di disaster recovery e business continuity. Tenendo presente questo aspetto, abbiamo creato una funzionalità che espande automaticamente il disco gestito in uso al livello successivo quando un disco sta funzionando in poco spazio.

Si tratta di un'impostazione che viene applicata per impostazione predefinita a tutte le nuove implementazioni VDS in Azure, garantendo che tutte le implementazioni proteggano gli utenti e i backup del tenant per impostazione predefinita.

Gli amministratori possono verificare che sia stata eseguita questa operazione accedendo alla scheda Deployments (implementazioni), selezionando un'implementazione e quindi connettendosi al server CWMGR1. Quindi, aprire il collegamento DCConfig sul desktop, fare clic su Advanced (Avanzate) e scorrere verso il basso.

[]

Gli amministratori possono modificare la quantità di spazio libero desiderata in GB liberi o in percentuale del disco che deve essere libero prima di passare al successivo Tier di dischi gestiti nella stessa sezione Advanced di DCConfig.

[]

Alcuni esempi pratici di applicazione:

- Se si desidera assicurarsi che sul disco siano disponibili almeno 50 GB, impostare MinFreeSpaceGB su 50
- Se si desidera assicurarsi che almeno il 15% del disco sia libero, impostare MinFreeSpacePercent da 10 a 15.

Questa azione si svolge a mezzanotte del fuso orario del server.

Accesso alle credenziali VDS in Azure Key Vault

Panoramica

CWASetup 5.4 è una deviazione dai precedenti metodi di implementazione di Azure. Il processo di configurazione e convalida è ottimizzato per ridurre la quantità di informazioni necessarie per iniziare un'implementazione. Molti di questi prompt rimossi riguardano credenziali o account come Local VM Admin, SMTP account, Tech account, SQL SA, ecc. Questi account vengono ora generati automaticamente e memorizzati in un archivio chiavi Azure. Per impostazione predefinita, l'accesso a questi account generati automaticamente richiede un passaggio aggiuntivo, descritto di seguito.

- Individuare la risorsa "vault delle chiavi" e fare clic su di essa:

  [larghezza=75%]

- In 'SImpostazioni', fare clic su 'Sdecrets'. Viene visualizzato un messaggio che indica che non si è autorizzati a visualizzare:

[larghezza=75%]

- Aggiungere una ‘policy di accesso’ per concedere a un account Azure ad (come un amministratore globale o un amministratore di sistema) l’accesso a queste chiavi sensibili:

  [larghezza=75%]

- In questo esempio viene utilizzato un amministratore globale. Dopo aver selezionato l’entità, fare clic su ‘Select’ (Seleziona), quindi su ‘Add’ (Aggiungi):

  [larghezza=75%]

- Fare clic su ‘S’Save' (Salva):

  [larghezza=75%]

- Policy di accesso aggiunta correttamente:

  [larghezza=75%]

- Rivisitare i ‘Ssegreti’ per verificare che l’account disponga ora dell’accesso agli account di implementazione:

  [larghezza=75%]

- Ad esempio, se è stata richiesta la credenziale Domain Administrator per accedere a CWMGR1 e aggiornare i criteri di gruppo, controllare le stringhe in cjDomainAdministratorName e cjDomainAdministratorPassword facendo clic su ciascuna voce:

  [larghezza=75%]

  [larghezza=75%]

- Mostra o copia il valore:

  [larghezza=75%]

Applicare Monitoring and Antivirus

Panoramica

Gli amministratori di Virtual Desktop Service (VDS) sono responsabili del monitoraggio dell’infrastruttura della piattaforma (che sarà costituita da CWMGR1 al minimo) e di tutte le altre infrastrutture e macchine virtuali (VM). Nella maggior parte dei casi, gli amministratori organizzano il monitoraggio dell’infrastruttura (hypervisor/SAN) direttamente con il proprio data center/provider IaaS. Gli amministratori sono responsabili del monitoraggio di server terminal e dati, in genere implementando la soluzione RMM (Remote Management and Monitoring) preferita.

L’antivirus è responsabilità dell’amministratore (sia per l’infrastruttura della piattaforma che per le macchine virtuali dei server di dati/terminali). Per semplificare questo processo, i server VDS per Azure utilizzano Windows Defender per impostazione predefinita.

Quando si installano soluzioni di terze parti, assicurarsi di non includere firewall o altri componenti che potrebbero interferire con l'automazione VDS.

In particolare, quando per impostazione predefinita sono in vigore policy antivirus molto specifiche, ciò può causare effetti negativi quando questi agenti antivirus vengono installati su un server gestito da Virtual Desktop Service.

La nostra guida generale è che, sebbene l'automazione della piattaforma VDS non sia generalmente influenzata dai prodotti antivirus o anti-malware, è consigliabile aggiungere eccezioni/esclusioni per i seguenti processi su tutti i server della piattaforma (CWMGR1, RDGGateway, HTML5Gateway, FTP, ecc.):

```
*\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
```

Inoltre, si consiglia di elencare in modo sicuro i seguenti processi sui server client:

```
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
```

Aggiunta e spostamento di unità mappate

Panoramica

Per impostazione predefinita, sono presenti tre cartelle condivise esposte alle sessioni dell'utente finale. Queste cartelle si trovano nel layer di storage definito. Potrebbe trattarsi di un file server (TSD1 o D1) o di un servizio di storage come Azure Files, Azure NetApp Files, NetApp CVO e NetApp CVS.

Per maggiore chiarezza, in questo articolo verrà utilizzato un cliente di esempio con il codice aziendale "NECA". Questo esempio presuppone che sia stato implementato un singolo server TDS1, denominato NECATSD1. Lavoreremo attraverso il processo di spostamento di una cartella in un'altra macchina virtuale (chiamata "NECAD1"). Questa strategia può essere utilizzata per passare da una partizione all'altra sullo stesso computer o su un'altra macchina, come illustrato nell'esempio seguente…

Percorso iniziale cartelle:

- Dati: NECATSD1 (TSD1 significa che è il primo Terminal Server e funziona anche come Data Server)

- FTP: NECATSD1
- Home: NECATSD1

Posizione finale cartelle:

- Data: NECAD1/G: Data (il D1significa che è il primo server dati)
- FTP: Lo stesso processo si applica, non è necessario descriverlo per 3 volte
- Home: Lo stesso processo si applica, non è necessario descriverlo per 3 volte

Add disk for G (Aggiungi disco per G): Su NECAD1

1. Per inserire la cartella condivisa nell'unità e: È necessario aggiungerne una tramite l'hypervisor (ad esempio Azure Management Portal), quindi inizializzarla e formattarla

   []

2. Copiare il percorso della cartella esistente (su NECATSD1, C:) nella nuova posizione (su NECAD1, G:)
3. Copiare le cartelle dalla posizione originale alla nuova posizione.

   []

Raccolta di informazioni dalla condivisione della cartella originale (NECATSD1, C: Data)

1. Condividere la nuova cartella utilizzando lo stesso percorso della cartella nella posizione originale.
2. Aprire la nuova cartella NECAD1, G: E nell'esempio viene visualizzata una cartella denominata codice società, "NECA".

   []

3. Nota: Le autorizzazioni di sicurezza della condivisione della cartella originale:

   []

4. Di seguito viene riportato il setup tipico, tuttavia è importante copiare le impostazioni originali nel caso in cui siano presenti personalizzazioni da conservare. Tutte le altre autorizzazioni utente/gruppo devono essere rimosse dalla nuova condivisione della cartella
   - SISTEMA:autorizzazioni consentite
   - LocalClientDHPAccess (sul computer locale):autorizzazioni consentite
   - ClientDHPAccess (sul dominio): Sono consentite tutte le autorizzazioni
   - NECA-All users (sul dominio): Sono consentite tutte le autorizzazioni, ad eccezione di "controllo completo"

Replicare il percorso di condivisione e le autorizzazioni di sicurezza nella nuova cartella condivisa

1. Tornare alla nuova posizione (NECAD1, G: Data) e condividere la cartella NECA con lo stesso percorso di rete (escluso il computer), nel nostro esempio "neca-data"

   []

2. Per la sicurezza degli utenti, aggiungere tutti gli utenti e impostare le relative autorizzazioni in modo che corrispondano.

   []

3. Rimuovere qualsiasi altra autorizzazione utente/gruppo che potrebbe già esistere.

   []

Modifica criteri di gruppo (solo se la cartella viene spostata su una nuova macchina)

1. Quindi, modificare Drive Maps (Mappe dischi) in Group Policy Management Editor (Editor di gestione dei criteri di gruppo). Per Azure ad Domain Services, la mappatura si trova in:

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

   []

2. Una volta aggiornati i criteri di gruppo, alla successiva connessione di ciascun utente, verranno visualizzati i dischi mappati che vengono riportati alla nuova posizione.
3. A questo punto è possibile eliminare le cartelle originali su NECATSD1, C:.

Risoluzione dei problemi

Se l’utente finale visualizza le unità mappate con una X rossa, fare clic con il pulsante destro del mouse sull’unità e selezionare Disconnect (Disconnetti). La disconnessione e la riconnessa dell’unità saranno presenti correttamente.[]